International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

RETHINKING THE INFORMATION TECHNOLOGY ACT IN THIS NEW CYBER AGE

Dhrumi Gada[1], Santosh Aghav[2]

[1]Symbiosis Law School, Pune
[2]Symbiosis International (Deemed University), Pune, India
*Email: [2]saghav@symlaw.ac.in

Abstract

We live in a world which brimming with digitization in all sectors. We started with wars when guns and barrels were used, but now at the press of a button an entire country's power-grid can be blown, or a nuclear system can be hacked. Also, someone sitting with a high technology computer in Panama can cause a cyber attack in the US, or completely rip off the digital transactions happening in any other part of the world. Such is the magnificent scope of the cyber world. One vulnerability in your system, and that is all that an attacker needs. The term cyber has been derived from 'cybernetics', that denotes the science of communication and control over man and machine.

The very most important thing that a country needs is a robust law to tackle cyber crimes and crimes related to the Internet. India already has an Information Technology Law and related guidelines and rules, but it seems that it is not strong enough from the practical viewpoint as well as for the crimes that are advancing in this world.

This paper discusses the various shortcoming of the current Information Technology Act, which is the only special act that is passed by the legislation to tackle cybercrimes. Apart from this in my tenure with Maharashtra Cyber, as a chief minister's fellow, I have also interacted with various officials and mapped out their recommendations for improving the law for practical application, based on the ground difficulties they face. Also, in the end a lot of inspectors and sub-inspectors, those who are actually involved in the field work and investigations have been spoken to, and the papers lists out various recommendations form their side based upon the impediments they face.

Key words: Information technology, cyber, cybercrime, digitization, reforms, amendments, data protection, current landscape, Maharashtra Cyber, recommendations, investigations, interview, loopholes, law enforcements agencies, stakeholders

Introduction

"There are only two types of organisations: Those that have been hacked and those that will be."- Kaffenberger, Lincoln

We live in a world which brimming with digitization in all sectors. We started with wars when guns and barrels were used, but now at the press of a button an entire country's power-grid can be blown, or a nuclear system can be hacked. Also, someone sitting with a high technology computer in Panama can cause a cyber attack in the US, or completely rip off the digital transactions happening in any other part of the world. Such is the magnificent scope of the cyber world. One vulnerability in your system, and that is all that an attacker needs.

The very most important thing that a country needs is a robust law to tackle cyber crimes and crimes related to the Internet. India already has an Information Technology Law and related guidelines and rules, but it seems that it is not strong enough from the practical viewpoint as well as for the crimes that are advancing in this world.

The phenomenon of cybercrime is such that crimes occur all over the global, but come in notice locally. These crimes know no boundaries. Unlike all the traditional crimes, cybercrimes follow no jurisdiction, and this is a global crime [United Nations Office on Drugs and Crime (UNODC), Report 2013]. The European Commission report (2000) specifically states that, "computer-related crimes are committed across cyberspace and do not stop

at the conventional state-borders. They can be perpetrated from anywhere and against any computer user in the world"[European Commission Report, 2000].

Crimes in the cyberspace have a very different dimension than the other crimes, which tend to make all the legal jurisdictions obsolete [Observations of the Mallimath Committee, 2003].

Some Suggestions For The Changes Needed In The It Act

Below are some suggestions for proposed amendments [The amendments proposed here are in furtherance to the last recent amendments done to the IT Act in 2008] in the Information Technology Act of India.

1. ***The difficult interplay between the general and the special act***: Before the Information Technology Act came into play, several general laws such as the Indian Evidence act and the Indian Penal Code, were amended to include the general provisions for the crimes in the cyber domain. But once the special law, i.e. the IT Act was introduced, the provisions of the cyber crimes were scattered throughout in a lot of general and special laws, making it difficult for the prosecutors, law enforcement and judiciary to understand the interplay between these different acts with respect to the provisions for the same crime and this further watered down the efforts taken for effective enforcement.

2. Overlap of Section 43 (j) and Section 65 of the IT Act: Section 65 of the IT Act, applies to the tampering and the stealing of source documents. This was a section that initially existed in the 2000 ACT But the 2008 amendment, introduced a section 43 (j), which mentioned the same things such as whoever steals, destroy or alters a computer source code with an intention to damage shall be liable. Thus, there is a need to remove the duplication and harmonize these two sections.

In fact, in the section 65 the punishment is as follows: "shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both", where as in the new section added in the 2008 amendment only has a compensation up to INR 1 crore attached to it to be given to the victim.

