CYBERCRIME / CYBER SECURITY LAWS FOR INDIA – A COMPLETE OVERHAUL OR REVISITING EXISTING LEGAL FRAMEWORK©*

October 2020

AUTHORED BY

Ms. N. S. NAPPINAI

Advocate, Supreme Court of India

Founder, Cyber Saathi Foundation

&

Author "Technology Laws Decoded"

Supreme Court Chambers: *J10, B. K. Dutt Colony, Jor Bagh, New Delhi 110 003;*
Bombay High Court Chambers: *No.111, 1st Floor, New Bake House No.12, Maharashtra Chamber of Commerce Lane, Fort, Mumbai 400 023*
Off: (+91) (22) 22021254; Mob (+91) 9820069014;
e-mail: nappinai@nappinai.com; nappinai@gmail.com;

CYBERCRIME / CYBER SECURITY LAWS FOR INDIA – A COMPLETE OVERHAUL OR REVISITING EXISTING LEGAL FRAMEWORK ©

- **N. S. NAPPINAI**[1]

"An *'ephemeral' measure*
to meet a perennial menace
is neither a logical step
nor national fulfilment."(Justice Krishna Iyer (1979)[2])

India is on the cusp of evaluating two critical legal frameworks – Criminal Law Reforms and review or revamp of its Information Technology / Cyber Laws. This review also necessarily requires a decision on whether India could resort to yet another 'band-aid' remedy of revamping existing legal frameworks or overhauling its entire cyber law ecosystem to provide future-ready laws to combat the challenges of the cyber domain *(Nappinai. N. S. (2017))*[3].

This paper analyses in brief, the issues and concerns permeating the present legal framework for cyber and espouses the need for new laws for cybercrimes and cybersecurity. The placatory mode of adaptation of

[1] N. S. Nappinai is an Advocate of Supreme Court and is the Founder – Cyber Saathi Foundation ("CSF"). CSF *inter alia* undertakes policy research and submissions and the present paper is a first in the series on India's law and policies for the Cyber domain. Ms. N. S. Nappinai is *Amicus Curiae In Re: Prajwala Letter dated 18.2.2015. Videos Of Sexual Violence And Recommendations*" (*(2018) 15 SCC 551*). She has contributed extensively on Government Committees *inter alia* on proposed amendments to the Information Technology Act, 2000 (as amended) and Electronic Evidence laws;

[2] Refer: Chapter 2, Page 289. Nappinai. N. S. (2017). *"Technology Laws Decoded"*. LexisNexis for the relevance of the above quote of Justice V. R. Krishna Iyer, In Re The Special Courts Bill v. Unknown, (AIR 1979 SC 478 : (1979) 1 SCC 380 : (1979) 2 SCR 476.) to the need for a complete overhaul of existing legal framework for the cyber domain;

[3] Nappinai. N. S. (2017). *"Technology Laws Decoded"*. LexisNexis;

Model laws, as India's legal framework and its fleshing out thereafter have all been reactive responses to immediate requirements.

The Indian narrative has however changed substantially and so have global trends. With India's 'Digital India' thrust; its better understanding of cyber threats and its impact; the need for national security from cyber warfare / information warfare; better laws and enforcement from economic cyber offences and the primary focus – of individual safety and the need for speedy remedies, are just some of the reasons for India to evaluate a fresh and separate legislation for Cyber security.

Online platforms, chat apps and content hosting platforms have amplified the threat scenario. Enhanced threats abound in the form of fake news and hate speech, that cause grave harms, including loss of life, violent attacks on individuals, particularly women and children, toxicity and manipulation of news that threaten national security and interests[4]. The need for reviewing hate crime provisions to evaluate the inclusion of other categories such as 'gender' and 'disability' were raised by the Law Commission in its Hate Speech Report of 2017[5]. These have become imperatives in the light of progressively violent acts on social media platforms affecting women and children[6] and toxicity on social media platforms and the increased threat to democratic processes through the wilful and malicious spreading of fake news online.

