Page 4168 - 4183 **DOI** *https//doij.org/10.10000/IJLMH.1110298*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Crime through Mobile Phones: A Critical Analysis

SHIVANGI MEHTA[1], JYOTI[2], DR RICHA RANJAN[3] AND GARIMA KANWAL[4]

ABSTRACT

The exponential rise in mobile phone usage has profoundly reshaped crime patterns, facilitating offenses spanning cyber fraud, smishing, coordinated organized crime, and device theft. In India, approximately 70% of cyber fraud cases involves mobile phones , and globally, attackers exploit Bluetooth vulnerabilities, malicious SMS apps, and SIM swap fraud to enable financial crime and identity theft.

Concurrently, mobile devices have emerged as vital sources of digital evidence. Forensic teams can retrieve call logs, message histories, GPS tracks, multimedia, and app metadata—and often recover deleted or encrypted content. Mobile device forensics is a rapidly evolving field that includes extracting data from flash memory, SIM and external storage, carrier call detail logs, and even volatile memory using physical dumps or JTAG/chip off techniques. Studies indicate that cell phones are implicated in most violent and drug related crimes, with recoverable evidence found in over 50% of such cases.

Despite this importance, mobile forensics faces significant challenges. The rapid evolution of operating systems and new devices requires continuous updates to forensic tools. Proliferating encryption, biometric locks, and frequent data overwrites further complicate evidence retrieval. The fragmented app ecosystem and absence of standard protocols complicate investigations. Even when data is acquired, legal and human factors—such as privacy rights, variable judicial acceptance, and low practitioner awareness—limit its admissibility and use.

This study critically examines both sides: mobile phones as enablers of crime and as tools for law enforcement. It synthesizes technical literature, legal frameworks, and case studies—including high profile Indian cases and global mobile forensics initiatives—to underscore trends, limitations, and opportunities. It calls for enhanced public awareness, stronger device security measures, and standardized, legally sound forensic practices. Addressing technological, operational, and legislative hurdles is essential to balance crime prevention with digital privacy in the mobile era.

[1] Author is an Assistant Professor at Swami Devi Dyal Law College, Haryana, India.
[2] Author is an Assistant Professor at Swami Devi Dyal Law College, Haryana, India.
[3] Author is a Professor at Swami Devi Dyal Law College, Haryana, India.
[4] Author is an Assistant Professor at Swami Devi Dyal Law College, Haryana, India.

 [ISSN 2581-5369]

I. INTRODUCTION

"The world, it is not run by weapons any more, or energy, or money. It is run by ones and zeros, little bits of data…It is all electrons. There's a war out there, a world war. It's not about who has the most bullets, it's about who controls the information – what we see and hear, how we work, what we think. It's all about information"[5]

Digital Space or Cyberspace is the driving force for the world today. From ordering a cab to ordering food to booking tickets for travel to shopping, everything can happen with just tapping a finger. The magic that made this happen was the advent of internet and technology.[6]

Technology has left no aspect of human life untouched and has made human life easier. Technology has given birth to the machines known as computers that has the capacity of storing as well as bringing advancements in terms of various applications such as networking types of mobiles having better and advanced technology possible in the market. These technological advances made transition into paperless contact feasible.

Rapid growth in internet-enabled mobile phone lets us manage our financial transfers, official and institutional orders, easy email or social networking access, and more. Internet-enabled smartphones, laptops, etc. are capable of performing the functions of machines but it lacks protection which is a very crucial feature.

However, as they say every coin has two sides. Cybercrime is the bad boy of the digital world. While the technology and the internet have several advantages, the abuse as well as expansion has culminated in a heuristic rise of internet-related crimes.

With our mobile phones we have become capable of virtually performing the tasks of computer but this is also making our cell phones vulnerable to various types of cybercrimes such as risk of fraud, theft of financial information, identity theft, etc. In recent times, India has become a major spot for cybercriminals, where most hackers and other malicious users commit crimes through the internet.

