CERT-INTY IN VPN REGULATIONS: DEFICIENCIES IN CYBER SECURITY DIRECTIONS OF 28.04.2022

—Devanshi Singh[*]

Abstract—In a country with 692 million active internet users, any legislation impacting its use invites exceptional scrutiny. India purports to be committed to the fundamental rights of its citizens, despite the digital arena being encumbered with regulations and penalties. Virtual Private Networks (hereinafter, 'VPNs') have had a legal footing through the Information Technology Act 2000 so far, permitted in an arena largely without regulations. On 28th April 2022, CERT-In issued the Cyber Security Directions, which require VPNs to maintain personal information of its users and comply with stringent reporting guidelines. The author has examined the legal position of VPNs prior to and post the CERT-In Directions, alongside the effect it would have on companies and consumers.

The issues with implementation, such as ambiguous definitions and subjective criteria, impractical reporting timelines, overbroad data retention period, and lack of personal data protection laws, have been enumerated in the light of other governing authorities, including MeitY and TRAI. The FAQs issued by CERT-In, clarifying the Directions, appear to have become a source of law despite being merely advisory. The author recommends the delegation of VPN log control to users themselves through the establishment of a dashboard. Additionally, it is suggested that storage of PII must be consent-centric, and real-time monitoring may replace onerous compliance burdens. VPNs are an emblematic extension of the freedom of speech and expression, and the author highlights the emphasis on state order instead of a rights-based perspective, comparing and contrasting the same with the approach towards VPNs in other countries and international regimes. A legislation that creates some form of impracticality for every single stakeholder is prima facie flawed; amendments to align the Directions with international democratic standards are the need of the hour.

Keywords: Cyber Security Directions, CERT-In, VPN, Compliance Regime, State Order, Right to Privacy.

[*] Student, National Law Institute University, Bhopal.

INTRODUCTION TO VPNS AND MANNER OF FUNCTIONING

A Virtual Private Network (hereinafter, 'VPN'), in layperson terms, may be considered a system that creates a point-to-point connection across a publicly available network allowing connected devices to transmit and obtain data from the secure private network.[340] It operates upon the underlying public infrastructure of the Internet by encrypting and sending data through tunnelling procedures.[341] A VPN does not provideaccess to the Internet, and as such, cannot be considered an Internet Service Provider (hereinafter, 'ISP'). It merely establishes a private network through the use of an intermediate server, by using parts of publicly available networks. From a commercial perspective, VPN services must meet the international definition given by the International Telecommunication Union (hereinafter, 'ITU') of a 'network-based VPN' as *'that part of a network which provides connectivity amongst a limited and specific subset of the total set of users served by the network provider,'* in order to avail a licence.[342] ITU further defines the specifications to be met by Layers 1, 2, and 3 of VPNs.[343] Of these, only Layer 2 and 3 VPN services (concerning the hardware interface layer and the network layer, respectively) are permitted by the government.[344]

From a legal perspective, VPNs currently fall within the ambit of an 'internet intermediary' as defined by Section 2(w) of the Information Technology Act 2000 (hereinafter, 'IT Act'), within the categories of 'network service providers' and 'web-hosting service providers'.[345] The usage of VPNs generally invites a negative connotation due to the obscurity of activities carried out through them. The individual can access the internet for any activity, even illegal, circumventing the internet censorship put in place by their government. Nevertheless, the primary purpose of VPNs is to augment internet privacy, and protection against marketing agencies, cybercriminals, and government surveillance. Companies use it to share encrypted information remotely, a service that was endorsed by the Indian government itself during the COVID-19 pandemic for Work from Home (hereinafter, 'WFH').[346] Individuals use it to main-

[340] CISCO, 'What is a VPN? - Virtual Private Network' <www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html> accessed 5 June 2022.

[341] US Legal, 'Virtual Private Networks Law and Legal Definition' <https://definitions.uslegal.com/v/virtual-private-networks/> accessed 5 June 2022.

[342] International Telecommunications Union, 'Network-Based VPNs – Generic Architecture and Service Requirements' (March 2002) <www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.1311-200203-I!!PDF-E&type=items> accessed 5 June 2022.

[343] ibid.

[344] MoCIT, 'Guidelines for Permission to Offer Virtual Private Network (VPN) Services by Internet Service Providers (ISPS)' (*Department of Telecommunication,* 16 December 2004) <www.dot.govin/sites/default/files/IP-VPN_Guidelines__web_version_.doc?download=1> accessed 29 January 2023.

[345] Information Technology Act 2000, s 2(w).

[346] Department of Telecommunication, 'Guidelines for Other Service Providers' (5 November 2020) <https://static.pib.govin/WriteReadData/userfiles/OSP%20Guidelines%2005.11.2020.

tain multi-device connections, use public Wi-Fi safely, and bypass restricted networks or geologically-blocked applications. Such activity, if falling within the list of cyber offences in the IT Act, is prohibited and may attract the attention of law enforcement. Even though the police cannot track live, real-time VPN usage, they can obtain traffic logs from the ISP or VPN provider. Access to some content even comprises cognizable offences,[347] and one may be arrested ipso facto for the use of the VPN if the police suspect them of misuse.