All of the above buttress the need for India to not merely review and modify existing legal frameworks but evaluate formulation of laws specifically addressing Cyber Security concerns. The purpose and impact

[4] Refer: EU Parliament's 2018 Study on *'Cyber violence and hate speech online against women'* (https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf);
[5] http://lawcommissionofindia.nic.in/reports/Report267.pdf;
[6] Refer: *In Re: Prajwala Letter dated 18.2.2015. Videos Of Sexual Violence And Recommendations*" (*(2018) 15 SCC 551*);

of effective laws are best encapsulated by Bleich, Erik. (2011)[7]: "*Legislation has a strong declarative effect when it is enacted: in these cases, it asserts that certain expressions are deemed unacceptable by the country as a whole and reassures vulnerable groups that their interests and identities are considered worthy of national acknowledgement.*" Whilst Bleich (Supra) refers to legislations for hate crimes, the conviction of the above elucidation applies equally to the need for effective legislations to combat cyber security threats, which would meet the fundamental principles of clarity, certainty and efficacy needed for Criminal law enforcement.

That a separate legislation would be the best step forward for India is also supported through global trends. Most jurisdictions have opted for such independent legislations, to combat cyber threats and vulnerabilities.

India requires a legal framework that will address not just existing threats and vulnerabilities but a dynamic legislation that will withstand the test of time against technology mediated crimes impacting individuals, businesses and national security. Whilst doing so, India would have to review substantive and procedural laws, with the latter including a complete revamp of laws pertaining to electronic evidence and jurisdiction in cyberspace.

With emerging technologies already posing new challenges and threats even to the very fabric of a democracy, an overhaul of substantive laws would have to encompass *inter alia,* effective and enforceable laws to combat crimes; precise and explicit provisions for Intermediary liability, safe harbour / exemptions and mandatory compliances; evaluate laws to criminalize abuse of emerging technologies; and international enforcement mechanisms that will overcome the limitations that

[7] Bleich, Erik. 2011. "The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies." Journal of Ethnic and Migration Studies 37(6):917–934.

sovereign rights and territoriality pose whilst regulating cyber domains. These again would have to cover aspects of data sharing, cooperation between law enforcement agencies, drawing clear lines of sovereignty, be it over data or applicability of municipal laws to foreign nationals; recording of evidence and reliance thereof across borders and expedited processes for extradition. Laws have to be formulated keeping in mind the gravity of the offences. For instance, whilst existing laws may be applied across varying degrees of offences from cybercrimes to acts of terrorism or warfare, neither are the punishments structured to deter or even commensurately punish.

Finally, over the last few years India has expressed interest in revisiting its decision on adapting the Convention on Cybercrime (or the Budapest Convention)[8]. The need for international cooperation, especially to facilitate investigations into cross border crimes and harmonising laws for cyber to enable better enforcement are just some reasons to revisit India's earlier decision. Options that are open presently are acceptance or adaptation of the existing soft law, as above or for India to drive policy frameworks through integration of the intersections between the Budapest Convention, which is by far the one that most Countries have adapted, and the other Resolutions proposed and having partial regional adaptation. Either way, that there is a need to review and adapt / formulate and propose, international cooperation treaties for enforcement against cyber threats is critical.

Cyber warfare was first addressed by the Tallinn Manual (2013)[9], as a form of Cyberattack '*designed to further sovereign interests by compromising the network systems of another nation'*. Libicki. M.

[8] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185;
[9] The 'Tallinn Manual on the International Law Applicable to Cyber Warfare' was a non-binding collaborative opinion document of NATO Cooperative Cyber Defence Centre of Excellence and published by Cambridge University Press in 2013; The Tallinn Manual 2.0 version ("Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations") was published in 2017 (https://ccdcoe.org/research/tallinn-manual/);

(1995)[10] distinguishes this from "Information Warfare" or "Info war" as '*the technology enabled possibility of manipulating information entrusted by individuals to engineer their decisions or thoughts to align with that of the propagator of such act or to promote the interests that the perpetrator of such acts intends'.*

India has and continues to face the larger threat of cyber warfare and that of 'Information warfare'. Reports indicate widespread attack on Government networks from neighbouring Nations including China[11]. Whilst Healthcare and Academia have been the most recent targets of attacks reportedly emanating from China and Pakistan[12], the potential of these persistent attacks and their impact on National Security, through cyber warfare and to India's democratic structure through 'Information Warfare' are already prevailing and pervasive.