In the words of Dr. Debarati Halder and Dr. K. Jaishankar, Cybercrimes are "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim

directly or indirectly, using modern telecommunication networks such as Internet (Chat

[5] M. Dasgupta, Cyber Crime in India- A Comparative Study, 2009
[6] India: Revisiting the Current Scenario of the Safeguards for Cybercrime, SSRN

 [ISSN 2581-5369]

rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)."[7]

According to the UNO expert recommendations, the term Cybercrimes covers any crime committed by using computer systems or networks, within their framework or against them. Theoretically, it embraces any crime that can be committed in the electronic environment. In other words, crimes committed by using e-computers against information processed and applied in the internet can be referred to cybercrimes.[8]

Under Indian law, the legislation that deals with offences related to such crimes is Information Technology Act, 2000, which was later amended as Information Technology Act, 2008. In order to define such an offence, it can be done through cause of action, it is a combination of computer and crime.

Cybercrime is a modern development created by intelligent, professional offenders. These offences are conducted using computers and mathematical structure, rendering them distinct from regular forms of offences. These are blue collar offences since they aren't that distinct from other technology offences, though known under specific titles.

For a long period, criminal jurisprudence was completely ignorant of these kinds of offences. But cybercrime started becoming a great threat to mankind and protection against cybercrime became a vital part for social, cultural and security aspects of a country.

Therefore, there is a need to learn from the hackers and use that knowledge to prevent future crimes. The present situation is that there are several laws for the protection from cybercrimes but each one has its own scope and limitations. India, is no doubt, imposing sanctions to deal with such crimes.[9] However, the conviction rate is found to be insignificant. What is needed, a specific law particularly dealing with cybercrimes.

II. INSIDE THE DARK WEB: TYPES OF CYBER CRIMES YOU SHOULD KNOW

1. Malvertising

Malware among all types of cybercrime, is the most dangerous and serious threat to the internet and e-commerce. Malvertising malware refers to different kinds of viruses, trojans, worms, and other harmful software that lock your computer without realizing their presence. Possibly, one of the most commonly executed cybercrimes in India, malvertising occurs when cyber criminals place malicious advertisements on websites without the knowledge of the latter. They secretly break into the computer system and steal valuable data from the system

[7] Jonathan Clough, Principles of Cybercrime 12, Cambridge Publication, 2nd Edn 1998
[8] Deccan Chronicle , Cybercrime
[9] https://ssrana.in/articles/india-revisiting-the-current-scenario-of-the-safeguards-for-cybercrime-

 [ISSN 2581-5369]

without any permission. Once clicked, the malicious code will be downloaded to the device. This is one of the fastest growing types of cybercrimes in the world, particularly, in India. To avoid this, you should download ad-blockers to your computer and make a conscious effort not to click suspicious-looking ad-links.[10]

2. E-mail Bombing

It is a form of cybercrime in which a person sends a number of emails to the inbox of the targeted system/person. Mail bombs usually fill the email space and can end up crashing the email server.

3. Phishing

Phishing refers to the stealing of information such as passwords, credit card details, usernames, etc., from the targeted person over the Internet. Phishing is done by email spoofing and instant messaging. In this type of crime, hackers make a direct link that directs the targeted person to a fake page that looks and feels the same as the actual one.

4. Cyber Warfare

It refers to any politically motivated attacks on information systems on the internet. Such information systems, which are usually vulnerable to disruption caused by cyber warfare, are government-owned systems. Cyberwar attacks may disable official websites and networks, disrupt essential services, steal or alter classified data, and cripple financial systems.

5. Voice Phishing

Voice phishing is a technique used to obtain access to private, personal and financial information from the public. Voice phishing uses a landline phone or a mobile phone call to obtain information by falsifying their true identity.

6. Cyber Trafficking

It refers to the Internet user as a tool for trafficking in arms, drugs, human beings, etc.[11]

7. Smishing

Smishing is a malware assault in which the recipient receives an SMS acting as a profitable service that requires them to reveal their ultimately misused personal details. It is also intended to implement mobile phone app ransomware which are close to phishing and vishing

[10] 4 types of Cyber Crimes That Everyone Should Know About: https://yourstory.com/2016/12/4- types-of-cybercrime?utm_page loadtype=scroll (last visited at May 4, 2020

[11] Cyber Laws In India - Security – India: available at http://mja.gov.in/Site/Upload/GR/Mobile_Cell_Phones_and_Cyber_Crime_in_India__How_Safe_Are_ We.pdf (last visited at May 4, 2020)

 [ISSN 2581-5369]

assaults that capture and abuse sensitive personal details. In such assaults, the attacker obtains internet banking credentials, credit card information, email ID and password.

