Business Standard

Forensic auditors in a fix over Data Protection Bill, seek exceptions

Fear that proposed provision will hamper investigation

Ruchika Chitravanshi & Neha Alawadhi | New Delhi **January 02, 2020** Last Updated at 23:18 IST

The Personal Data Protection Bill, 2019, has thrown up a fresh set of challenges for forensic auditors, who want the proposed law to carve out exceptions for their services, which entail accessing personal data such as bank details, emails, and medical insurance.

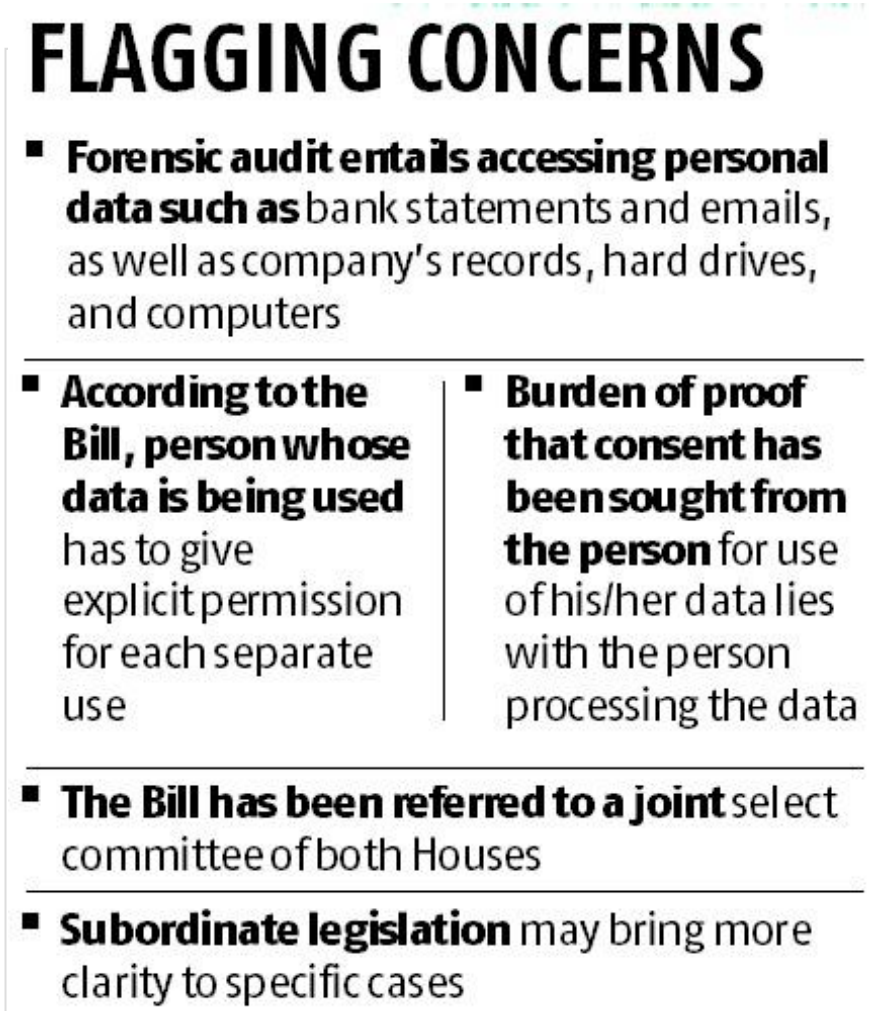
A forensic audit requires a deep inspection of the auditee company's records by accessing its hard drives, laptops, and desktop computers. The data on the hard drive contains both official and personal information, which forensic auditors have to sift through to find what they are looking for.

The data protection Bill, introduced in the Lok Sabha in the winter session, says, "Personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing." It further says personal data should not be processed by any person, except for any specific, clear and lawful purpose, and the burden of proof that consent has been sought from the person for use of his or her data lies with the person processing the data.

While processing such data, the employer needs to take formal consent from the individual for carrying out procedures such as the digital evidence recovery exercise — forensic imaging of electronic devices.

“Formal consent may impact the element of secrecy that such procedures might involve. Additionally, on the basis of a preliminary reading of the Act, it also appears that individuals have the right to withdraw consent, which has the potential to hamper any corporate investigation,” said Samir Paranjpaye, head of forensics, Grant Thornton.

Auditors warn that a lot of cascading issues will arise under the proposed law. Performing investigation on a fund trail, for instance, will lead the auditor to the personal bank account of an individual. “If there are deterrents to companies initiating forensic audit, their ethical ecosystems will get impacted. Appropriate exceptions need to be made in the Bill,” said Jayant Saran, partner, Deloitte India.



Similarly, in a cross-border scenario where a bribe might have changed currency and moved countries, data localisation will again pose a problem for auditors trying to access such information.

“In data analytics and process assessment, a lot of identifiable data will come to the fore, such as vendor information, travel expenses, and payouts,” Saran said.

The Bill does provide some exceptions to the processing of personal data of a person without their consent, but a forensic audit is unlikely to be covered by any of the scenarios mentioned.

“Provisions in the Bill are really broad. We will have to wait for subordinate legislation to deal with some of the provisions of the Bill. For several kinds of data, specific permission will have to be taken, and as these cases come up the legislation will evolve over time. Not just forensic audits, regulatory proceedings will also have an impact,” said Pratibha Jain, partner at legal advisory firm Nishith Desai Associates.

While in the normal course, forensic auditors keep the personal data aside but if search for a particular item or a keyword takes them into such data, they will have to access it and look into the matter deeper.

Moreover, if a person is allowed to withdraw some content, that too would affect the forensic investigation.

“From a contractual perspective, greater diligence will be required. Investigations have to start immediately...We err on the side of caution else both, our clients and we can be impacted,” Saran added.

While a large part of the focus with regard to the Bill has been on technology firms, it will be applicable to every industry that collects individuals’ data. In the coming days, it is likely that more such issues will arise as more and more industries realise the impact on them from the Personal Data Protection Bill.