Cloud networks store data regarding their usage and related elements through a process known as logging. The logs maintained by a VPN service, if any, depend upon the kind of data they have access to and the extent to which they can track user activity. Almost all free VPNs have in-built tracking and logging source code, but paid VPNs have differentiated levels of security depending upon the subscription and company. Their primary claim is being logless,[348] or no-log VPNs, but to evaluate whether this holds true in actuality, it is important to note the manner of logging. The logs maintained by them may be of three kinds- troubleshooting logs (concerning issues with usage, to improve the efficiency of the VPN), connection logs (storing the length of the user session, and the IP address used), and activity logs (tracking each and every request sent or received over the VPN).[349] The latter two kinds involve Personal Identifiable Information (hereinafter, 'PII'), and breach the purposes of privacy guaranteed by VPNs.[350]

In India, VPN service providers such as NordVPN, SurfShark, ExpressVPN, and ProtonVPN have strict no-log policies,[351] which would now be eroded in the face of directions to maintain extensive logs for a prolonged period of time.

---

pdf> accessed 4 August 2022.

347 Information Technology Act 2000, ss 65, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67C, 70 and 72A; Press Trust of India, 'Non-IPC Offences with up to 3 Years in Jail Cognizable, says Bombay High Court' *(NDTV*, 5 March 2021) <www.ndtvcom/india-news/bombay-high-court-says-non-indian-penal-code-offences-with-up-to-3-years-in-jail-cognizable-2383951> accessed 18 August 2022.

348 Paul Bischoff, 'Best Logless VPNs in 2022' (*Comparitech*, 15 August 2022) <www.comparitech.com/blog/vpn-privacy/best-logless-vpns/> accessed 20 August 2022.

349 Deeba Ahmed, 'What is a VPN and What Does Data Logging by a VPN Mean?' (*Hackread,* 21 April 2022) <www.hackread.com/what-is-vpn-what-is-data-logging-vpn-means/> accessed 16 June 2022.

350 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ('SPDI Rules'), ss 2(i) and 3.

351 Express VPN, 'Express VPN Privacy Policy <www.expressvpn.com/privacy-policy> accessed 14 June 2022; Nord VPN 'No-log VPN Service' <www.nordvpn.com/features/strict-no-logs-policy/> accessed 14 June 2022; Surfshark 'No-logs VPN for Ultimate Digital Privacy' <www.surfshark.com/features/no-logs> accessed 14 June 2022; Andy Yen, 'Proton VPN's No-Log Policy Confirmed by an External Audit' (*Proton VPN,* 13 April 2022) <www.proton-vpn.com/blog/no-logs-audit/> accessed 14 June 2022.

LEGAL POSITION PRIOR TO CERT-IN DIRECTIONS

VPNs are legal in India, with their area of operations limited by the Information Technology Act, 2000. Even so, they have had a large degree of autonomy with regard to how they function and what privacy policies they employ.

The Indian Computer Emergency Response Team (hereinafter, 'CERT-In') has been tasked with issuing guidelines and advisories for internet intermediaries,[352] and is authorised to ask for information or give directions to implement the same.[353] In light of the same, it issued the Cyber Security Directions of 28 April 2022,[354] which are to come into effect from 25th September, deferred from 27th June, the original date of enactment.[355] VPN companies may be called upon at any point to intercept, monitor or decrypt any information relayed over their secure link if the Government deems it necessary to do so.[356]

The necessity of such action is determined when there is an apprehension of a threat to the sovereignty of India or its relations with foreign states, the security and defence of India, or for the investigation of cognizable offences. Further, the IT Act empowers the authorities to collect and oversee traffic data to maintain cyber security.[357] 'Traffic data' in this case refers to data that identifies or possesses the potential to identify the originator or recipient of the transmission and details underlying information such as the time, duration, type, destination, and size, among other elements.[358] While there exist certain exceptions to intermediary liability as opposed to creator liability,[359] they are still expected to comply with geo-blocking directions and disable illegal content if uploaded from India.[360] VPNs had so far circumvented Section 4 of the

---

[352] Information Technology Act 2000, ss 70B and 4(e).

[353] Information Technology Act 2000, s 70B(6).

[354] Indian Computer Emergency Response Team, 'Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents For Safe & Trusted Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022.

[355] Indian Computer Emergency Response Team, 'Extension of Timelines for Enforcement of Cyber Security Directions of 28th April, 2022 Issued Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 For MSMEs and also for Implementation of Mechanism for Validation of Subscribers/Customers Details by Data Centres, VPS Providers, Cloud Service Providers And VPN Service Providers' (*CERT-In*, 27 June 2022) <www.cert-in.org.in/PDF/CERT-In_directions_extension_MSMEs_and_validation_27.06.2022.pdf> accessed 3 September 2022.

[356] Information Technology Act 2000, s 69.

[357] Information Technology Act 2000, s 69B.

[358] Information Technology Act 2000, s 69B(4) expl ii.

[359] Information Technology Act 2000, s 79.

