International Journal of Legal Expatiate Vol 1 (2021) Pg. 1-14
Published by Author Lens
ISSN: 2583-7885 (Online)

"Emerging Cyber Security Challenges and Problems: An Analysis of Jurisdictional Cybercrime"

-Varda Mone[*]

Abstract

The impact of the silicon revolution on the criminal law infrastructure has transcended national borders, transforming it from a tribal mandate to a mass of rule-making authority. When new paradigms emerge in the cyber world, technology progresses at such a dizzying pace, and criminal behaviour transcends continents and oceans, laws can no longer be local. International cooperation is required to address the growing threat of cybercrime. The human aspect of the internet cannot be disregarded; the two worlds cannot live happily ever after until the two worlds reconcile, unless the obduracy of legal dictums is loosened, and unless boorish online behaviour is brought within the legal web.

Key Words: *Cyber Security, Cyber Law, Data Protection, Privacy, Jurisdiction, Cybercrimes.*

I. INTRODUCTION:

A global revolution that moved the new century with an ever-unceasing reliance upon technology and particularly the internet. The pace of development was fastened and commerce crossed boundaries. Though it is a boon it is a curse as well since the percentage of cybercrimes has increased by 63% in 2019 According to the New Indian Express (2018), India is the 33rd most vulnerable country on the planet when it comes to cyber-threats. By 2025, India's digital transactions could surpass $1 trillion. A safe online environment for our citizens is now more important than ever in light of these alarming statistics. Therefore, it is necessary to bridge the gap between cyber laws and cybercrimes; the safety wall needs to be rebuilt with effective measures this time. The tech boom has had two effects on the criminal community: first, it has broadened the scope of criminal activity by giving it a global arena, and second, it has enabled non-deviant and previously inactive criminals to engage in new, primarily online illegal activities. Except in circumstances of strict liability, mensrea is an

[*] Research Scholar, VIT-AP School of Law, VIT-AP University.

essential ingredient of criminal liability. With the emergence of e-crimes, the legal system has encountered new challenges in establishing mens rea in cybercrimes.[1]

II. CHANGING TRENDS OF CYBER SECURITY:

Every online transaction necessitates the involvement of many intermediaries and may include two or more parties. The fact is true not only in case of e-commerce transactions but also in the entire crime line where the *"principal actors"* have something to contribute towards the crime although their liability may not arise in each case. Cyberspace is overflowing with all tiers of human society, including artists, statesmen, individuals, and so-called criminals. Without the intervention of human hands, the virtual world will cease to exist. Thus, even if a crime is committed in the most intangible setting, its perpetrators and criminals are still from the actual world. As the ripples of the wrongdoing are felt in the physical environment, the law cannot remain mute and the perpetrator must face the consequences. Before a criminal is brought to justice, legal laws demand that the perpetrator's culpability be established.

"In an important judgment passed by the Delhi High Court, where Jogesh the employee-defendant of the plaintiff's company had sent derogatory and defamatory e-mails to the employers and to other subsidiaries of the company in order to defame the company. As a consequence, the company terminated the employee. A suit was filed by the company for issuing a permanent injunction to restrain the defendant from sending such mails as it was maligning the reputation and goodwill of the company. The Delhi High Court passed an ex-parte ad interim injunction restraining the defendant from sending such derogatory e-mails. And the learned Delhi High Court restrained the defendant from publishing any information in the actual world or in cyberspace which is derogatory or defamatory to the plaintiff. The verdict was in itself historical as it was for the first time that an Indian Court assumed jurisdiction regarding a matter connected with cybercrime."[2]

These questions are significantly more prevalent in computer and internet crimes than they are in multinational or organised crime. The vast majority of Internet crimes, whether cyber stalking, unauthorised access, spamming, or any other form, are committed remotely, and frequently from another state or nation. Cybercriminal activity has extraterritorial aspects. In

[1] Hathaway, Melissa E., and John N. Stewart. "Taking Control of Our Cyber Future." Georgetown Journal of International Affairs, 2014, pp. 55–68.
[2] SMC Pneumatics (India) (P) Ltd. v. Jogesh Kwatra.

the context of the state, jurisdiction refers to the landmass within which the administrator's sovereign authority can be exercised. In respect to a court, jurisdiction is the territory and subject matter over which the court has the authority to take cognizance and try a case. The concept of a court's judicial jurisdiction derives from the sovereign and territorial theories of state.