3. Need to redefine section 43 under the IT Act with respect to the various different cyber crimes: Section 43 is a huge section encompassing many cybercrimes at one go. In today's digital world, with so many cyber crimes evolving daily, there is a need that there should be a separate head created for each and every cybercrime mapped out under section 43 to make the enforcement as well as the interpretation of that section easier. Section 43 deals right from hacking, virus contamination attacks, data theft, computer resource theft, denial of service attacks to network disruption. There is a need that each of these crime are dealt with separately and different punishments are accorded to them according to the severity of the crime, rather than just defining an upper cap of 1 crore rupees.

The essence of the crime lies in its component and the actions that make the act a crime. If the crimes are elucidated in the right manner then a reasonable man shall also no as to which acts could be labeled as an offence, and which could not be. The Apex Court in the case, *Kartar Singh v. State of Punjab* [(1994) 3 SCC 569] made a point that: "The division of each of these 9 heads under section 43 into different cyber crimes, will assist the police in enforcing an offence effectively as well as to collect evidence to sustain and support his prosecution under a single head. Similarly, the court shall also be capable to deal with cases in a very smooth and focused manner.

4. Addition of the provision of biometrics in section 66C of the IT ACT: Section 66 deals with identity theft. The provision in itself is complete and to the point, but according to the advances in todays fast-paced world, the parameters relating to a man's unique identifications should be defined as to include the biometrics of an individual. Addition of illustrations shall make it easier for the judiciary as well as the law enforcement to effectively register as well as prosecute the offender. Thus the width of the parameters should be expanded to include retina, fingerprints and other such biometrics.

5. What exactly is personation under Section 66D: Thus, Section 66D of the IT Act says that: "*Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with*

imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees." Thus what exactly is personation here is unclear. Would personation also mean that adopting an identity of a person who is already alive, or who is dead, or a person can just create a fictitious person in mind? Let's say a person calls being the manager of Kotak Bank for committing a phishing fraud, this is cheating by personifying a real person who may be the manager of the Kotak Bank, but if there occurs a romance matrimonial fraud, wherein the person makes up an avatar of a high investment banker, studied from oxford, and tries to lure the girl to marry her and transfer money. Now will this also come under cheating by personification? Thus, there should be clarity on what should fall under this section and more illustrations should be given to clarify its stance.

6. Lack of clarity in Section 66E of the IT Act: The construction of sec 66 E is too narrow, as it concentrates on the transmitting or publishing of images or videos of private parts of individuals without their consent. In the *Justice Puttaswamy v. Union of India [WRIT PETITION (CIVIL) NO 494 OF 2012]* case, it was mentioned that apart from just concentrating on the private body parts, the importance should also be given to the privacy of an individual.

Also there should be different kinds of severity in this particular crime, like the person who just circulates and transmits such nude images of an actress from a friend he has got has to be treated on a different level other than a person who has committed the crime of sharing it deliberately to take revenge, also know as 'revenge porn', or a person who has raped a girl and then circulated the videos and photos online of her private body parts. Thus, the punishment given for such crimes like revenge porn and transmitting of rape videos and photos online has to be so stringent that the purpose of deterrence is achieved, as an imprisonment up to 3 years or a fine extending up to INR 3 lakhs will not suffice.

7. Too much power given to law enforcement agencies under section 69-69B of the IT Act- Section 69-69B deals with monitoring, decryption and blocking of content that the state feels likes is in the interest of the nation. Now what about intermediaries that have end-to-end encryption enabled on their platforms? How will the WhatsApp be able to detect the source from where the message is coming or the source of the information, if the platform itself does not allow for the same? Will that platform be liable for failure in assisting the government agency just because it has certain norms to respect the privacy of an individual? Also, this section is inserted to have a regulatory checks and balances mechanism and enable the fair take down of illicit content on the web. The law enforcement agencies that are liable to direct such notices for takedowns, are only responsible for themselves determining what should be monitored, decrypted and intercepted. That may give too much surveillance powers to the law enforcement agencies to collect any traffic data they may feel pleased to, if they feel it is so called 'necessary or expedient to do so'.

Thus, it is essential that such provisions may be reviewed as well as reconsidered. An independent committee completely free of the law enforcement agencies can be set up to review the request by such law enforcement agencies for monitoring, decryption and intercepting messages from the source which is in the interest of the security of the state and for other reasons.

8. Various provision are not accounted for- Today due to new cybercrimes evolving, the act does not sufficiently tackle those and thus these kind of crimes are unaccounted for. Crimes like crypto currency scams, romance scams, matrimonial frauds, cyber bullying and trolling, ransomware, hate speech, self-harm due to games like blue-whale, do not find a specific mention in the IT Act, though some bits and pieces would be in the general laws like the IPC. But it is better to define and account or these kind of evolving crimes by an amendment in the current IT Act.