[360] *Swami Ramdev v Facebook Inc* 2019 SCC OnLine Del 10701; Arvind Ravindranath, Aarushi Jain and Gowree Gokhale, 'Court Orders Global Takedown of Content Uploaded From India'

Sensitive Personal Data or Information (hereinafter 'SPDI') Rules regarding the mandate to make policies for privacy and disclosure of information, in that they did not collect any such information at all.[361] If personal or sensitive information were to be stored by such a network provider, they would have been required to obtain prior consent from the individual concerned before sharing it with a third party.[362]

However, the SPDI rules allowed government agencies to circumvent the requirement of consent from VPN users.[363] Prior to the proposed Directions, VPNs had not yet been ordered to collect any specific user data, which is why the SPDI exception has not been a major thorn in VPN privacy protocols.The government had attempted to rein in the autonomous operations of VPNs through the 233rd Rajya Sabha Report presented on 10th August 2021, intended to be not only the first but also the final nail in the coffin of VPN services altogether. Citing the threat of "VPN services and Dark Web that can bypass cyber security walls and allow criminals to remain anonymous online," the Committee recommended to MeitY to permanently block VPN operations in India.[364]

VPNs were described as hotbeds of criminal activity, including hacking, piracy of copyrighted content, sale of drugs and weapons, and human trafficking through the Dark web. While such a ban is technologically possible through Deep Packet Inspection,[365] the actual challenge for the government would have been compliance. Countries like China, which have censored popular websites as well as banned VPNs, have been largely unsuccessful since foreign VPNs are hard for the government to surveil and control.[366]

(*Nishith Desai Associates,* 25 November 2019) <www.nishithdesai.com/SectionCategory/33/Technology-LawAnalysis/12/60/TechnologyLawAnalysis/4454/1.html> accessed 23 June 2022.

361 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ('SPDI Rules'), s 4.

362 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ('SPDI Rules'), s 6(1).

363 ibid.

364 Department-related Parliamentary Standing Committee on Home Affairs, *Action Taken by the Government on the Recommendations/Observations Contained in the 233rd Report on the Atrocities and Crimes Against Women and Children* (Rajya Sabha August 2021 Report No. 233, 2021) para 3.13.6.

365 Marcia Sekhose, 'Who Should Worry about the Proposed VPN Ban in India?' (*Business Insider*, 2 September 2021) <www.businessinsider.in/tech/news/who-should-worry-about-the-proposed-vpn-ban-in-india-and-who-dont/articleshow/85856285.cms> accessed 21 June 2022.

366 Chiara Castro, '7 VPN Trends you may not Know about' (*Techradar,* 7 June 2022) <www.techradar.com/in/news/7-vpn-trends-you-may-not-about> accessed 21 June 2022.

The most effective VPN companies have their servers in countries such as Panama,[367] British Virgin Islands,[368] and Romania, outside of the purview of the Fourteen Eyes agreement.[369] This is why they cannot be regulated by domestic authorities or international intelligence-sharing covenants[370] and would render any ban ineffective. This recommendation was also shelved due to concerns about freedom and accessibility of the internet. Nations that have implemented a full VPN ban are authoritarian or totalitarian regimes, and are generally associated with restrictive regimes for freedom of speech and expression.[371] By contrast, in India, the same is a constitutionally guaranteed right under Article 19(1)(a) alongside unrestricted access to internet services for business and trade purposes.[372]

CONTEMPORARY POSITION OF VPNS: CERT-IN DIRECTIONS

CERT-In introduced new regulations surrounding VPNs on 28 April 2022, which were to take effect two months from the date of the notification.[373] CERT-In is the appointed national agency to coordinate cyber incident response activities, issue advisories, guidelines, or emergency directives, and request information from intermediaries and service providers.[374] As such, it is conferred with complete authority to implement these regulations for VPN companies operating within Indian jurisdiction.

---

[367] NordVPN, 'Where is NordVPN Based?' <https://support.nordvpn.com/General-info/Features/1061811142/Where-is-NordVPN-based.htm> accessed 8 August 2022.

[368] Surfshark, 'Surfshark Terms of Service' <www.surfshark.com/terms-of-service> accessed 8 August 2022; ExpressVPN, 'BVI Jurisdiction: Why it Matters' (28 April 2017) <www.expressvpn.com/blog/bvi-privacy-legislation/> accessed 8 August 2022.

[369] CyberGhost, 'Discover the Best VPN Servers' <www.cyberghostvpn.com/en_US/vpn-server> accessed 8 August 2022.

[370] FIORC, 'Charter of the Five Eyes Intelligence Oversight and Review Council' (*Director of National Intelligence*, 2 October 2017) <www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf> accessed 8 August 2022; Privacy International, 'Eyes Wide Open v 1.0' (*Privacy International*, 26 November 2013) <www.privacyinternational.org/sites/default/files/2018-02/Eyes%20Wide%20Open%20v1.pdf> accessed 9 August 2022.

[371] Dr Keith Goldstein, Dr Ohad Shem Tov and Dan Prazeres, 'The Right to Privacy in the Digital Age' (*OHCHR,* 9 April 2018) <www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf> accessed 19 June 2022.