The present legal framework for combating cyber threats despite the refurbishing through the amendments of 2008 are woefully inadequate to meet or combat these existing and emerging threats. A robust cyber security legal framework is the need of the hour to equip India with the legal arsenal required to meet the challenges of the cyber domain.

Information Technology Act, 2000

It is now twenty years since India got its first codified laws for the cyber domain, the Information Technology Act, 2000 (as amended) (**"2000 Act"**). Whilst this enactment does not encompass all of India's cyber laws, as even this very law brought in amendments *inter alia* to Indian Penal Code, 1860 ("**IPC**") and the Indian Evidence Act, 1872, it was still

[10] (Libicki. M. 1995). Libicki, Martin (1995), *What Is Information Warfare*? ACIS Paper 3, Washington, DC: National Defense University;
[11] https://www.oneindia.com/international/us-looks-out-for-5-super-hackers-from-china-who-attacked-indian-govt-websites-3150719.html;
[12] https://economictimes.indiatimes.com/tech/internet/india-facing-more-cyber-attacks-from-china-and-pakistan-since-nationwide-lockdown/articleshow/76962155.cms?from=mdr;

a first step for a special law to deal with the complexities that the cyber domain brought with it.

With the UNCITRAL[13] Model Law on Electronic Commerce being adapted by the General Assembly of the United Nations on January 30, 1997, and the same requiring signatory Nations to consider the Model Law favourably to harmonise laws pertaining to e-commerce India passed the IT Act of 2000. The stark silence about cybercrimes in its original 'Statement of Objects & Reasons' for the enactment is reflective of its intent and purpose.

Whilst the focus of the IT Act of 2000 was primarily on e-commerce, salutary provisions for cybercrime did find their way into the legislation and also through amendments to IPC. Barely about ten provisions were introduced to combat cybercrimes (Chapter XI comprising Sections 65 to 78 IT Act). Of these only about 4 provisions provided for substantive offences. Cyber-attacks ravaging businesses and impacting national security such as hacking, virus attacks, denial of service attacks and data theft were relegated to civil violations under S.43 of the IT Act. These loopholes were bridged to some extent by the 2008 amendments to the IT Act, as set out hereunder.

Information Technology Act, 2000 - 2008 Amendments

Immediately after the horrific terror attacks in Mumbai in 2008, wherein technology played a key role to facilitate and intensify the magnitude of the attack, the urgent need for incorporating suitable cyber security provisions, especially those pertaining to cyber terrorism was felt. Consequently, in December 2008, the Information Technology Act, 2000 was amended (**"IT Act**"). Some highlights of the IT Act, post the 2008 amendments:

[13] United Nations Commission on International Trade Law;

- Several substantive criminal provisions were introduced, including for combating and prosecuting cyber terrorism; child pornography; sexually explicit content; privacy violation; data protection, identity theft; cheating by personation; and disseminating of offensive content. All the violations under Section 43 of the 2000 Act, including hacking, data theft, virus attacks, denial of service attacks amongst others were also made criminal offences;
- Other significant additions were on data protection and revisions to Intermediary liability;
- The restrictive use of technology and domain to which the enactment applied to i.e., "digital" was replaced with the more open-ended "electronic". This enabled applying the provisions to a wider array of technology;
- Provisions were added for the creation of two very important Government agencies:
    - The National Critical Information Infrastructure Protection Centre (**"NCIIPC"**) was appointed as the nodal agency in respect of Critical Information Infrastructure;
    - The Indian Computer Emergency Response Team (**"CERT-IN"**) was appointed to serve as India's national agency for incident response;

The above are merely illustrative additions through the 2008 amendments to the IT Act.

Immediate Concerns over the IT Act Amendments

The draft presented in the backdrop of the horrific terror attack we through without any debate and several loosely worded provisions found its way into the legislation (Nappinai N. S. (2017)[14]). A few illustrations:

[14] Refer for detailed analysis: Nappinai N. S. (2017). '*Technology Laws Decoded*'. LexisNexis.