8. Bluejacking

Bluejacking is the transmission of unintended files, such as handheld devices, from Wi-Fi to Android. People using Bluetooth on mobile phones and PDAs can send messages, including pictures, to any other user within a range of 10 meters or so. While connecting to Bluetooth, the hacker may act on the user's device by stealing pictures, documents and personal information.

III. INDIAN CYBER CRIME LEGISLATION

In India, the Indian Penal Code,1860 (now replaced by the Bharatiya Nyaya Sanhita,2023) is a very comprehensive penal legislation. The penal code does not specifically cover cybercrimes. This is because at that time the legislators never thought of visualization of internet and thus as a result of this, the various challenges that criminal exploitation of computer networks and internet throws up were not addressed effectively.

An amendment in the Penal Code was made by the Information Technology Act, 2000. The said amendments purely relate to making certain categories of offences under the Indian Penal Code applicable to electronic records. Thus, as a result, a need was felt by the legislators to include a distinct chapter on cybercrime in India's first cyber law.

Information Technology Act, 2000

Enacted in 2000, India's first cyber law was passed by both the houses of the parliament on17th May, 2000. It received the assent of the President on 9th June, 2000 was finally implemented on 17th October, 2000 and came to be known as the Information Technology Act, 2000. This Act is the prime legislation dealing with cyber offences and electronic commerce in India which is based on the United Nations Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL).

The Indian cyber law embodies the Indian Legal Response to the emerging challenges of cybercrime. Chapter XI of the IT Act entitled 'Offences' is the relevant chapter that deals with kinds of cybercrimes and investigation powers. These acts have been declared penal offences, which are made punishable with imprisonment and fines.

 [ISSN 2581-5369]

As per Section 2(i) [12] of the I.T. Act, 2000, mobile phones are encompassed in the definition of a Computer. Mobile phones have been used for exchange of information. Thus, any information exchanged on a mobile phone, even though it may be calls, email or input of information, is included in the frame work of the I.T. Act, 2000.

The first category of cybercrimes which it addresses deals with the issue of unauthorized access and hacking.

Section 65 of the I.T. Act, 2000 deals with causing damage to a computer source code. It states that anyone who knowingly or intentionally conceals, destroys, or alters any computer source code, when the source code is required to be kept or maintained by any law currently in force, is brought within the ambit of penalty. This offence is made punishable with imprisonment for up to three years or with a fine up to two lakh rupees or both.[13]

Section 66 I.T. Act,2000 criminalizes hacking. This offence involves the following elements:

1. There should be intent on the part of the accused to cause wrongful loss or damage to the public or any person, or

2. There should be knowledge attributable to the accused that he is likely to cause wrongful loss or damage to the public or any person.

3. The accused must destroy or delete or alter any information residing in computer resource, or

4. The accused must diminish the value or utility of any information residing in computer resource, or

5.The accused must affect any information residing in a computer resource injuriously by any means.[14]

If one of the first two and one of the last three of these conditions are satisfied, then it constitutes the offence of hacking within the meaning of section 66 I.T. Act, 2000.

Section 67 addresses Online Obscenity. This provision deals with the offences of publishing or transmitting obscene electronic information. The punishment for this offence on the first conviction is imprisonment for a term up to one lakh rupees. In the event of a second or

[12]The Information Technology Act (No 21 of 2000), Section 2(i)
[13]The Information Technology Act (No 21 of 2000), Section 65
[14]The Information Technology Act (No 21 of 2000), Section 66

 [ISSN 2581-5369]

subsequent conviction, the quantum of imprisonment and fine both are doubled.[15]

The first case of conviction under section 67 of the IT Act, 2000 was **State of Tamil Nadu v. Suhas Kutti,** in which the accused was found guilty under section 469, 509 of the Indian Penal Code and Section 67 of the I.T. Act, 2000 for posting some defamatory and obscene messages about the victim on a yahoo messaging group as a result of which the victim started receiving annoying calls.[99]

Further, in the case of **Avinash Bajaj v. State (NCT) of Delhi,** obscene material was put up for sale by one person on the website of Bazee.com and was also sold within a short duration to several people in various parts of the country. The Hon'ble Court while deciding whether the publication of the material indirectly comes within the purview of section 67 or not, held that the website is liable under the section as ultimate transmission of obscene material wasn't possible without initial facilitation by the website.[100]

In **Mohammed v. State,** the High Court of Gujarat analyzed Section 67 of Information Technology Act, 2000 and held it is not applicable to the case of threatening email received by Chief Minister of Gujarat, hence ordered to be deleted from the matter.