III. JURISDICTIONAL ISSUES AND CHALLENGES IN CYBERCRIME:

Internet Jurisdiction as per *"lex loci delicti"* rule explains that Jurisdiction in cyberspace arises when one is online and is almost everywhere. While jurisdiction simply means limitation of some sort, be it subject matter related or territorial, in the internet age it means worldwide.

A webpage hosted on a computer server is accessible to anybody in the globe via the internet, and email sent through mass mailing list transmissions can reach people in numerous distinct jurisdictions, even if the transmitting party did not intend for someone from that country to be involved.

It was approved by the English Court in London's Queen's Division Bench of the Royal Court of Justice to serve process via email over the internet when service of process was to be transmitted by email. In *US* the pre-internet rules of jurisdiction emanate directly from which constitution, are being applied and the matter of internet jurisdiction. As Cybercrimes transcend the physical Frontiers, the question of Jurisdiction along with their trial is a complex one. There are offences which are not completed in one particular area but the nature is such that they are protected to a greater length of time and place like ticketless travelling, etc. In *India,* the applicability of legal rules to crimes committed in cyberspace is the interplay of several Acts. The Cr. PC of India takes note of all those various shades of offences and makes categorized provisions for them but Section 177 envisages the basic rule regarding the place of enquiry and trial. Thus, the most straightforward way to start a trial is to see the area or geographical limits within which the particular crime was committed and then to enquire and start trial in court having jurisdiction over such area. However, chapter XIII contains Section 178 - 186 and Section 188 which are meant to enlarge the ambit of "local jurisdiction" in which the enquiry or trial of offences might take place. This is to minimize the inconvenience and hardship which may result from strict adherence to the rule given in section 177. The rules laid down in this section "are not mutually exclusive but

cumulative in effect and intended to facilitate the prosecution of offenders by providing a wider choice of court for initiating the enquiry or trial". Apart from offences committed within India the CRPC also supplements Section 4 IPC[3] which contains the extension of the IPC to extraterritorial offences.

Section 4: provision of this code applies also to any offence committed by- 1. Any citizen of India in any place without and beyond India; 2. Any person on any shape or aircraft registered in India where ever it may be; 3. Any person in any place without and beyond India committing offences targeting computer resources located in India; The expression computer resource shall have the meaning as assigned to it in clause k of subsection 1 of section 2 of the information technology act 2000.

The extraterritorial extension of CrPC is twofold; firstly, it concerns the person or citizen of India and secondly, it concerns the place namely the aircraft and ship. In either case, the CrPC is applicable in the situation as if it is applied in Indian surroundings. The rule is further explained by the illustration appending to the section which says that whoever is a citizen of India commits a murder in Uganda he can be tried and convicted of murder in any place in India in which he may be found. The amendment to the section is meant to make it suitable for internet situations. It is a known fact that cybercrime or borderless crimes have defined the fundamentals of Jurisdiction yet they cannot be ignored by saying that. Hence it has been the effort of lawmakers to tailor the law according to the new demands with the same view the one and half-century-old provisions, namely, Section 4 of IPC has been amended accordingly. Thus, the section envisages the rule of extraterritorial jurisdiction. It underlines the three grounds for the exercise of Jurisdiction by Indian Court:

“1. The committer being an Indian citizen;

2. The place of commission being the territory of India.

3. The computer resource situated in India being targeted by anyone with or beyond India.”

Any place that comes within the Ambit of the word territory i.e., be it ship or aircraft registered in India, is covered by Section 4 for any of these Grounds are enough to give a legitimate exercise of judicial power to the Indian Courts.