- Provisions such as the ambiguous Section 66A IT Act were clearly inviting judicial review even without the rampant abuse, that resulted in its strike down;
- Inclusion of Hate Speech provisions was suggested under the Law Commission Report of 2017. These still remain to be implemented. Meanwhile there has been exponential growth in hate speech crimes affecting individuals to national security;
- Meanwhile fake news concerns have reared their head through methodologies that threaten the very fabric of a democracy. For instance, in April 2020, CNN did an expose of Russian Troll farms in Ghana & Nigeria, which they apprehended were intended to tamper with US elections[15]. There is no reason to believe India would not be a target of such or similar fake news propaganda intended to *'manipulate information to engineer decisions'* or use of 'information warfare' as defined herein above. Existing provisions do not provide redress for such harms that affect national security;
- Section 66 under the old IT Act of 2000 had faced extensive criticism for the ambiguities in drafting and proposals for its amendments were circulated in 2006 for public consultations and views expressed were almost unanimous for its deletion. Yet, it was merely transposed to Section 43 and was read into the new section 66;
- Further additions made in Section 43 seem tautologous considering the retention of Section 65, as is;
- Whilst provisions for cyber terrorism were added, they still require a review given its open-ended wording, particularly of Section 66F(b)IT Act;
- Reliance on electronic records was the very foundation for the passing of the 2000 Act. Yet the additions to the Indian Evidence Act, 1872 have merely complicated the very process that it intended

[15] https://edition.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html;

to facilitate. Despite the 2008 amendment process offering an opportunity to review these additions, the same was not undertaken;

- Jurisdictional issues need harmonizing across Nations considering the seamless execution of criminal activities on cyber domains. However, India's Cyber laws spread across special and general enactments have not harmonized provisions even between municipal laws[16]. These require immediate attention.

Supreme Court Decisions & Their Impact

From or about 2014, several case laws have emerged from the Supreme Court and several High Courts, impacting the IT Act as well as general laws such as the Indian Evidence Act, 1872. Significant amongst these are the following:

- The decision of the Supreme Court in *Shreya Singhal v. UOI*[17] , which struck down Section 66A IT Act dealing *inter alia* with dissemination of offensive content through electronic means*;*
- *Shreya Singhal* dealt with Section 66A IT Act in the face of rampant abuse of the said provision[18]. Even without the trigger of abuse prompting its strike down, the very drafting of the provision with its ambiguities was a powder keg awaiting the spark from the proverbial judicial gavel to strike it down. This decision however neither addressed nor dealt with the vicious crimes of cyber bullying, stalking or revenge porn and other heinous offences trending online. It was not called upon to review these in any event. With the awareness borne out of innumerable studies and the increasing toxicity of online and content hosting platforms and chat

[16] Refer: Chapter 6: 'Jurisdiction in Cyberspace'. Nappinai. N. S. (2017) 'Technology Laws Decoded'. LexisNexis.
[17] (2015) (5) SCC 1;
[18] Refer Chapter 2. Technology Laws Decoded. Nappinai N. S. (2017) (Supra);

apps, it has become imperative to review this provision and to formulate a sustainable and constitutional equivalent;

- Hate speech and fake news issues abound, as set out above. All of these also could have been substantially combatted using Section 66A IT Act. Again, these were neither the issue nor points for consideration before the Supreme Court in the above decision and again, the very structuring of the struck down provision did not validate its continuation despite such serious crimes requiring to be addressed specifically. The need for a comprehensive Cyber Security law is further buttressed with the exigencies that these crimes bring forth;
- The Supreme Court took *suo motu* cognizance of the increasingly menacing and depraved offences such as child pornography and rape and gang rape videos being uploaded online, in *Re: Prajwala Letter Dated 18.2.2015. Violent Videos & Recommendations*[19]. The suggestion for use of Artificial Intelligence tools to combat crime was put forth to evaluate 'active filtration' of such criminal content. This remains to be decided by the Supreme Court. However on October 23, 2017, the Supreme Court passed an order directing implementation of the consensus proposals put forth by the Government Committee appointed by the Supreme Court. One of the proposals that became an order of Court was for commencement of research to develop AI tools. In the three years since, there has been substantial developments particularly of use of AI enabled tools to identify hate speech / fake news. It is imperative to evaluate the proposals, that emanated from this decision of the Supreme Court for regulating technology companies (including content hosting platforms, search engines and chat apps);
- Whilst *Prajwala* (Supra) evaluated AI for pre-emptive filtration and 'unblocking' of content isolated to balance victim rights with free

