FREQUENTLY ASKED QUESTIONS ON LAWS FOR CRISIS MANAGEMENT IN INDIA

Dipak Rao
Senior Partner
E: dipak@singhania.in

1. **Regulator or Government Agencies to be notified in discovery of data breach in India**

- When a data breach occurs in India, any person, including a company affected by it, should report it to the Indian Computer Emergency Response Team (CERT-In) established under the Information Technology Act, 2000 within a reasonable time. Certain cyber security incidents, for example, compromise of critical systems or information, malicious code attacks, identity theft, DoS and DDos attacks etc. are required to be mandatorily reported to CERT-In. The report can be communicated to the authority by telephone, fax, email, post and/or through CERT-In's website – www.cert-in.org.in.

- In the case of a data breach in a banking company or a non-banking financing company (NBFC), a report must be filed to the Reserve Bank of India (RBI) in a Security Incident Reporting (SIR) form by the company within two to six hours from the time of occurrence or on noticing such data breach. The SIR form requires particulars of the incident, specifically name of bank, details of incident, chronological order of events, etc. Further, a subsequent update must be sent to the RBI in Cyber Security Incident Reporting (CSIR) outlining further details of the breach.

2. **Legislations in India relating to criminal offences and civil wrongs in case of data breach**

- No legislation in India expressly defines data breach. However, The Information Technology Act, 2000 provides for protection to sensitive personal data or information as defined therein. It covers both civil wrongs and criminal offences. A company can be liable for a civil wrong when a breach of data is caused by its negligence in the implementation and maintenance of security protecting sensitive personal data or information which it owns, controls or operates. That failure must result in wrongful loss to the person whose data has been compromised or wrongful gain to the company causing the breach.

- A criminal breach of data is when any person, including a company, gains access to any material containing information about another person and discloses the same, without consent or in breach of a lawful service contract, to another person with an intent or with knowledge that the disclosure will cause wrongful loss to the person whose data has been compromised or wrongful gain to the person committing breach.

3. Agencies in India that can conduct dawn raids on private sector companies and legislation that give those agencies the power to undertake those inspections.

- **Competition Commission of India:** The Competition Act, 2002
- **Registrar of Companies**: Companies Act, 20131
- **Central Board of Direct Taxes**: Income Tax Act, 1961
- **Food Safety and Standards Authority**: The Food Safety and Standards Act, 2006
- **Directorate of Enforcement**: The Foreign Exchange Management Act, 19992; Prevention of Moneylaundering Act, 20023
- **The Police**: The Information Technology Act, 2000; The Code of Criminal Procedure, 1973; The Trademarks Act, 19994

Hide Note

1. Section 208 of the Companies Act, 2013.
2. Section 37 of The Foreign Exchange Management Act, 1999.
3. Section 17 of the Prevention of Money-laundering Act, 2002.
4. Section 115 of The Trademarks Act, 1999.

4. Criteria to permit or refuse the seizure of documents in India. On what bases, including privilege and/or confidentiality, may organisations refuse to permit the seizure of documents?

A company in India cannot be compelled to disclose confidential communication with its legal advisors unless such company offers itself as a witness before any court.5 Privilege in India extends to the documents which have come into existence in anticipation of litigation for the purpose of seeking legal advice with the client's legal advisors.6 However, privilege does not extend to in-house counsel employed by the company. Further, a company may refuse to permit the seizure of documents which are outside the scope of the warrant for search and seizure.

Hide Note

5. Section 129 of the Indian Evidence Act, 1872.
6. Larson & Tourbo Limited v Prime Displays (P) Ltd and Ors 2002(5) BomCR158.

5. What are the circumstances in India under which an employee is entitled to protection when reporting an alleged wrongdoing?

India has enacted the Whistle Blowers Protection Act, 2011 (the Act); however, it is not yet in force. The Act provides protection for a whistle blower in circumstances where relevant disclosures are made by the employee under the Act in good faith. The disclosures must be accompanied by a personal declaration stating that the complainant reasonably believes that the information disclosed or the allegations made by him/her are substantially true. Such disclosures can be made in writing or by electronic mail message and must contain full particulars and supporting documents, together with other relevant materials, if any.