The upcoming cyber legislation is meeting will infinitely change and development, be it issue of jurisdiction or any other issue. Such another untouched part is electronic evidences. Though, the first computer evidence offered in court was information generated by businesses. Long before computer became a household appliance telephone company and

[3] Indian Penal Code, 1860.

banks were using them to record, process and report information that their businesses required.[4]

But today things have changed much. Computers are no longer the exclusive appliance of commercial domains. They have reached the common men's table and thus they cover mines and mines of information stored in it, giving birth to critical legal issues. The long-standing doctrines, the traditional principles and the established legal norms look up for some change.[5] While on one hand, trite human acts are being registered digitally, passively or actively, and though a large amount of data is thus collected; the production of it in law courts and its admissibility as legal proof has become a formidable challenge. the effort less recording of facts in computer says that visiting the websites, giving a call, drawing money from ATMs, doing online shopping are all passive collection of evidence of some sort which may often, in the event of the Commission of some crime become useful material in prosecution.[6]

In fact, production of such information in criminal Court has given rise to the evidential problems. To make computer evidence more acceptable in law courts, there have been concerted efforts to legislate on the subject yet these have so far proved to be insufficient to deal with this problem of information technology criminal law. Not only that immense amount of data is stored but at the same time the new challenge is that it is deleted with as equal ease as it is gathered with. Encryption of files by user and their claim that they do not remember their password are yet add a problem which make the path of Investigation and prosecution all the more challenging.

On the basis of methodology adopted in extraction of the evidence the computer evidence can be divided into the following 3 categories:

1. *Real evidence* or evidence created by calculations or analysis generated by the computer itself through running of software and the receipt of information from the other devices such as built-in clocks and remote sensors.
2. *Hearsay evidence*; when some data is fed by human hand into the computer system and later the computer produces it on the basis of some command given to it then the kind of information produced is hearsay evidence.

[4] Reidenberg, Joel R. "Technology and Internet Jurisdiction." University of Pennsylvania Law Review, vol. 153, no. 6, 2005, pp. 1951–74.
[5] SESHU, GEETA. "Poor Guarantee of Online Freedom in India." Economic and Political Weekly, vol. 47, no. 24, 2012, pp. 14–16.
[6] Reidenberg, Joel R. "Technology and Internet Jurisdiction." University of Pennsylvania Law Review, vol. 153, no. 6, 2005, pp. 1951–74.

3. *Derived evidence*; which is a combination of real and hearsay evidence to form a composite record and which is also treated as hearsay evidence. Daily balance column of a bank statement is an example of this kind of evidence.

In United Kingdom Different treatment is given to computer generated evidence compared to other evidence. Hence, it is necessary to do a hearsay examination, a best evidence analysis and an authentication process before the court declares computer evidence "admissible." Article 9 of the Model Law on Electronic Commerce addresses, among other things, the admission and weight of evidence in data transmissions (1). As a signatory to the Model Law, India's legal system incorporates many of the concepts set forth therein. The traditional law defining the term evidence has been amended to include electronic evidence as well by amending section 3 of Indian evidence Act in the following manner:

"3. 'Evidence' means and includes:

(2) All documents including electronic records produced for the inspection of the court.

Another law i.e., The IT Act, 2000 gives legal recognition to the legal recognition of electronic record.

" 4. Legal Recognition of electronic records:

where any law provides the information or any other matter shall be in writing or in the type written or printed form , then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

A. Rendered or made available in an electronic form; and

B. Accessible so as to be usable for a subsequent reference."

Thus, Section 3 of the Evidence Act[7], and Section 4 and 65-B of the Information Technology Act, 2000 helps in legal recognition and admissibility of electronic evidences in the court of law. Though the legislation is not foolproof but it has started recognizing the admissibility of electronic evidences in the court to reach justice.[8]

Such another loophole in the cyber circuit is of data privacy and the raw regulations governing it as well as struggling to survive with the rapid development in the internet technology.

The shift of target point from the real wealth of the physical world to the virtual wealth, namely, the data and information of the cyber world is clear. Study and experience reveals about the greed of cyber criminals for data mines. The breach of privacy has made an individual a fully transparent entity, where privacy has emerged as a saleable commodity.