9. Investigations only to be done by officers above the rank of a police Inspector: Even though, the police have been proactive in identifying certain criminals as well as their modus operandi for conducting their crimes, they have also been reactive with respect to controlling the cybercrimes in the state and implementing respective preventive measures. Till date the cyber crimes reported in our country as well as the conviction rate is a very small figure in contrast to the reality. Interacting with the law enforcement officials, I got a chance to understand the whole reality of this scenario and below are some issues faced by the officers, the relevant impact it has on

their investigation as well as the recommendations from their side. Assignment/Appointment of an Investigation Officer under Section 78 of the Information Technology Act, 2000, states, "A police officer not below the rank of inspector shall investigate the matter".

Cyber Crimes are typical in nature and require special investigation, techniques and are time consuming. If only an official at the level of police inspector and above is capable to investigate such cases, the rate at which these cases will be solved and even entertained will be drastically reduced. Also, a lot of times since the inspector level officers are over-burdened with work, there is an official sub-delegation of work that happens and thus the prosecution and the investigation of the case goes weak, as these officers below the rank have not been given an opportunity or exposure to such investigations till date. Also, in police station headed by officers of the Assistance Police Inspector Level (API), it is very difficult as they have to handle the cases unofficially and do all the investigations themselves and then an inspector level officer just appears before the court as the investiating officer of the case, which increases the gaps and lacunas in the case.

As per the relevant provisions of Cr.P.C., the Officers at one level below the Inspector rank can investigate some of the crimes under section IPC 323,324,325,326. Similar delegation is recommended however based on the gravity and nature of the cyber offences under the IT Act. In case of financial or cyber economic frauds, such thresholds can be decided upon the damages caused e.g. any investigation where there is a data theft or phishing, pharming or any other offences where values of damages shall not exceed INR 40 lacs, can be investigated by a person of API level.

10. No criteria for selecting officials for cyber crime investigations: Till date IT Act does not mention that officials only with respective technical skills and understanding of the IT Act, shall be a part of those people who investigate a case that is registered with their law enforcement agency. Most of the Police personnel selected for the Cyber Crime Investigation purpose are not even aware of the job and role they are expected to perform, thus the quality of the investigation process lacks quality and outcome. E.g. If an investigation officer of even an inspector level is not aware of the fact of what is a digital signature or what are the digital payments modes or how the banking framework works, and how people perform phishing attacks, such personnels shall be the biggest weak link in the investigation.

The Police personnels who have proven core competence of investigation and understanding of such matters are to be selected. The roles and responsibilities with job objectives and description shall be clearly laid down upon and only such personnel shall be selected upon to work in this particular team designated in a police station. There should be certain qualifying internal parameters defined at each police station level, which shall also include basic education with a technical background, understanding of the information technology law, adept at various new technologies and also police manual and various laws applicable, and any other such parameters the department may deem to be fit.

11. Lack of investigation guidelines and absence of specific procedures and rules along with trainings: Since Cybercrime investigations are different from physical crime investigations, there are no certain specified rules for the investigation which provide a standard format or sets common norms and guidelines for investigation. As there are no fixed guidelines for investigation, each investigation officer has its own way and method of investigation, which may further create more loopholes in the case. There are no formal rules and procedures laid down for seizure of the evidence of cybercrimes, for preparing a chain of custody, for the storage of evidence or how it has to be sent to the forensic labs for investigation, presentation of evidence in the court along with relevant certificates to be furnished, etc. which further makes evidence preservation difficult, as digital evidence can be easily tampered with.

The emphasis shall be laid down for releasing and publishing at least basic guidelines for the investigation process and procedures to be followed. The stimulus trainings for latest investigation and evidence collection techniques at periodic intervals shall be provided, even if the same are required from private investigators outside. It should also focus on various aspects of the forensics procedures to be followed for the investigation including the relevance of chain of custody maintenance, forensic reports admissibility of evidence in the courts etc.

Recommendations For Solving The Current Cybercrime Landscape

(After Interviwing Officials At Maharashtra Cyber)

Since I got the change of working at Maharashtra cyber, in my chief minister's fellowship programme, I got to ***interview*** a lot of officials namely ***IPS Brijesh Singh***, Special Inspector General Police of India, ***IPS Harish Baijal***, Deputy Inspector General of Police, ***Dr. Balsing Rajput, Superintendent of Police***, Maharashtra Cyber, ***Mr. Sachin Pandkar, Superintendent of Police***, Maharashtra Cyber, ***Mr. Vijay Khaire, Deputy Superintendent of Police***, Maharashtra Cyber, ***Ms. Khushbu Jain, Advocate, Supreme Court of India***, and also had the chance to interact with ***Dr. Rama Vedashree, CEO, Data Security council of India***. Below are the outcomes of the interactions that I had regarding the current legal landscape of the cybercrime law in India and the ground difficulties they face while implementing it.