[19] *(2018) 15 SCC 551;*

speech, *Sabu Mathew George v. Union of India*[20] dealt with auto-blocking of search parameters. There is a lot of resistance from Intermediaries for each of these preventive or pre-emptive measures, as they apprehend dilution of their safe harbour exemptions that are predicated on absence of control or content moderation. It is important to lay down specific laws and rules to enable clarity and certainty on Intermediary liability and responsibility to enable effective enforcement and to ensure certainty of action by such Intermediaries;

- In *Internet And Mobile Association Of India v. Reserve Bank of India*[21] the Supreme Court decided the *vires* of the Reserve Bank of India's Circular on Cryptocurrencies. The decision that substantially rejected all of the Petitioner's contentions struck down the RBI Circular on the basis of proportionality or lack thereof. *Per se,* the decision appears to lack tenability considering that on one hand it categorically reaffirms the settled law that corporations cannot sustain their claims on the basis of Article 19 (and any of the fundamental rights comprised therein), directly or indirectly, and on the other supports its final conclusion of disproportionality on the basis of the corporate outcomes from RBI's circular. The same however has not been contested still by RBI. With India deciding on review of its cyber laws, a definitive decision on legality or otherwise of cryptocurrencies given the interest and involvement of young India would be a welcome addition. Further there is also need for delineating Blockchain, from cryptocurrencies and evolving laws and regulations to enable this technology. Law can and ought to enable innovation and is an imperative for emerging technologies. India's policy statements categorically identify the business potential of emerging technologies such as AI and Internet

[20] (2015) 11 SCC 545;
[21] *IAMAI v. RBI: Writ Petition (Civil) No.528 of 2018)(SC): DOJ: March 4, 2020 (https://main.sci.gov.in/supremecourt/2018/19230/19230_2018_4_1501_21151_Judgement_04-Mar-2020.pdf)*

of Things, to name a few but fails to address the need for law, as an enabler. It is imperative that these white spaces in law be addressed to ensure effective support for innovation and to ensure that India lives up to its potential to emerge as a dominant player;

- Supreme Court's decision in *Sharat Babu Digumarti Vs. State, Govt. of NCT of Delhi*[22] has been further interpreted by the Bombay High Court to exclude general laws for cybercrimes. The issues that have arisen due to this include the absence of clarity with respect to the exact scope and extent of exclusion that the special laws carve out, which has to now be resolved through precise legislation;
- ***Electronic Evidence & the Supreme Court's Decisions:*** Sections 65A & 65B Indian Evidence Act, 1872 are a veritable quagmire[23]. The provisions probably intended to facilitate reliance on electronic records were first interpreted by the Supreme Court in *State (N. C. T. of Delhi) Vs. Navjot Sandhu*[24], which in effect held them to be discretionary. In *Anvar V. Basheer*[25], a three-judge bench overrules *Navjot Sandhu's* decision. The decision in *Anvar (supra)* was recently upheld by the Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[26], by another three-judge bench. These decisions on Sections 65A & 65B point to the complexities involved in practical application of these provisions, which were also tainted with the focus on e-commerce and which consequently imposed conditions, that are impractical. The *Arjun Panditrao* (supra) decision of the Supreme Court has in effect taken away the little benefit that these provisions were probably intended to provide for easy reliance on electronic records and place a more

[22] 2015 SCC OnLine Del 11591;
[23] Nappinai. N. S. (2019). "Electronic Evidence - The Great Indian Quagmire". (2019) 3 SCC J-41. Also See Chapter 5. Nappinai N. S. (2017). Technology Laws Decoded. LexisNexis; & Nappinai. N. S. (2020). 'From Anvar to Arjun – A Tale of Two Any's'. livelaw.in (https://www.livelaw.in/columns/from-anvar-to-arjun-a-tale-of-two-anys-other-stories-157264)
[24] AIR 2005 SC 382: 2005 AIR SCW 4148;
[25] 2014 (10) SCC 473;
[26] *(2020) SCC OnLine SC 571;*

cumbersome burden on parties intending to rely on copies of electronic records, beyond what the provisions themselves appear to set out. This decision itself points to the need for legislature to review these provisions and to evaluate amendments thereto. The exercise that is undertaken for review and revamp of cyber laws would require to take into account the necessities for easy reliance on electronic records keeping in mind global trends in laws and the legal framework in India;

- Further, the historic 9-judge decision in *Justice K. S. Puttaswamy v. Union of India (2017 (10) SCC1)* (the privacy judgment) has mandated the need to enact a much-needed separate personal data protection legislation for India. With the draft Bill now before India's Parliament, the much-awaited personal data protection legislation will soon become law. This will result in amendments to the IT Act and repeal of the Rules made with respect to data protection.