[7] Indian Evidence Act, 1872 S 3
[8] Law on Information Technology by Dr. Ishita Chatterjee.

IV. ROLE OF DATA IN CYBER SECURITY

The issue of data protection is important both intrinsically and instrumentally[9]. Intrinsically, a regime for data protection is synonymous with protection of informational privacy. As the Supreme Court observed in Puttaswamy, "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state." The establishment in India of a robust legislative framework for the protection of personal data is the essential prerequisite for the growth of data-driven innovation and entrepreneurship in the country. If India wants to lead its citizens and the rest of the world into a digital future that is committed to empowerment, experimentation, and equal access for everyone, it is necessary for the country to foster such creativity and entrepreneurial spirit. Both of these goals can only be accomplished with the help of a data protection law that has been carefully crafted.[10]

"The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable. Edward Snowden shocked the world with his disclosures about global surveillance. States are utilizing technology in the most imaginative ways particularly in view of increasing global terrorist attacks and heightened public safety concerns. One such technique being adopted by States is 'profiling'. The European Union Regulation of 2016 on data privacy defines 'Profiling' as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Such profiling can result in discrimination based on religion, ethnicity and caste. However, 'profiling' can also be used to further public interest and for the benefit of national security. The security environment, not only in our country, but throughout the world makes the safety of persons and the State a matter to be balanced

[9] WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA
[10] C. Satapathy. "Role of the State in the E-World." Economic and Political Weekly, vol. 35, no. 39, 2000, pp. 3493–97.

against this right to privacy". (Justice K.S. Puttaswamy and Ors. v. Union of India (UOI) and Ors. :)[11]

The processing of personal data has already grown widespread in both the public sector and the private sector, despite the fact that the shift toward a digital economy is currently under progress. Data is useful in and of itself, but it becomes even more valuable when it is shared, as this can lead to the establishment of significant efficiencies. The fact of today's digital environment is that practically every activity carried out by a single person requires some kind of data exchange or another. This is the case regardless of whether the activity is online or offline. Because of the Internet, completely new markets have emerged, including those that deal in the acquisition, organisation, and processing of personal information, either directly or as an essential component of their overall business strategy. As has been noted by the Supreme Court in Puttaswamy[12]

"Uber', the world's largest taxi company, owns no vehicles. 'Facebook', the world's most popular media owner, creates no content. 'Alibaba', the most valuable retailer, has no inventory. And 'Airbn', the world's largest accommodation provider, owns no real estate."

Even though there are some exceptions for things like national security, defence, public security, and so on, the General Data Protection Regulation (GDPR) of the European Union is an all-encompassing data protection framework that applies to the processing of personal data in any way, shape, or form, and to processing activities carried out by both the government and private entities. In the same vein, it continues to acknowledge and put into practice the fundamental data protection principles that are outlined in the OECD Guidelines. The General Data Protection Regulation (GDPR) of the EU takes a rights-based approach to the protection of personal data and puts the individual at the centre of the legal system. As a direct consequence of this, it imposes stringent controls on the handling of personal data both at the time of the data collection and after it has been obtained. In addition, the collection of certain types of personal data, also known as sensitive personal data (which includes information regarding a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health and sex life), is generally prohibited, with a few exceptions. Therefore, in order for processing to be both lawful and fair, the entity that collects personal data must comply with a wide variety of

[11] Justice K.S. Puttaswamy and Ors. v. Union of India (UOI) and Ors.: MANU/SC/1044/2017
[12] Supra Note 14.

principles, such as those of purpose specification, data minimization, data quality, security safeguards, and many others. Only then can processing be considered lawful and fair.[13]

Such another problem is of information vandalism. Where, viruses, worms, Trojan horse and logic bomb fall are under one armour as all are the cyber weapons to destroy digital information. All are the brainchild of cyber crook; all are the tools of vandalism. They all run on electrons, feed on technology and die or costly death. They are all illegal. The similarity thus, calls for almost common legal approach. Most of the major legal system of world cluster them under the term "vandalism", and make the provision to minimize the loss by providing the compensation relief to the victim or some even punish the accused criminally. Following discussion scrutinizes the why and wherefores of the difference in legal attitude as mentioned here.