1. Formation of an Intelligence hub:

Establishment of an 'intelligence hub' or information sharing community that facilitates information sharing through a public-private partnership within and across industry sectors, FIs, banks, LEAs and even international stakeholders and provides:

i. In depth investigations on cyber crime methodologies adopted for a range of cyber crime types;

ii. Training and dissemination of knowledge on the preservation of digital evidence and seamless real-time data sharing; and

iii. Aid to law enforcement agencies and investigative bodies for various prosecutions in India as well as overseas for faster investigations

2. Lack of seamless information sharing across financial industry:

As a lot of crimes today are cyber and deal with payment methods, the highest amount of cooperation required by the LEAs is from the Banks, FIs, and NPCI. But due to the regulatory authorities like RBI, FIU, banks are still not free to share transaction details with the LEAs unless a notice is served on them, which makes the complete process more slow. Banks, FIs, NPCI are still conscious of what they can legally share within their regulatory framework, and its my opinion that, where needed, regulators and legislators should be encouraged to make changes in the rules and legislation, so that the cooperation with LEAs can be smooth which in turn can increase the enforcement of law and the implementation levels.

3. Need for working towards a shared goal:

I would like to mention an example of EMMA operation. The major reason why operations like these are successful is because they receive great cooperation of the banks and financial institution, and then they work in tandem with LEAS. As criminals nowadays work in tandem and due to which they get across any technological and organizational barriers, we as LEAs also need to come together and need not work in our own silos. **Co-working towards a shared goal** amongst all the members of the 'family of policing', banks, individuals, business and civil society and regulatory bodies though partnership is an essential aspect to be considered, as policing in itself is not the only silver bullet solution. Mah-cyber has an anti-phishing portal, where we act as links between the victim as well as the several stakeholders involved. It would be great if banks can take prompt action and help us close the loop in our initiative for helping the victims.

4. The need of a shared platform with nodal officers of various stakeholders for prompt action

Many a times the investigation becomes slow as nodal officers of intermediaries, Internet service providers, telecom providers, banks, payment gateways, mobile wallets, e-commerce platforms do not share the details with the LEAs. According to me, there should be an online platform where LEAs and every nodal officer of the above mentioned stakeholders shall be **mandatorily** involved in this platform for acting on notice and take down regimes, freezing accounts, blocking numbers, blocking wallets, suspending telecom connections and for

taking any other prompt action that may be required by the LEAs.

5. Intra-interaction platform for LEAs for smooth communication

Just like Quora, which is an information sharing platform in a question and answer format for the public to interact, there should be a platform for only LEAs where investigating officers can share their experiences or officers can discuss the difficulties they are facing during investigation and seek advice from other officers of other states and jurisdiction. Intelligence can also be shared on this platform for other police units to stay alert.

6. Coordinated action to pursue cyber threats by following the 'four Ps':

To follow a coordinated action against key cybercrime threats and targets, the police should follow a four P's method: Pursue, prevent, protect and prepare.

- **Pursue** organized criminals by prosecution and disruption;

(By relentless and coordinated action across the jurisdictions involved, with various stakeholders in the society, also by employing more manpower of officers for the cyber investigation for tackling the volume of cybercrimes today and by funding the police for better performance by being technically and tool-wise sound)

- **Prevent** people from becoming criminals;

(This will only happen if criminals can see the ease with which LEAs catch hold of them which will discourage them from further committing these crimes)

- **Protect** businesses and the laymen against such serious and organized crime; *(Raising awareness and taking prompt action and also develop intelligence led policing. Also adopt the reactive and the proactive method wherein reactive is prompt action against the crime and proactive means predicting, warning and preventing future crimes)*
- **Prepare** for attacks by building post-event resilience to reduce the impact of crime and improve resilience for future prevention

(Improving the infrastructure, tools, techniques and methods to solve crime)

7. Segregation of crimes intensity wise:

Most of the time and resource of the police force are used up in investigating the high-volume of economic cybercrimes but which have really meager value of financial loss attached to them, where as the ones that require the most attention are crimes of relatively higher value and lesser in volume. Thus, there needs to be segregation of cases and they need to be taken up intensity wise.

