Safeguard your e-house, India legal 2017

From fighting black money to leading the nation into a cashless era, the government's demonetization drive has taken a sharp turn, plunging the nation into troubled times

~By Karnika Seth

Gone are the days when criminals would attack their victims physically. They have now found internet and computers a safe haven for committing crimes. Norton Cyber Security Report, 2015, estimated that Indians had, on an average, lost about Rs 16,558 that year through cyber crime as compared to the global average loss of Rs 23,878.

In 2015, 48 percent of the Indian online population became victims of cybercrime. Post demonetisation, cyber awareness is the need of the hour as digital space is being used by the common man to pay through e-wallets, apps and plastic money.

Law enforcement agencies need to be trained to enable them to investigate and combat cyber crime. Specialised courses need to be imparted to police officers as well as the judiciary.

Many short and long-term courses on cyber awareness have been introduced by institutions such as IGNOU, National Law Universities and NGOs such as Foundation for Institutional Reform and Education.

It is also imperative to amend the existing cyber law in the country. The Information Technology Act, 2000, has many lacunae that need immediate attention. For example, there are no express provisions in IT Act, 2000 to deal with emerging crimes such as cyber bullying, sextortion or online child trafficking. The privacy law also needs to be revisited and stricter punishments prescribed for data theft and breach of privacy. Section 43A of the IT Act requires a corporate body to maintain reasonable security practices to safeguard sensitive data of persons from whom it collects it. They are required to comply with ISO 27001 certification or other such standards as permitted by the government. In case of breach of data or its unauthorised disclosure, such a body is liable to compensate the victim. Even in the case of unauthorised access of sensitive data where Section 66 of the IT Act kicks in and prescribes punishment up to three years imprisonment and fine, it is not enough of deterrence as it is a bailable offence.

In case the cyber crime involves more than one jurisdiction, the current system of Mutual Legal Assistance Treaty is not efficacious enough to collect and preserve the required electronic evidence in a timely manner. Thus, it is imperative that India signs a cyber crime convention to address rising crimes with adequate measures to combat these from a global standpoint.

It is imperative to amend the existing cyber law in the country. The Information Technology Act, 2000, has many lacunae, such as no express provisions to deal with cyber crimes

Other steps for strengthening the enforcement of cyber laws include establishing special criminal courts for speedier adjudication of such cases and framing appropriate rules for filing of electronic evidence such as emails, phone records, etc. In addition, certain offices created under the IT Act are not functional, such as the Cyber Appellate Tribunal, due to non-appointment of functionaries. In many states, the registration authority for issuing mandatory licenses to cyber cafes has not been notified yet. Also, an Examiner of Electronic

Records, who is required to be appointed as per Section 79A of the IT Act, has not been appointed yet.

If Digital India has to take off, India should devise ways to prevent and combat cyber crimes through a national plan of action. Such a plan should include forming think-tanks for amending cyber law, suggesting infrastructure changes such as forming special criminal courts for e-crimes and imparting training to law enforcement agencies and spreading cyber awareness among the general public. An advisory by the government on how to safeguard one's financial information online will also prove useful for the public. Also, the RBI and other banks should play a vital role in making systems more secure, apart from the Computer Emergency Response Team that protects critical information infrastructure systems.

The National Informatics Centre and the Centre for Development of Advanced Computing have enhanced cyber security and imparted cyber training in India and they too have roles to play here.

A combined effort by all these institutions will ensure better cyber safeguards.

—The writer is a cyber law expert and advocate, Supreme Court