[372] Constitution of India 1950, art 19(1)(g); *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

[373] Indian Computer Emergency Response Team, 'Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022, 3(v).

[374] Information Technology Act 2000, ss 70B(1), (4), (5) and (6); Information Technology Act 2000, s 87(2)(*zf*); Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.

Clarifications on these Directions were issued by the CERT-In on 18 May 2022 in the form of Frequently Asked Questions (hereinafter, 'FAQs').

The Directions mandate such service providers to record and maintain the usage and access information of their customers for a period of at least five years from when they cancel or withdraw their subscriptions. This includes their name, period of subscription, email, and IP addresses, contact address and number, purpose for subscription, and 'ownership patterns'.[375] They may be required to furnish the same for the government at their command.[376] Intermediaries are also required to maintain logs for a rolling period of 180 days to submit to CERT-In alongside any incident report they order.[377]

Further, 'cybersecurity incidents' must be reported to CERT-In by the companies within six hours of receiving information regarding them. These are defined as 'any real or suspected event[s] in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of services or disruption, information without authorisation, and unauthorised use of a computer resource for processing or storage of information or changes to data.'[378] On the other hand, 'vulnerabilities' need not be reported.[379] Despite the list of reportable incidents as have been specified by CERT-In,[380] broad definitions and subjective criteria create room for ambiguity in the classification of what would constitute a reportable cyber incident.

The ostensible purpose of implementing such regulations is cybersecurity. According to the FAQs, 'technological advancement has opened vulnerabilities by malicious actors' against which the Directions will 'ensure Open, Safe, [and] Trusted and Accountable Internet in the country.'[381]

---

[375] MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*,18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022.

[376] Information Technology Act 2000, s 70B(6).

[377] Indian Computer Emergency Response Team, 'Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022, 3(iv).

[378] Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions And Duties) Rules 2013, s 2(*h*).

[379] Indian Computer Emergency Response Team, 'Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022 2(p).

[380] MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022 Annex I p 16.

[381] MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022.

EFFECT ON VPN COMPANIES AND CONSUMERS

VPNs, being internet proxy services, do not maintain traffic logs of their customers to preserve their anonymity and security. Firstly, the proposed regulations require all VPN companies catering to general internet subscribers to maintain user logs for a period of five years. It fails to establish the need to do so in order to achieve the end of an accountable internet. This is applicable even after the user cancels their subscription or withdraws from the network. However, these Directions do not apply to corporate or enterprise networks.[382] These logs must include *"(a) validated names of subscribers/customers hiring the service, (b) period of hire including dates, (c) IPs allotted to/being used by the members, (d) email address and IP address and time stamp used at the time of registration/onboarding, (e) purpose for hiring services, (f) validated address and phone number, (g) ownership patterns of the subscribers/customers hiring services."*[383]

'Validated' in this case would refer to verified information using some degree of PII from the consumer, eroding the anonymity of a random user session. Even so, the definition of 'ownership patterns'[384] has taken into account the extent to which VPN services can intrude upon user privacy. Rather than the determination of the ownership itself, which may have created an oppressive obligation upon companies, VPNs are only required to maintain key details about the management.

The unique selling point of a VPN is the insurmountable fortress built to protect the privacy and security of the consumer. These very functions are obliterated by the magnitude of data to be stored and the time period of storage. The Directions alongside the IT Actallow the guidelines to have an overriding effect over all contractual obligations that the companies undertake.[385] SPDI rules, if they become applicable, would require these companies to allow consumers to either opt-out from or withdraw sensitive information.[386] However, VPN consumers would not have this option since the collection of

[382] MeitY, 'Frequently Asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022, q 34.

[383] Information Technology Act 2000, p 3(v).

[384] MeitY, 'Frequently Asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*,18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022 q 33.

[385] Information Technology Act 2000, ss 70B and 81; Information Technology Act 2000, ss 70B(1), (4), (5) and (6); Information Technology Act 2000, s 87(2)(zf); Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ; Dr Keith Goldstein, Dr Ohad Shem Tov and Dan Prazeres, 'The Right to Privacy in the Digital Age' (*OHCHR,* 9 April 2018) <www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf> accessed 19 June 2022 q 22.

[386] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ('SPDI Rules'), s 5(7).

the above-mentioned data is already mandated. Therefore, the element of consent at the core of PII collection and processing would be wholly absent.

The right of an individual to privacy also includes the right to control his/her existence on the internet.[387] Even though a consent-centric information system is lacking in the Directions, the consumers have not been granted the right to erasure, or the right to be forgotten, either. It refers to the removal of personal data when such data is no longer required for processing.[388] An arbitrary minimum time period of five years, extendable at the order of CERT-In, has been prescribed,[389] without any justification linking it to illustrated cybersecurity reasons.