Section 68 criminalizes a failure to comply with the order of the Controller of Certifying Authorities.

Any person who breaches a protected system leaves himself open to criminal liability under section 70**.** Anyone who accesses or attempts to access a protected system commits an offence and can be punished with imprisonment for a term of up to ten years and shall be liable for fine.[16]

Section 71 of I.T. Act, 2000 deals with misrepresenting or suppressing a material fact from

[15]The Information Technology Act (No 21 of 2000), Section 67: Punishment for publishing or transmitting obscene material in electronic form.– Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees

[16]The Information Technology Act (No 21 of 2000), Section 70: Protected system.– [(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Explanation.–For the purposes of this section, ―Critical Information Infrastructure‖ means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.] (2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1). (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine. (4) The Central Government shall prescribe the information security practices and procedures for such protected system.

 [ISSN 2581-5369]

the Controller of Certifying Authorities in order to obtain any license or Digital Signature Certificate. It states that whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or electronic signature certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.[17]

Section 73 criminalizes the publication of a Digital Signature certificate that is false concerning certain particulars. It states that–

(1) No person shall publish an electronic signature certificate or otherwise make it available to any other person with the knowledge that–

(a) The Certifying Authority listed in the certificate has not issued it; or

(b) The subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended unless such publication is for the purpose of verifying an electronic signature created prior to such suspension or revocation.

(d) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.[18]

Section 74 deals with the offence of publication of a Digital Signature Certificate for fraudulent or unlawful purposes. It states that, whoever knowingly creates, publishes or otherwise makes available an electronic signature certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.[19]

Breach of confidentiality and privacy by an authorized official under IT Act,2000 is made punishable with imprisonment up to two years, with fine of up to one lakh rupees.

Section 77 IT Act,2000 elaborates the issue of non-interference of penalties with other punishments. It provides that no penalty imposed or confiscation made under the Act shall prevent the imposition of any other punishment to which the person affected is thereby liable under any other law currently in force.[20]

[17]The Information Technology Act (No 21 of 2000), Section 71
[18]The Information Technology Act (No 21 of 2000), Section 73
[19]The Information Technology Act (No 21 of 2000), Section 74
[20]The Information Technology Act (No 21 of 2000), Section 77

 [ISSN 2581-5369]

Section 76 IT Act, 2000 provides for the power of confiscation. It lays down the conditions under which any computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto that have been used to contravene any provision of the IT Act or any rules, orders or regulations made there under can be confiscated. It states that the above-described articles can be confiscated if it is established to the satisfaction of the court adjudicating confiscation that the person in whose possession, power, or control any such article is found, has committed one of the violations described above. If it is determined that the possessor is not responsible for the offence, the court may, instead of ordering confiscation, make such other order authorized by this Act against the offender as it may think fit.[21]

Section 78 IT Act, 2000 deals with the power to investigate offences under the Indian cyber law. It provides that notwithstanding anything contained in Criminal Procedure Code,1973 (now replaced by The Bharatiya Nagrik Suraksha Sanhita, 2023, no police officer below the rank of Deputy Superintendent of Police shall investigate an offence under the IT Act, 2000.[22]

Section 80 of the Act deals with Power of the Police Officer and other officers to enter and search. Section 80(1) confers two distinct forms of discretion on a DSP. The first is the right to enter any public place and without a warrant to search and arrest any person. The second is that a DSP can search and arrest without warrant anyone whom he reasonably suspects of having committed, of committing, or of being about to commit any offence under the IT Act. The new law has not defined guidelines for exercising discretion under section 80, and the requirements for deciding whether the DSP may have fair suspicion of the individual concerned are unclear. Many find the authority given under section 80(1) to be a significant infringement of individual rights and privacy.

