Business Standard

Data protection legislation is best bet for Aadhaar security, say experts

Legal experts note that the implementation of the Aadhaar Act has accentuated the gaps in various data security and privacy laws in the country

Sudipto Dey Last Updated at January 15, 2018 00:54 IST

The public consultations by the Srikrishna Committee, drafting the legal framework for data protection, could not have come at a more opportune time. The committee, headed by retired Supreme Court (SC) judge B N Srikrishna, currently on a month-long tour of cities, including Delhi, Hyderabad, Bengaluru and Mumbai, is seeking suggestions on what should be the underlying principles for the country's proposed data protection law.The brouhaha over recent unauthorised access to the Aadhaar database has put the spotlight on the ability of the Aadhaar Act, 2016, to protect and secure an individual’s personal data. This comes at a time when the SC will begin final hearing from on Wednesday on the petitions challenging the Aadhaar scheme. egal experts note that the implementation of the Aadhaar Act has accentuated the gaps in various data security and privacy laws in the country. “The current Aadhaar Act is outdated as the government moves to make Aadhaar mandatory,” says Pavan Duggal, advocate, Supreme Court. The Act does not adequately deal with parameters for cyber security and privacy protection of the Aadhaar system, he adds.The Act is specific to the Aadhaar enrolment and use, points out Tejas Karia, partner, Shardul Amarchand Mangaldas & Co. What galls legal experts is that in case of any breach or misuse of data, all

remedial powers are concentrated with the Unique Identification Authority of India (UIDAI). “Only the UIDAI can take action against any such breach,” says Vaibhav Parikh, partner, Nishith Desai Associates. What does not help matters is that the UIDAI is essentially a technology company, not an enforcement agency, experts point out.Duggal is in favour of amending the Aadhaar Act and make it topical to current ground realities. The Act needs to specifically define the roles, duties and responsibilities of various stakeholders in the Aadhaar ecosystem, he adds.However, many legal experts believe amendments to the Act need not be necessary. A data protection law, currently being framed by the Srikrishna committee, could be the answer to the data security issues faced by the UIDAI.“A data protection law will address the data security-related issues facing Aadhaar, as it will provide a framework for collecting, processing and transferring personal data,” says Karia. Most legal experts want the government to expedite the framing of such legislation.The proposed data protection law needs to be umbrella legislation, something on the lines of the Indian Penal Code, feels Supratim Chakraborty, associate partner, Khaitan & Co. However, the challenge for the country's data protection law will be to strike a balance between innovation and privacy. This is more so with technologies such as Big Data, the Internet of Things and Artificial Intelligence going mainstream in the coming years.The White Paper on Data Protection Framework, released by the Srikrishna Committee in November clearly spells out the challenges ahead in framing a data security law: “Despite an obligation to adopt adequate security safeguards, no database is 100 per cent secure.

In the light of this, the interplay between any proposed data protection framework and the existing Aadhaar framework will have to be analysed”.How the Aadhaar Act, 2016, protects dataWhat are the obligations of the Unique Identification Authority of India (UIDAI) in protecting data?According to the Aadhaar Act, 2016, the UIDAI has to ensure confidentiality of identity, information and authentication records of individuals. It has to take all necessary measures to ensure that the information in its possession or control, including those stored in the Central Identities Data Repository, is secured and protected against access, use or non-permitted disclosure under the ActDoes the Act allow an individual access to his or her own identity data? No person can collect, store or use the Aadhaar number without the owner’s consent. Further, the Act prohibits publishing the Aadhaar number. An Aadhaar number holder may request the UIDAI to provide access to his or her identity information in a manner specified through regulations. But, the Act does not give the holder access to core biometric informationWhat is the recourse for an individual in case of breach or misuse of personal data?According to the Act, only the UIDAI is authorised to file a complaint of any breach or misuse of the data. The aggrieved individual has to first approach the authority with the complaint. Only after verifying its validity can UIDAI file the complaint with the investigating agencies. Only a Chief Metropolitan Magistrate or a Chief Judicial Magistrate can try any offence punishable under this Act.What are the offences and penalties for any breach or misuse of data?Any person who causes harm or mischief to an Aadhaar number holder or impersonates by providing any false demographic or biometric information is punishable with imprisonment up to three years or with a fine up to Rs 10,000 or both. Similarly, unauthorised collection of identity information could attract jail term up to three years or a fine up to Rs 10,000. In case of a company, the fine could go up to Rs 100,000.

INDIA'S UPCOMING DATA PROTECTION FRAMEWORK

The 'Magnificent Seven'

The founding principles of data protection framework as envisaged by the Srikrishna Committee

- Law should be flexible to take into account changing technologies
- Law must apply to both government and private sector entities
- Consent should be genuine, informed and meaningful
- Processing of data should be minimal, only for the purpose sought
- Entities controlling the data should be accountable for any data processing
- Enforcement by high-powered statutory authority
- Penalties should discourage any wrongful acts

The models India could choose from

- The EU model is a rights-based one, where protection of personal data is equated with protecting the fundamental right to privacy
- The US approach focuses on protecting the individual from excessive state regulation

India could possibly settle for a hybrid model

First Published: Mon, January 15 2018. 00:41 IST