Telecom Regulatory Authority of India (hereinafter, 'TRAI') prescribes varying periods of data retention depending upon the nature of the data being collected. Call history is recorded for a period of one year and is erased afterward. Information pertaining to SIM is erased after a lapse of 60 days without usage.[390] ISP License and Unified Access Services License (hereinafter, 'UASL') License prescribe a period of six months for the retention of the audit trail of remote access activities.[391] RBI mandates banks to maintain transactional records for five years, in compliance with anti-money laundering standards.[392] In light of these comparable data retention regulations, the prescribed five-year period has not been satisfactorily rationalised.

Secondly, CERT-In also requires companies to store IT and Communications logs for a rolling period of six months in local servers within Indian territory, which they would be required to furnish in the event of a cybersecurity concern, or at the direction of CERT-In.[393] There is no guideline

---

[387] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

[388] EU General Data Protection Regulation (GDPR) 2016/679, art 17.

[389] Indian Computer Emergency Response Team, 'Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022 (v) p 3.

[390] TRAI, 'Deactivation of SIMs Due to Non-Usage' (28 December 2012) <https://trai.govin/consultation-paper-deactivation-sims-due-non-usage> accessed 13 August 2022.

[391] DoT, 'License Agreement for Provision of Internet Services' (8 April 2016) <www.dot.govin/dataservices/license-agreement-internet-service-including-internet-telephony-amendments> accessed 27 August 2022; DoT, 'License Agreement for Provision of Unified Access Services after Migration from CMTS' (3 December 2009) <www.dot.govin/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1> accessed 27 August 2022.

[392] RBI, 'Master Circular - Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/Combating Financing of Terrorism (CFT)/ Obligations of Banks and Financial Institutions Under PMLA, 2002' (1 July 2015) <https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9848>5(2)(d).

[393] Indian Computer Emergency Response Team, 'Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted

on what would constitute these logs,[394] beyond a non-exhaustive list in the FAQs intended to 'provide flavour of logs to be maintained.' VPN companies based in other countries are compelled to maintain localised records even if they do not have a physical presence in India otherwise. Many VPNs operate with RAM-only servers at present, which delete user data whenever the hard drive is switched off.[395] They cannot practically comply with the Directions without a complete overhaul of their operations.

Thirdly, cybersecurity incidents must be reported within six hours of being brought to notice. Even as the FAQs have expanded the list of such incidents,[396] VPN companies, consumers, and intermediaries would have differing opinions, to begin with, on the manner of occurrence, whether the report needs to constitute sensitive logs, and whether it requires action. No impact threshold has been specified, and successful or unsuccessful security breaches would invite the same action against them. Isolated 'vulnerabilities' do not need to be reported mandatorily.[397] They have been defined as "*flaw[s] or weakness[es] in hardware or software of a computer resource that can be exploited resulting in their adverse or different functioning other than the intended functions.*"[398]

It is unclear why such a distinction has been created, especially when such flaws possess the potential to be leveraged by a threat source to install malware, gain unauthorised access, or collect information.

In addition to this, VPN services are required to designate a Point of Contact (hereinafter, 'POC') to act as an interface through which information would be relayed, and directions would be received from CERT-In.[399] It applies to those companies, too, which cater to Indian customers without a physical

---

Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022.

394 MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022.

395 Michael Kan, 'India Orders VPN Providers to Log and Hand Over Customer Data' (*PCMag*, 3 May 2022) <www.pcmag.com/news/india-orders-vpn-providers-to-log-and-hand-over-customer-data> accessed 3 August 2022; 'SurfShark Upgraded its Infrastructure to 100% RAM-Only Servers' (*SurfShark*, 15 July 2020) <www.surfshark.com/blog/surfshark-upgraded-to-ram-only-servers> accessed 3 August 2022.

396 MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*,18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022 annex I.

397 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, 12(1)(a).

398 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, 2(p).

399 Indian Computer Emergency Response Team, 'Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet 2022 ('Cyber Security Directions')' (*CERT-In*, 28 April 2022) <www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 20 June 2022.

presence in the country.[400] The reporting responsibility cannot be indemnified or transferred by the VPN service provider when various parties are involved. The FAQs estop joint party reporting or contractual delegation of this responsibility, creating difficulties for multinational firms which outsource their operations.[401]

It is alarming that the FAQs seek to legislate at many junctures, rather than staying true to their advisory nature.[402] The burden of compliance is extremely onerous, especially in a regime where the companies are in the dark about directives to fulfil the same. Even so, penalties for circumvention extend to a fine of up to rupees one lakh, or a prison sentence of one year for executives of the firm.[403]

Information Technology Industry Council (hereinafter, 'ITIC'), the global policy organisation for technology, too has raised concerns about the overbroad definition of 'incident' and the impracticality of the reporting timeline, alongside recommendations to modify the same to be at par with global regulations.[404] VPN regulations in India have drawn international attention in light of increasingly divisive government policies and autocratic censorship across countries.

STATE ORDER VERSUS PRIVACY

Restrictions on the free net have been observed as some of the first signs of an autocratic state.[405] The universal value of digital rights is more curtailed, than recognised, by governments across the world for the purported reasons of combating terrorism and maintaining security. India has had a contentious history with mass surveillance and data collection, landing among the top three countries for active government surveillance of citizens.[406]

---

[400] MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022 q 29.

[401] MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022 q 13.