The Explanation to section 80(1) says that the term 'public place' includes any public conveyance such as a bus, train, aircraft, any hotel, any shop, or any other place intended for use by or accessible to the public. The definition of 'public place' in the explanation to

[21]The Information Technology Act (No 21 of 2000), Section 76 : Confiscation.–Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation: Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act

[22]3 The Information Technology Act (No 21 of 2000), Section 78

 [ISSN 2581-5369]

section 80(1) is very wide and is likely to include numerous things within its ambit. For example, a hotel has been considered a public place. It has not been specified which part of the hotel is a public place and thus, by implication, every portion of the hotel including the rooms booked by the clients would come within the definition of a public place. In addition, the legislature has used the words 'any other place intended for use by, or accessible to the public. This is a very wide definition of the term 'public place' and would include almost any place that is accessible to the public including offices, banks, chambers, hospitals and many others.

Section 80(2) of the IT Act further states that any entry, search or arrest subject to the provisions of section 80 of the IT Act shall be subject to the provisions of the BNSS, 2023. Therefore, according to section 80(1) of the IT Act, the legislature gave priority to the police force.

Section 81 deals with overriding effect of the Act. It states that the provisions of the IT Act shall have an effect, notwithstanding anything inconsistent therewith contained in any other law currently in force, this includes the BNSS, 2023.[23]

IT Amendment Act, 2008

Being the first legislation in the nation on technology, computers, e-commerce and e-communication, the Act was subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it to be too diluted and lenient. There were conspicuous omissions resulting in the investigators relying more and more on time tested BNS, 2023 even in technology-based cases with the IT Act also being referred in the process.

Thus, the need for an amendment was felt in the IT Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the IT Act and comparing it with similar legislation in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the IT Amendment Act, 2008 was placed in the parliament and passed without much debate. The Amendment Act got the president's assent on 5th Feb, 2009 and was effective from 27th October, 2009.

Some of the notable features of IT (Amendment) Act, 2008 are as follows:

[23]The Information Technology Act (No 21 of 2000), Section 81

 [ISSN 2581-5369]

- Focusing on data privacy
- Focusing on information security
- Making digital signature technology-neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team for the inclusion of additional cybercrimes like child pornography and cyber terrorism.

Additions to the IT Act in 2008 protects against identity theft under Section 66C[24] or cheating by impersonating online under Section 66D. Victims of revenge may register complaints for violation of their privacy under Section 66E [25] as also under Section 67[26] and Section 67B which provides for prosecution of pornography and child pornography respectively. In case of the latter, the provisions of the POCSO[27] Act may also be invoked.

As children are armed these days with cameras and data on their mobile phones with raging hormones at an increasing rate, the instances of revenge porn attacks by children against children are on the rise. Irrespective of the age of the accused, if the offence of circulating sexually explicit content or violating privacy through dissemination of images or videos of private parts, is committed, the person is susceptible to prosecution.

With respect to child pornography, the law is very stringent. It is not only publishing or transmission of child porn that is an offence, but even browsing for such content and retaining or downloading it is an offence too, unlike for pornography where only the dissemination and transmission, sale, etc. are considered offences. Further, actions intended to entice children through social media for creating child porn content or to record abuse of children and circulating the same are all offences punishable under the IT Act, 2000.

New clause applied to the I.T. Act, 2000 in the form of Section 67(A),[28]provides for penalties

[24]The Information Technology Act (Act 21 of 2000), Sec 66 C: Punishment for identity theft.– Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, 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 rupees one lakh

[25]The Information Technology Act (Act 21 of 2000), Sec 66 E: Punishment for violation of privacy.– Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

[26]The Information Technology Act (Act 21 of 2000), Sec 67

[27]The Protection of Children from Sexual Offences Act 2012 (Act No 32 of 2012)

[28]The Information Technology Act (No 21 of 2000), Section 67 A

 [ISSN 2581-5369]

for the publishing or transmission of material involving sexually explicit acts, etc., in electronic form. This is most important for teenagers. Trends in sharing pornographic content on mobile phones are on the rise and this Section plays a significant role in modern times.