8. Need to take proactive measures:

- All the LEAs should come together and develop full-proof strategies to alert the individuals and also take proactive measures
- Narrowing and zeroing down on certain specific suspects and targeting messaging to handpicked specific groups, identifying their specific vulnerabilities is key. Novice users can be categories differently; people can be clubbed according to age groups where a particular crime is more prevalent in their age group, for e.g. dating scams is common in people between their 20's-30's.
- Requesting institutions such as banks to have in place sufficient and apt levels of installed controls, also partner along with technology companies to sell their devices with preinstalled countermeasures.
- Partner to work with bodies already working and connected with groups (from schools to Citizens Advice, to signal events to spread awareness etc.)

Conclusion

India is not well equipped to deal with the growing menace of cybercrimes, as we are more on the reactive side of taking measures rather than the proactive. A quick rethinking is the need of the hour for placing effective

enforcement in place as alternatives. Formation of a robust cyber security policy, revamping the entire IT Act in order to keep up with the new evolving crimes, creating special court for assignment of such cases along with special prosecutors for such case, giving more importance and defining the severity of the punishments for crimes against women and children, training the current law enforcement agencies on the way to tackle cybercrimes and giving a hands-on experience on cutting edge technologies, supporting the capacity-building and improving the infrastructure of the forensic labs so that evidence examination reports can be submitted effectively in a timely and detailed manner. Also, there should be a fixed timeline for deciding cases, especially for those, which are very heinous, and details of laws, regulations and remedies available to a victim shall also be made available to the public online.

It is very apt to reproduce a quote said by Justice Krishna Iyer [Justice V.R. Krishna Iyer, in Re The Special Courts Bill v. Unknown, AIR 1979 SC 478 : (1979) 1 SCC]. He says that "An 'ephermal' measure to combat a perennial menace is neither a logical step nor national fulfillment". Just by applying Dettol to a wound does not really heal it or curb it from being hurt more, but just acts as a temporary provision. To curb this menace, which is going to be evergreen, we need to have similar strong provision and a complete revamp of the IT Act which can fit into these new times.

References

1. Bansod, A. (2013) Legal Control of Cyber Crime against E-Banking in India. Pt Ravi Shankar Shukla University, Raipur.

2. Date, S. (2003) Monitoring of Economic Offences: A Management Control Systems Perspective. Indian Institute of Cost And Management Studies and Research (INDSEARCH), Pune.

3. Directorate of Forensic Science Laboratories, G. of M. (2017) Information about Directorate of Forensic Science Laboratories, Introduction, Vision, Divisions, Hierarchy, Organisational set up, Cyber Division. Available at: https://dfsl.maharashtra.gov.in/1119/Cyber-Forensic (Accessed: 28 October 2017).

4. FIU-IND (2015) Financial Intelligence Unit-India Ministry of Finance Government of India Financial Intelligence Unit-India Annual Report. Available at: http://fiuindia.gov.in/pdfs/downloads/annualreport2015-16.pdf.

5. Godara, S. (2011) Prevention and Control of Cyber Crime in India: Problems, Issues and Strategies, Maharshi Dayanand University, Rohtak.

6. Gour, H. S., Srivastava, A. B. and Lal, C. S. (2011) Dr. Hari Singh Gour's Commentaries on the Indian Penal Code: Section 302 to section 511. Law Publishers (India) (Dr. Hari Singh Gour's Commentaries on the Indian Penal Code: As Amended by the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) and Revised Edition on a Wider Format, Covering All Notable Verdicts of the Supreme Court, Hight Courts, with). Available at: https://books.google.co.in/books?id=6bZrtQAACAAJ.

7. N. S. Nappinai (2017) Technology Laws Decoded, LexisNexis

8. Law Commission of India, G. (1972) The Trial and Punishment of Social and Economic Offences. Government of India, Minstry of Law and Jusitce. Available at: http://lawcommissionofindia.nic.in/1-50/report47.pdf.

9. Mallimath, V. S. (2003) Justice Mallimath Committee on Reforms of Criminal Justice System. Available at: http://mha.nic.in/sites/upload_files/mha/files/pdf/criminal_justice_system.pdf.

10. Mittal, S. and Singh, A., 2014. A Study of Cyber Crime and Perpetration of Cyber Crime in India. In Evolving Issues Surrounding Techno ethics and Society in the Digital Age (pp. 171- 186). IGI Global.

11. Minstry of Home Affairs, G. (2018). Advisory on cyber Crime Prevention and Control. New Delhi: Minstry of Home affairs, Governement of India