[402] MeitY, 'Frequently asked Questions (FAQs) on Cyber Security Directions of 28.04.2022' (*CERT-In*, 18 May 2022) <https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf> accessed 29 June 2022.

[403] Information Technology Act 2000, s 70B.

[404] ITI, 'ITI Raises Concerns that India's Proposed Cybersecurity Directive Could Undermine Security Goals' (6 May 2022) <www.itic.org/news-events/news-releases/iti-raises-concerns-that-india-s-proposed-cybersecurity-directive-could-undermine-security-goals> accessed 17 July 2022.

[405] Dr Keith Goldstein, Dr Ohad Shem Tov, and Dan Prazeres, 'The Right to Privacy in the Digital Age' (*OHCHR,* 9 April 2018) <www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf> accessed 19 June 2022.

[406] Paul Bischoff, 'Data Privacy Laws & Government Surveillance by Country: Which Countries Best Protect their Citizens?' (*Comparitech,* 15 October 2019) <www.comparitech.com/blog/

A 2021 report by the Pegasus Project[407] exposed a surveillance database of over 300 phone numbers of journalists, politicians, and judicial officers subjected to targeted scrutiny, circumventing procedures of lawful interception.[408] Against this backdrop, the government seeks to restrict and collect data from a service frequently used by journalists and activists to access the internet safely. It even creates scope for unbridled discriminatory surveillance.[409]

In the absence of a personal data protection law, there is a large unregulated area for the policing authorities to operate in, and use the stored data to profile individuals. 'Profiling' refers to the association of characteristics to a person based on their digital footprint. For instance, China has started a 'Police Cloud', which appears capable of tracking social and ethnic communities, leading to disproportionate incarceration of specific social groups.[410] VPNs have more specifically been banned in repressive regimes with ethnic tension, or military conflicts. Geopolitically, the world stands divided: those with access to the free internet, and those digitally isolated.

VPNs are an emblematic extension of the right to freedom of expression on the internet. This is a constitutionally[411] as well as internationally protected right.[412] States have been entrusted with fostering the independence of internet services, in addition to preserving the access of individuals to such services.[413]

In the case of *Faheema Shirin v State of Kerala*, the Kerala High Court acknowledged access to the internet as a fundamental right, which "*comprises part and parcel of day-to-day life.*"[414] Any regulations thus imposed would have to meet the test of necessity and proportionality, in pursuance of a legitimate aim, and cannot go beyond the grounds of reasonable restrictions in Article 19(2) of the Constitution.[415] In *Shreya Singhal v Union of India*, the

---

vpn-privacy/surveillance-states/> accessed 28 June 2022.

407 'The Pegasus Project' (*OCCRP,* 18 July 2021) <www.occrp.org/en/the-pegasus-project/> accessed 8 August 2022; 'Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally' (*Amnesty International,* 19 July 2021) <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/> accessed 8 August 2022.

408 Information Technology Act 2000, s 2(w).

409 Dr Keith Goldstein, Dr Ohad Shem Tov, and Dan Prazeres, 'The Right to Privacy in the Digital Age' (*OHCHR,* 9 April 2018) <www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf> accessed 19 June 2022.

410 Human Rights Watch, 'China: Police 'Big Data' Systems Violate Privacy, Target Dissent' (19 November 2017) <www.hrw.org/news/2017/11/19/china-police-big-data-systems- violate-privacy-target-dissent> accessed 27 June 2022.

411 Constitution of India 1950, art 21; *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

412 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force on 23 March 1976) 999 UNTS 171 (ICCPR) art 19; UNHRC 'General Comment 34' (GC 34) (12 September 2011) UN Doc CCPR/C/GC/34 [12], [15] and [43].

413 UNHRC 'General Comment 34' (GC 34) (12 September 2011) UN Doc CCPR/C/GC/34 [15].

414 *Faheema Shirin R K v State of Kerala* 2019 SCC OnLine Ker 2976.

415 Constitution of India 1950, art 19(2).

Supreme Court has held that a proximate relation to public order or damage to reputation must be thoroughly established to restrict expression on the Internet. Further, the nature of the internet itself renders it all the more important for the legislation to be the least restrictive possible.[416] In *Anuradha Bhasin v Union of India,* the Supreme Court has decreed that the *"degree of restriction and the scope of the same, both territorially and temporally, must stand in relation to what is actually necessary to combat an emergent situation."*[417]

The Directions also eclipse the right to privacy, guaranteed by the ICCPR and Article 21 of the Indian Constitution. The state has a positive obligation to protect the privacy of its citizens,[418] especially when India remains lacking in any form of data protection laws. In the *Puttaswamy judgment,* privacy has been interpreted as a fundamental right, comprising the right to anonymity, the right against biometric coercion, the right to be forgotten, and the right against the collection of data.[419] An individual is entitled to control their existence on the online platform and call for the erasure of data concerning them. The new Regulations prove to be an abuse of the fundamental right of privacy through the collection of profiling information which may be accessed by the government at any point with no transparent basis. As such, CERT-In becomes the custodian of citizen data, ready to strike the hammer at the whims of the government.