IV. CONCLUSION

India is the home to the fourth highest number of internet users in the world. It comes third in amount of cybercrime cases after the United States and China. Not only this, India is also the second largest user of mobile phones after China and according to telephone regulation of India on 31st March, 2014, there are around 933 billion mobile users in India but of these, users are still unaware of what is cybercrime and how can one tackle with this serious issue.[29]

Yet technological development cannot be absolutely halted. In cope with culture, law enforcement agencies, private businesses and companies would all need to adjust. Tech experts are required to tackle these cyber issues. Furthermore, knowing such experts is not enough. They do need the requisite technological hardware and tools to battle cyber criminals efficiently. Thus, appropriate infrastructure must be built in different parts of the country to curb crime in the virtual environment. Another thing that needs to be addressed is that a tradition of ongoing preparation and development needs to be inculcated among law enforcement agencies as the world of information technology is quite diverse. Police force modernization in India is still needed.

The virtual space is at risk. To protect it, continue with mitigating the harm done and reducing the recovery period from cyber threats by developing cyber-attack-resistant systems, because it is really necessary to stand up on your feet and prevent more risk. Often the battle of cybercrimes is against an anonymous perpetrator or tracking the criminal's roots requires a tremendous period of time, making it really necessary to constantly stay on one's feet to be conscious of every assault. The assault would be on the nation's critical infrastructure, which holds a country's security network targeting a country's sovereignty, rendering it important for a government to make attempts to deter cyber threats on the country's critical infrastructure while keeping it invisible to cyber attackers.

Training, like in most situations often plays a very significant role in such crimes because the public should be trained about these crimes, and technologies immune to cybercrime should also be applied rising national susceptibility to cyber-attacks. As properly said, data has become the new oil, where all countries run after data to better understand the enemy country and by remotely tracking the actions of that country's people, it becomes very necessary that

[29]Supra Note 3.

 [ISSN 2581-5369]

networks and systems vital to national security are adequately secured and that an early watch and alert system is in place for potential cyber-assault attempts. Cyber threats in today's age, when digitalization is at its peak and the environment is available by clicking a click, and threatening to cripple the economy, great focus must be put on defending against concerted assaults capable of causing crippling economic harm. As of today, as technology reaches new heights, these assaults are still developing and getting even greater. Therefore, to combat these threats, continuous innovation and technological advancement must be made to allow vital infrastructure organizations to protect their IT properties. Such threats are highly sophisticated and need advanced techniques and skills to counter cybercrimes. There is also a need for more stringent deterrence that not only occurs, but is also converted into practice, such that potential cyber offenders can pause before targeting India. Currently, the crimes under the Information Technology Act, 2000 are bailable with 3year probation, and will become stricter, altering the mentality of computer offenders.

Cybercrime is a primary indicator of cross-border crime. The authority here is complex and vague. Thus, even the police face problem due to the uncertainty of the jurisdiction in which the case falls under. For example, it came into notice of a school teacher that an amount equal to Rs. 30,000 was withdrawn from his savings account without his consent and knowledge. The ATM from which the amount was withdrawn was located outside the city limits and some amount was withdrawn from the one located outside the state limits. In such a situation, it is confusing which jurisdiction he should file the complaint.

Though cybercrime legislation has been introduced, but there is a shortage of clarity about how to perform an investigation into cybercrimes. Cyber-crime cell and police station were both established to identify and prosecute these crimes. Combating with legal measures involves a multi-pronged strategy. With the arrival of cyber cells in various cosmopolitan cities in India, there is a significant need to build a high-tech crime investigation network along with highly trained personnel. Present cyber cells have a mix of police officers and IT experts. It also requires additional training to enhance the overall technological skills of police officers, rather than relying exclusively on cyber cells. [30]

Cyber terrorism violates civil rights. The count of cyber breaches intended to capture personal details is increasing. The perpetrators exploit personal information and benefit from their action and challenge the basic philosophy of 'right to live with integrity.' Because cyber criminals are practitioners of using new science and technology, it is very difficult to achieve

[30]Supra Note 5.

 [ISSN 2581-5369]

successful law enforcement. Technology often helps offenders. Efficient compliance is similarly challenged by cyberspace's transnational existence. Cyber offenders challenge sovereign nations' traditional jurisdictions.

Special cybercrime laws are required to deal with modern forms of crime and secure digital data which should include Intellectual Property Violations and Human Rights Abuses.