6. What legislative protection does that employee enjoy in India?

The employee blowing the whistle against their employer or rendering assistance in the inquiry into a whistleblowing investigation enjoys the following protection under the Whistle Blowers Protection Act, 2011:

- **Protection against victimisation** – An employee can file for redress before the competent authority under the Act in circumstances where that employee is being victimised
- **Protection of identity of the employee** – The competent authority under the Act is obligated to conceal the identity, documents and information furnished by the employee for the purpose of inquiry under the Act unless so decided by the competent authority or the court directs otherwise;
- **Protection of action taken in good faith** – No prosecution or suit or other proceeding can lie against an employee whose actions were undertaken in good faith or the intent was in good faith;
- The competent authority under the Act can issue appropriate directions to concerned authorities including police for protection of the employee if it is of the opinion that such employee needs protection.

7. Main anti-corruption laws and regulations in India

The Prevention of Corruption Act, 1988: Central Vigilance Commission

- The Prevention of Money Laundering Act, 2002: Directorate of Enforcement

8. Extra-territorial effect of legislation in India

- The Prevention of Corruption Act, 1988 applies to all the citizens of India, whether located in or outside India.
- The Prevention of Money Laundering Act, 2002 (the 2002 Act) is applicable to the Indian territory, and extends beyond India in the following circumstances:
    - where any act by a person outside India constitutes an offence in that place and such act would also be an offence under Part A, Part B or Part C of the

2002 Act had it been committed on the Indian territory and such person transfers the proceeds of such offence to India, or

- where an offence has been committed under Part A, Part B or Part C of the 2002 Act and proceeds of such crime have been transferred, or an attempt has been made to transfer such proceeds or part thereof, to a place outside India.

9. Enforcement bodies in India

- **Central Bureau of Investigation** – investigates and prosecutes cases under the Prevention of Corruption Act, 1988 of undue advantage of or by public servant and the employees of Central Government, Public Sector Undertakings, Corporations or Bodies owned or controlled by the Government of India.
- **Enforcement Directorate** – investigates and prosecutes the offence of money laundering under the provisions of Prevention of Money Laundering Act, 2002 and takes actions for attachment or confiscation of property if the same is determined to be proceeds of the crime.

10. Is there any duty to report the issue, for example to a regulator?

Where an internal investigation has been undertaken into the affairs of a company, the company must report it to a regulator in the following circumstances:

- **Regional Director** – Under the Companies Act, 2013 (the 2013 Act), an internal investigation may be initiated on receipt of information by the company itself; however, such reporting is not obligatory. A company may, by passing a special resolution, intimate to the Regional Director that its affairs ought to be investigated.7 A company may also, subject to the provisions of the 2013 Act, make an application to the Regional Director for compounding of offences if the company is of the view that it has contravened any of provisions of the Act or rules or regulations made thereunder.8
- **Reserve Bank of India or Directorate of Enforcement** – The Foreign Exchange Management Act, 1999 (the 1999 Act) provides that a company may submit an application to the Reserve Bank of India or Directorate of enforcement, as the case may be, for compounding of offence if the company is of the view that it has contravened any of the provisions of the Act, regulations, rules, notifications, directions or orders thereunder.9

Hide note

7. Section 210 of the Companies Act, 2013.
8. Section 441 of the Companies Act, 2013.
9. Section 15 of the Foreign Exchange Management Act, 1999.

11. What is the protection available in India from disclosure for documents generated as a part of the investigation (for example, privilege)?

- A company in India cannot be compelled to disclose confidential communications with its legal advisors, unless such company offers itself as a witness before any court.10 Privilege in India extends to the documents which have come into existence in anticipation of litigation for the purpose of seeking legal advice with the client's legal advisors. However, privilege does not extend to any in-house counsel employed the company.
- A barrister, attorney, pleader or lawyer practicing in India is also barred from disclosing any communication made to him in the course and for the purpose of engagement by the company, except with the express consent of the company.11

Hide note

10. Section 129 of the Indian Evidence Act, 1872.
11. Section 126 of the Indian Evidence Act, 1872.

12. Is the advice given by an in-house lawyer in India in relation to the investigation privileged and/or confidential?

In order to take advantage of client-attorney privilege in India, an attorney, pleader, barrister or lawyer must be a full-time practicing attorney. However, an in-house lawyer is a full-time employee of the company and therefore outside the protection of client-attorney privilege.12

Hide note

12. Rule 49 of Chapter II – The Standards Of Professional Conduct And Etiquette, Part VI of the Bar Council of India Rules.

This compilation of FAQs was originally prepared for **TERRALEX GLOBAL CRISIS MANAGEMENT REGULATORY GUIDE 2019**

manner shall be responsible for any damage or loss of action to anyone, of any kind, in any manner, therefrom