Need to Review / Replace Existing Laws For Cyber Security

Additions of the above provisions was expected to improve cyber enforcement and to make the cyber domain a safer place. Inclusions such as Section 67B IT Act to combat the heinous crime of child pornography, which is one of the most stringent provisions across the world ought to have deterred the crime substantially.

This is not the reality, as was demonstrated by the incident reports from India shared by NCMEC, USA, with which the Government of India entered into a Memorandum of Understanding, pursuant to the order of the Supreme Court in *Re: Prajwala Letter Dated 18.2.2015. Violent Videos & Recommendations*[27] and the prosecutions that have been launched against paedophiles thereafter.

[27] *(2018) 15 SCC 551;*

Significant increase in cybercrimes during the recent Corona Virus ('COVID19') pandemic and in particular of sharing of child sexual abuse content was testimony to the hardships faced by law enforcement to combat these and other increasing threats to cyber security and safety on digital domains.

Be it with respect to dissemination of child sexual abuse content or offences against women; or the increasing threat to businesses despite introduction of offences such as data theft as a specific offence; or the offences and threats of cyber terrorism and veritable cyber warfare being perpetuated persistently against India, the existing legal frameworks have proven ineffective and insufficient to combat increasingly potent threats and vulnerabilities to cyber security.

Despite two powerful Government agencies being inducted through the 2008 IT Act, it is only in recent times that business have even responded with seriousness to cyber security incident reporting to CERT-IN. Protections and protocols for securing critical infrastructure, as a national security threat are still nascent.

Law Enforcement Agencies have faced persistent resistance to data sharing and cooperation in investigations from Intermediaries. Whilst these situations have improved (one of the Chief Investigators played a key role in both the *Prajwala* matter above and also in bringing about clarity through her advice and engagement, on Intermediary rights and liabilities and better response to notices from law enforcement) there remains wide chasms of requirement that India, as a nation and law enforcement, as its key arm to ensure cyber security faces.

Cybercrime Statistics:

The details culled out from the National Crime Records Bureau for India, as of 2019[28], are set out hereunder.

A total of 18,372 cases have been registered under Cyber Crimes, showing an increase of 81.9% over 2018 (being approximately 10,098 cases). The rate of cybercrime reported cases also increased from 8.9% in 2018 to 16.1% in 2019.

Crime head-wise cases, Computer Related Offences under the Information Technology Act, 2000 (Amended) was **13,814 cases** in 2019 which formed the highest number of Cyber Crimes accounting for 75.2% during 2019.

The metropolitan cities of Mumbai (2527 cases) and Bangalore (10555 cases) reporting amongst the highest number of cybercrime cases in 2019.[29]

The above statistics do not appear to reflect reality. For instance it is reported that in UK, every 10 seconds, a Cybercrime is committed[30]. That India's cybercrime statistics is as reflected in the NCRB Report appears untenable given its population, permeation of data and the continuous stream of crimes committed particularly the rampant individual and financial frauds that proliferate. Through the orders passed in *Prajwala (supra)*, the Ministry of Home Affairs set up an online portal, cybercrime.gov.in, which was initially intended for online filing of cybercrime complaints pertaining to offences against women

[28] Statistics set out in this report pertain to 2019, as they are the latest available online (Available at: https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%201.pdf)
[29] https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf;
[30] https://economictimes.indiatimes.com/a-cyber-crime-every-10-seconds-in-uk/articleshow/2356802.cms?from=mdr;

and children. Presently, this portal has been expanded to include online filing of all cybercrime complaints. Whilst this was a welcome move, there are still a lot of jurisdictional and practical difficulties that impede effective enforcement against rampant cybercrimes. It is important that the present trust deficit that is probably reflected in the low statistics for cybercrime filings be bridged and the formulation of a specific law for cyber security may meet this requirement.