Within its security system, the government will create a special division of cybercrimes and intellectual property violations, so that compliance officials may take swift action against cybercrimes. All kinds of infrastructure facilities must be accessible to investigating officers, especially in terms of accessibility, communication, technological usage. Scientific preparation for investigating officers to deal with new problems within different enforcement departments that deal with cybercrimes.

The government provides good infrastructure and equipment for coping with cybercrimes to the Cyber Crime Cell and Cyber Crime Police Station. With inadequate services, police officers experience enormous challenges identifying and investigating crimes and sometimes feel helpless. The government should develop specialized cyber-labs and provide police with various levels of training such as sensitizing data security, recognizing cybercrime, knowing how to assess a crime scene and saving information, detecting digital evidence, understanding computer hardware, and storing data. By this it can be concluded that the rule cannot continue to remain stagnant, increasing conditions viz. cyberspace is all the more important, since certain technologies will be used to enhance society. The bottom line is that the legislation will be adaptive and it can quickly respond to society's demands and technical growth.

INTERPOL, the International Police Organization, can be used to quickly exchange information and materials needed to apprehend cyber criminals for their trans-border existence. In the lack of an extradition deal with a variety of nations, it became impossible to arrest computer offenders and obtain required details from other nations while illegal activities were carried out from other countries. Therefore, the government may consider taking INTERPOL's support as a matter of urgency. It is also planned to include necessary legal requirements in the proposed new legislation.

Alike Green Bench, a Separate Bench for coping with cybercrimes can be established at least in any high court. Unique divisions may also be established in any metropolis and district. Training and equipping judges, defense prosecutors and police authorities to cope with this latest transnational, nuanced, high-tech activity is of vital significance to consider investigation and litigation procedures specific to cybercrime. The argument raised by others,

 [ISSN 2581-5369]

i.e., a rule claiming extraterritorial authority in the modern universe is not enforceable, has some validity. Contrary to the concept of international law, claiming authority over residents of another country is likely to result in violation of sovereignty in various courts in separate national jurisdictions. This is, therefore, necessary to remember that state rules, judicial structures and practices vary.

Further compounding problem is that, a certain act in one national jurisdiction might be lawful and not prohibited by law but, at the same moment, it is unconstitutional and forbidden by law in another national jurisdiction. Another explanation for concern was that section 1 of IT Act, 2000 may not set the criterion on whether such law should be enforceable in effect through transnational borders and jurisdictions. Government can use the extradition mechanism to bring cybercriminals to their jurisdiction for prosecution if a legitimate extradition treaty exists between the countries concerned. Yet the path in section 1 of the IT Act, 2000 is expected to build a dynamic environment with complexities in real day-to-day execution.

In India, it was claimed that the need for the present law is attributed to the rise and expansion of cyberspace, which has no borders. As the internet makes history, it is crucial that nations adopt legislation that have an all-pervasive applicability and effect. Therefore, such a strategy allows nations to capture cybercriminals directly beyond national borders. On the other side, the clause is likely to be challenged in as far that no government should claim authority over another country's resident, merely because that person has broken another nation's national laws. The step was dismissed as opposite.

The Indian solution in section 1(2) as modified by section 75 IT Act has generated uncertainty in the real application of the legislation. It is much more apparent from the evolving concepts of multiple decisions on internet authority. Since the beginning, the question of authority has proceeded to test legal minds, cultures, and nations in the light of the internet's peculiarly intrinsic nature. Similar standards have been established in various regional jurisdictions. In conventional conceptions of jurisdiction, judges claimed authority depending on when the cause of action originated. Because of cyberspace's peculiarity, the well-established jurisdictional rules no longer offer clarification. Although acknowledging some of the obstacles the internet presents to jurisdiction law, the courts have sought to address problems by incorporating well-established legal standards.

Through an Indian viewpoint, given the entire problem of cybercrime control, there are far through defined concepts. Civil law authority, however, has been created. Such jurisprudence is still important and may aid with the development of cybercrime case law over time.

 [ISSN 2581-5369]

Existing foreign law on a country's sovereignty also specifies whether a sovereign entity may create legislation impacting citizens inside its boundaries. Nevertheless, the internet's emergence has seen geography becoming ancient, and network transfers become transnational in nature, complicating the whole jurisdiction problem.

*****

 [ISSN 2581-5369]