The earliest legal response came from the US Congress, which, in 1986, passed the computer fraud and Abuse Act in an attempt to catch those responsible for the crime. Its primary objective is to safeguard the computers used by the federal government as well as those used by financial and medical institutions. A provision of the same Act prohibits the transmission of a programme, information, code, or commands to a computer or computer system with the intent to damage, or cause damage to, or to withhold or deny the use of a computer, computer service, or computer network, information, data, or programme. This includes the ability to withhold or deny the use of the computer. It is also against the law to transmit such information in a way that shows a wilful and wanton disregard for the substantial and unreasonable danger that it poses.

In UK though late in coming up with a specific provision in this area, has, however, applied successfully some of its traditional Acts to tackle the menace. The Criminal Damage Act, 1971 though an Act to contain the damage caused to tangible property was successfully interpreted and applied to the "unauthorized deletion and modification of Computer Based information" in the landmark judgment like Cox v. Riley[14]. Practical hardship arose in getting such results, thus Computer Misuse Act, of 1990 contains specific provision to deal with the

[13] O'Neil, Michael. "Cyber Crime Dilemma: Is Possible to Guarantee Both Security and Privacy?" The Brookings Review, vol. 19, no. 1, 2001, pp. 28–31.
[14] *COX v. RILEY*, CIVIL ACTION NO. 5:10CV-P121-R (W.D. Ky. Sep. 24, 2010)

menace of viruses and worms. Section 3 of the Act deals with the situation under the name of "unauthorized modification" of the computer material it is made a substantial offence.[15]

The law came in a wake of the loss caused by virus distribution and hence, was much made to suit the requirements. The Indian law to deal with the virus situation is given in Section 43 dealing with the damage to computer, computer system, etc. As it is clear from the wording of the Act, it is civil law provisions which remedy the wrong by paying compensation to the victim instead of penalizing the defendant. Moreover, it being a Civil wrong, the question of intention does not arise and strict reading of the section reveals that mere introduction of virus or contaminant is enough to complete the wrongful act.[16]

PROTECTION OF PRIVACY UNDER CYBER LAWS

In the Revolutionary cyber age breach of privacy has made an individual of fully transparent entity and privacy has evolved from a right close to heart to a marketable commodity. Today cyberspace is embedded with a rich trove of personal data and privacy has emerged as a saleable commodity. Privacy on web is largest concern today. Certain technological devices play a crucial role in commodifying personal data. Breach of privacy also estranges the employer-employee relationship whereas and employees work performance etc along with his email can be electronically scanned. Technological advancements have left no secrecy privacy for an individual. Right to privacy like any other right is not absolute; disclosure of personal information is justified under certain circumstances. In the age of Information Technology right to privacy may be influenced by the following ways:

1. Utilizing Private data for the purpose other than that for which it is collected.

2. Sending of unsolicited email or spamming.

3. Unauthorized reading of emails of employees etc.

Much before the technological proliferation, privacy was valued as right and efforts were made to secure it. In 1948, The UDHR[17] in Article 12 states: neither one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack on attack on his honour or reputation. Everyone has the right to protection of the law against

[15] FATIMA Tatat, Cyber Crimes, EASTERN BOOK COMPANY 2012
[16] Allen, Jeffrey. "TECHNOLOGY AND ETHICS: A DOUBLE-EDGED SWORD." GP Solo, vol. 27, no. 7, 2010, pp. 34–39.
[17] Universal Declaration of Human Rights A12

such interferences or attacks. In India the right to privacy is nonetheless treasured and cherished, yet it is still to find a place of pride in law books. Though Indian Judiciary has culled this valuable right out of Article 21 of constitution, yet legislation to that effect is long overdue. Under the lone Cyber Act of the country, "privacy" is mentioned at two places in two different contexts which can be characterized as: Firstly, right to privacy under Section 72 which envisages the breach of confidentiality. This section the confers criminal liability on the interceptor. So far privacy meant privacy of personal details and maintaining secrecy, having the option to live according to one's own wish.

