Technology Law Analysis

November 15, 2022

CERT-IN DIRECTION NEEDS REVISITING

As readers may be aware, the Indian Computer Emergency Response Team ("**CERT-In**") issued a direction dated April 28, 2022 ("**Direction**") relating to "information security practices, procedure, prevention, response and reporting of cyber incidents".[1] The Direction created anxiety among all stakeholders. To clarify some aspects in relation to the Direction, the Ministry of Electronics and Information Technology ("**MeitY**"), on May 18, 2022, issued a list of frequently asked questions[2] ("**FAQs**").

It has been 6 months since the issuance of the Direction. In our view, CERT-In should now conduct one round of consultation with the industry and resolve outstanding issues. Further, it should also be considered whether the Direction should be withdrawn, and relevant provisions should be included in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**Rules**") by way of appropriate amendments.

Here are some reasons for this recommendation.

1. **The Direction is ultra vires the IT Act and the Rules:**

   Upon a combined reading of Section 70-B(6) of the Information Technology Act, 2000 ("**IT Act**") and Rule 15 of the Rules, it is clear that CERT-In's power to issue directions under Section 70-B(6), refers to a direction which is specific to a service provider, intermediary, data centre, or body corporate ("**Relevant Entities**"). This power cannot be exercised for issuing a general direction (like the Direction). In addition, point 3 below further elaborates how the Direction goes beyond the IT Act and the Rules.

2. **The Direction creates criminal liability that is not contemplated in the Rules**:

   Rule 17 of the Rules requires the Relevant Entities to designate a Point of Contact (PoC) to interface with CERT-In and inform regarding PoC details to CERT-In in the prescribed format. CERT-In is required to send all communications seeking information and compliance directions to the said PoC. This requirement is materially similar to the second part of paragraph (iii) of the Direction. The only differences are that the Direction also imposes this requirement on Government organisations and also prescribe the format in which the information regarding the PoC should be sent to CERT-In.

   There is also a significant overlap between the mandatorily reportable cyber security incidents listed under the Annexure to the Rules and the incidents (i) to (x) listed under Annexure-I of the Direction. The requirement to report these incidents to CERT-In is contained in Rule 12(1)(a) of the Rules and paragraph (ii) of the Direction.

   Notably, non-compliance with Rules 12 and 17 would attract fine / compensation under Section 45 of the Information Technology Act, 2000 ("**IT Act**") up to INR 25,000. However, any non-compliance with the Direction may be punishable with imprisonment of up to one year and/or fine which may extend up to INR 1,00,000 under Section 70-B(7).

   This has significant consequences. In case an entity did not designate a PoC prior to June 27, 2022 (i.e., the date of enforcement of the Direction), the entity would only be punishable with a fine of up to INR 25,000. However, subsequent to June 27, 2022 the maximum possible punishment is four times the fine which would have been payable earlier, and / or imprisonment. This would also be the case with respect to non-reporting of incidents which are listed under the Annexure to the Rules (and overlap with the incidents listed in the Direction).

3. **The Direction has the effect of amending the Rules and the IT Act**:

   As can be clearly seen, the Direction has the effect of amending the Rules as well as the IT Act. CERT-In does not have the authority to do so.[3] Moreover, under Section 87(2)(zf) of the IT Act, the power to issue rules in relation to Section 70-B is granted to the Central Government. Once any rule is issued, it is required to be laid before each House of Parliament, while it is in session, for a total period of thirty days. Subsequently, if both Houses agree that the rule should be modified, or should not be made, the rule will accordingly only take effect in such modified form or not take effect at all.

   Hence, CERT-In has bypassed the powers of the Parliament as well as the Central Government for amending the IT Act and the Rules. This is a dangerous precedent since the amendment of the IT Act would have required a democratic process, and an amendment of the Rules would need to be approved by the Parliament.

OTHER PENDING ISSUES

Research Papers

Compendium of Research Papers
January 11, 2025

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Research Articles

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals
January 15, 2025

Key changes to Model Concession Agreements in the Road Sector
January 03, 2025

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

Audio

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper

Since the issuance of the Direction, stakeholders have made representations to CERT-In and the MeitY seeking amendments/clarity in the Direction. Paragraph (v) of the Direction relating to know your customer (KYC) obligations of virtual private network (VPN) service providers is already under challenge before the Delhi High Court *inter alia* on grounds of being beyond the scope of powers of CERT-In under the IT Act, violation of right to privacy of users of VPN and similar services, and violation of right to carry on business of VPN providers.

Considering that several aspects of the Direction remain grey areas today and the points discussed above, MeitY should consider withdrawing the Direction and introducing clear obligations by way of amendments to the existing law.

– Aniruddha Majumdar, Aparna Gaur & Gowree Gokhale

You can direct your queries or comments to the authors

[1] Available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (Last visited on November 11, 2022).

[2] Available at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf (Last visited on November 11, 2022).

[3] Such penalty cannot be imposed through delegated legislation such as Rules or administrative orders such as Direction. The IT Act does not delegate the power to the Central Government or CERT-In to prescribe penalties for non-compliance with such rules or with any directions of CERT-In.

on Simplification of registration for FPIs

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024