INTERNATIONAL APPROACH TO VPN REGULATION

The most repressive VPN restrictions are seen in autocratic nations such as North Korea,[420] Iraq[421] and Belarus,[422] which impose a blanket ban on their use. China boasts of a 'Great Firewall' preventing access to common websites such as Google and Facebook, and VPN services face the threat of revocation of business licences and a fine of up to 50,000 Yuan, alongside impris-

---

[416] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637 [53], [55].

[417] ibid 71.

[418] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force on 23 March 1976) 999 UNTS 171 (ICCPR) art 2.

[419] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1; Sohini Chatterjee, 'In India's Right to Privacy, a Glimpse of a Right to be Forgotten' (*The Wire*, 28 August 2017) <www.thewire.in/law/right-to-privacy-a-glimpse-of-a-right-to-be-forgotten> accessed 25 August 2022.

[420] Max Fisher, 'Yes, North Korea has the Internet. Here's What it Looks Like.' (*Vox,* 19 March 2015) <www.vox.com/2014/12/22/7435625/north-korea-internet> accessed 19 July 2022; Amiee O' Driscell, 'Where Are VPNs Legal and Where are they Banned?' (*Comparitech,* 23 November 2021) <www.comparitech.com/vpn/where-are-vpns-legal-banned/> accessed 19 July 2022.

[421] Timothy Shim, 'Are VPNs Legal? 10 Countries Ban the Usage of VPN' (*Web Hosting Secret Revealed*, March 15 2019) <www.webhostingsecretrevealed.net/ar/blog/security/are-vpns-legal/> accessed 19 July 2022; (*Freedom House*) <www.freedomhouse.org/country/iraq/freedom-net/2021#footnote7_78l6fb8> accessed 19 July 2022.

[422] Tetyana Lokot, 'Belarus Bans Tor and Other Anonymizers' (*Global Voices*, 25 February 2015) <www.advox.globalvoices.org/2015/02/25/belarus-bans-tor-and-other-anonymizers/> accessed 17 July 2022.

onment for up to seven years.[423] In UAE, the use of unauthorised VPNs, even for Voice over Internet Protocol, attracts imprisonment and a fine of Dh 500,000-Dh 2,000,000.[424] However, the government specifies that using VPNs is not outlawed as long as it is for a lawful purpose. This raises two alarming questions about what would constitute a digital crime in UAE, and what the extent of government surveillance would be to monitor activities carried out through VPNs. So even if it can be argued that VPNs are not technically banned, the right to privacy is completely repudiated. In Russia, VPN companies are expected to coordinate with the national database of blocked websites, Roskomnadzor, and assist the government as and when required to clamp down on politically sensitive content.[425]

India's form of restriction may be considered the closest to Oman, where VPN services are allowed as long as they collect and furnish activity logs to the Sultanate.[426] It must be noted that Oman does not hold a candle to India's democratic nature, given that the former is a theocratic state with a strong emphasis on moral and political policing. Even so, many of the world's leading democracies, including the US, UK, Canada, France, and Germany, are part of intelligence-sharing alliances, such as the Five Eyes and the Fourteen Eyes which allow cross-country surveillance.[427] A VPN company based in, or having its servers in any of the alliance countries can be mandated to provide activity logs to the government at any time, which could, in turn, be accessed by any other nation in the alliance. Therefore, democratic nations, too fall short of protecting their citizens' rights; however, instead of simple curtailment, they take a step further to actively violate it by enabling the creation of a global surveillance network.

The General Data Protection Regime (hereinafter, 'GDPR') for Europe has a strong emphasis on user privacy, where individuals can opt out of sharing PII, and need to give consent if companies propose to share their data with a third party.[428] Further, users have access to view, edit and delete any of their personal data that the VPN has stored, affirming the right to erasure and privacy.[429] Thus, citizens of GDPR countries can remain anonymous even with logging policies as long as they are alert about the information they are sharing.

---

[423] Coco Feng, 'China's VPN Providers Face Harsher Punishment for Scaling the Great Firewall under New Data Regulation' *South China Morning Post* (15 November 2021) <www.scmp.com/tech/policy/article/3156095/chinas-vpn-providers-face-harsher-punishment-scaling-great-firewall> accessed 17 July 2022.

[424] Cyber Crimes Law 2012, art 1.

[425] Ksenia Idrisova, 'Explainer: What is Russia's New VPN Law all about?' (*BBC*, 1 November 2017) <www.bbc.com/news/technology-41829726> accessed 17 July 2022.

[426] Jack Wherry, 'Are VPNs Legal?' (*Cybernews*, 14 June 2022) <www.cybernews.com/what-is-vpn/are-vpns-legal/> accessed 17 July 2022.

[427] FIORC, 'Charter of the Five Eyes Intelligence Oversight and Review Council' (2 October 2017); Privacy International, 'Eyes Wide Open' (26 November 2013) v 1.0.

[428] Anas Baig, 'What GDPR Means for VPN Providers (and Users)' (*Global Sign,* 8 June 2018) <www.globalsign.com/en/blog/what-gdpr-means-for-vpn-providers-and-users> accessed 29 June 2022.