Global Trends in Cyber Security laws

The above issues and concerns that national security or law enforcement faces are global. Same also is the case of victims seeking remedies. With insufficient means to combat the terrors, threats and vulnerabilities of the online domain, several nations have resorted to specific cyber security enactments or separate cybercrime enactments.

Across multiple jurisdictions, laws specific to cyber security or cybercrimes are being enacted. There are also emerging trends and laws specific to Intermediary liability, particularly with respect to offences against women and children. Australia, Singapore, Sri Lanka are all instances of progressive and pre-emptive legislative actions that provide effective remedies against cybercrimes and Intermediary liability. China with its overarching provisions under its 2017 Cyber Security law ensures tight rein on data including of companies to submit to 'spot checks'. Without effective data laws for India, even countering these intrusive external legal formulations becomes ineffective. Resorting to probable consequent bans or restrictions of anything related to China or such other jurisdiction with intrusive enabling provisions would not be sufficient to protect India's interests. On the contrary, the same may be misconstrued as erratic or arbitrary actions that may impact economic decisions and be counter-productive to India's economy. The better alternative would be to ensure clarity and certainty through laws that

provide explicit provisions with respect to data storage, sharing and sovereignty, if any. Absence of clarity on these aspects harm as much as continued lack of effective provisions to protect personal data.

Law enforcement and Intermediary cooperation has been a huge pain point for India. This has been further aggravated due to persistent hate speech and fake news controversies on social media platforms. Misuse of content hosting apps and platforms has been another cause for concern. Intermediary liabilities and responsibilities, especially to combat violent online offences against women and children in particular and all individuals in general are much needed for India.

Several precedents are now available for India to evaluate including the very precise requirements under Australia's laws. Intermediary safe harbors, which have their beginnings in USA are being rewritten and reviewed even in such liberal democracies. USA is presently evaluating its first federal law that may restrict Intermediary protections. In the light of these emerging trends and keeping in mind the much larger stake that Nations are required to meet now, there is imperative need for review and formulation of Intermediary laws and regulations that will ensure clarity and certainty in its implementation. Contrary to perception, this will not only help Nations cope better to ensure cooperation from Intermediaries but will also help Intermediaries through assurance of clarity and certainty that law is expected to provide.

Laws that were cumbersome for reliance on electronic records such as the need for a certificate, have been repealed or replaced and simple methodologies have been adapted in many jurisdictions that had resorted to cumbersome procedures similar to those in India. Even the parent provision from UK, that India relied on was repealed even before India enacted its 2000 Act. Yet these cumbersome procedures have

continued for two decades under Indian law. It is important to immediately review these provisions to harmonize with global trends.

Need for India to Lead

India with its large population, which is technology savvy and well connected has an increased risk factor if cyber security is not better implemented.

The Digital India initiative has been implemented with expedition and a substantial part of young India is likely to be fully connected and online most of the time. Whilst 5G may still be a distant dream, it is still a reality, which will arrive in India within a couple of years. With such increased access to data and speed of access, cyber security risks and threats are only bound to grow exponentially.

India has refused to be party to the Convention on Cybercrime or what is referred to as the Budapest Convention. Instead, it has resorted to bilateral talks for ensuring cooperation. Whilst this is still welcome it may not be sufficient to meet the requirements of emerging threats. The recent trend in India also indicates that it is poised to review its international policies with respect to cyber.

Recent developments clearly indicate the increasing strength of voice that India has in being part of and leading global / international policies. It is imperative that India looks both inward and outward to evaluate its future position with respect to cyber security and bring it on par with global trends through separate legislation to combat cyber security threats and crimes. It is equally important for India to lead in deciding the future of regulating emerging technologies. This would start with India leading the fray on deciding and regulating Intermediary

liabilities to ensure and enable law enforcement without impacting fundamental rights.

In the light of the above, it is imperative that India reviews its existing cyber security legal framework and provide path-breaking legislation to ensure effective enforcement and a secure and safer cyber domain with remedies to combat individual, business and national security threats and vulnerabilities.

*****