[429] ibid; EU General Data Protection Regulation (GDPR) 2016/679, arts 51 and 59.

India does not have data retention laws or personal data protection legislation. This exacerbates the overreach of the Directions.

THE WAY FORWARD: SUGGESTIONS

It is the view of the author that the regulations would be more effective within constitutional bounds if the users had control over the logs maintained by VPN service providers. If the collection of logs is absolutely necessary, a more realistic timeline may be proposed for immediate utility. VPN companies may be required to maintain a dashboard of the information they are recording, alongside detailed scope of where this data would be utilised or sent to. The GDPR even allows the users to edit or delete this data. This would enable end-to-end visibility of privacy settings and their control. Instead of focusing on a restriction and punishment-based approach to VPN usage, India should direct its efforts to an awareness and transparency-based outlook. The dashboard may apprise users of what would constitute a digital crime with adequate information and penalties, similar to compliance actions in GDPR regimes.

Explicit consent must be obtained from the user for accessing and storing PII, and they must be notified when their data is shared with third parties. The provision for storing activity logs may be replaced with real-time monitoring of users accessing prohibited websites promoting criminal activities. A tiered list for such crimes may be created, ranging from those which require immediate action on the part of the VPN companies, to those which require further monitoring. The reporting criteria must be adequately defined with illustrations, and the timeline for reportage must be extended to at least 24 hours for investigation and collection of data, as is the case with police complaints.

Designating a Point of Contact in India or localising servers would prove to be difficult for companies that do not have a physical presence in the country, and the government may instead ask these companies to create direct communication channels from the country it is based. If not, joint reporting must be permitted whereby the responsibility may be shared by the multiple intermediaries involved. CERT-In must specify the circumstances under which it is permitted to ask for any user data and establish a clear and rational nexus to the crime sought to be prevented.

At the very least, the discussion period can be extended, and opinions invited from a more diverse group in order to strike the right balance between state order and privacy. This may include major VPN companies, users, non-profit organisations, and international technology associations alongside government agencies. As it stands, several VPN services may have to pull their services out of India[430] simply because the compliance burden is not feasible.

[430] Subhrojit Mallick, 'NordVPN to shut VPN Servers in India from June 26' *The Economic Times* (14 June 2022) <www.economictimes.indiatimes.com/news/india/

This would deprive citizens of the net neutrality created by VPNs and violate their right to privacy and free access to internet services. The government must prioritise the enactment of the data protection legislative regimes, especially in light of the withdrawal of the Personal Data Protection Bill, 2019.[431]

CONCLUSION

In a world increasingly concerned with data privacy and security, VPNs provide a failsafe. Data not stored cannot be leaked. Nevertheless, the author is aware of the sheer scale on which such networks may still be used for mala fide purposes. To counter this, real-time monitoring has been proposed with a tiered list of offences. An outright ban on access to certain websites, even though VPNs would put India in the same category as China, and as a champion of democratic rights, it cannot take a step so backward.

The Directions propose a strict-compliance regime for VPNs, violating which would make them liable to be banned. They must meet invasive logging standards, unreasonably short timelines for reporting, and other compliance requirements in the light of arbitrarily defined criteria and guidelines. Though the deadline to meet such requirements of the Directions has been extended by three months, to become effective from 25th September 2022, they are themselves are in excess of the IT Act and the CERT-In Rules. Adherence is almost impossible without compromising the privacy of citizens and the security guaranteed by VPN services. The punitive measures proposed[432] are harsh for ambiguous and impractical requirements in the first place.

In a country with 348.7 million VPN users,[433] the government certainly has not taken into account the needs and perspectives of all stakeholders affected by such regulations. Regulations surrounding cybercrime have attracted several controversies over the years, and India needs to find a way to overcome its autocratic image in the digital world.

---

nordvpn-to-shut-vpn-servers-in-india-from-june-26/articleshow/92211097.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> accessed 19 August 2022; Regina Mihindukulasuriya, 'Netherlands VPN Provider Latest to Quit India after Modi Govt's Directions to Share User Data' (*The Print*, 8 June 2022) <www.theprint.in/india/netherlands-vpn-provider-latest-to-quit-india-after-modi-govts-directions-to-share-user-data/988293/> accessed 19 August 2022.

431 Personal Data Protection Bill 2019 [373]; 'Govt Withdraws Data Protection Bill, 2021, Will Present New Legislation' Business Standard, (3 August 2022) <www.business-standard.com/article/economy-policy/centre-withdraws-personal-data-protection-bill-2019-to-present-new-bill-122080301226_1.html#:~:text=The%20PDP%20bill%20was%20first,personal%20and%20non%2Dpersonal%20datasets> accessed 19 August 2022.

432 Information Technology Act 2000, s 70B (7).

433 Sindhu Hariharan, 'VPN Use in India Grows Over 600% in H121' *The Times of India* (18 August 2021) <www.timesofindia.indiatimes.com/business/india-business/vpn-use-in-india-grows-over-600-in-h121-report/articleshow/85412089.cms> accessed 18 July 2022.