The common understood term namely, "breach of privacy" entails the dispelling of personal information to others, without the knowledge or consent of person concerned or consent of person concerned consent of person concerned. However, the amended IT Act introduces a new concept of privacy though original is well known but its representation in law provision is unprecedented. Secondly, the amendment of IT Act talks of privacy which can be termed as physical privacy as envisaged in the newly inserted section 66E. The new section makes it an offence to publish the private and Physical image of person through electronic medium. Nations with high connectivity responded in a similar manner and they are able to have able to have similar manner and they are able to have able to have some control over privacy breach and are able to pin down the wrongdoers to some extent. The Acts of UK and US namely the ECPA and DPA and envisages eight principles formulated by the OECD regarding personal data protection and also inspired by the UNHR declaration of 1948. The UK law addresses the data controller and the IT Act 2000 refers to "any person who in pursuance of any of the power conferred under this Act", The US law in section 25(1) (a) uses the word "anyone" thereby enlarging the grip of law over commoners or over another perpetrator Thus, the US law has a broader application as it not only brings authorized person within its purview but also anyone who intercepts the data. The consent factor is common in the law provisions of the three countries which reminds one that the consent factor is already recognized in OECD principles and in some other international instruments. The US law seems to be exhaustive and extensive as it is particularly privacy-specific legislation just like the UK law.

The Indian provision even after the amendment and insertion of Section 66E relating to privacy does not cover all areas relating to individual privacy. Section 72 is deficient in more than one way as understandably it is only a brief and isolated law provision regarding internet

privacy as a right. Though we had amidst vulnerabilities, the fire fire-spewing dragon of Cyber terrorism is still at a safe distance and the entire scenario is overhyped. Nevertheless, the situation is alarming and urges one to be prepared.[18]

There exists another loophole as the accountability of published sources lies absurd. The need to develop laws enforcing accountability of social media platforms is an alarming need of the time. The digital site, in contrast to traditional forms of media, which are subject to extensive regulation, presents opportunities for unethical behaviour due to the absence of rules that must be followed and the ability to conceal the identities of owners and editors, as is the case with websites that publish fake news. There is a lack of awareness regarding the culpability and trustworthiness of the content that is being hosted on their individual websites due to the absence of such essential information. The capacity to maintain one's anonymity while operating under the cover of a media source is the primary advantage enjoyed by those who generate fake news. The vast majority of online news outlets do not provide any fundamental information about the registered firm, including the editor, publisher, or physical address of the business.

Posting fake news on social media involved three parties: firstly, the person who publishes the information, secondly, the service provider that hosts the platform and thirdly, those who share and forward the post. Despite the fact that the proliferation of fake news is neither new nor recent, its capacity to reach people has increased as a direct result of the proliferation of online platforms and applications that are available to consumers at no cost. Users who create content that promotes hatred and then share it with others can be prosecuted under the appropriate section of the Indian penal code; however, due to the vastness of the Internet and the anonymity it provides, it is extremely difficult to track down individuals who engage in such behaviour.

When directed against the state, any form of speech can be considered an act of sedition and be punished as such under Section 124A of the Indian Penal Code. On the other hand, Section 153A of the Indian Penal Code prohibits and punishes the promotion of enmity between different groups on the basis of religion, etc. Instances of the spread of any remark or rumour that causes public mischief and animosity amongst classes, as well as intentional and malicious acts meant to offend the religious feelings of any class by insulting its religion, are both illegal under the Indian Penal Code (IPC). However, the Information Technology Act imposes limited liability on intermediaries like search engines and social media giants like

[18] FATIMA Tatat, Cyber Crimes, EASTERN BOOK COMPANY 2012

Google, Facebook, and WhatsApp for providing a platform to any content that is objectionable. At the same time, the Act exempts intermediaries from liability for any content provided by third parties. They are required by Section 79 of the Information Technology Act to remove any content that falls under this category in response to takedown notifications issued by various government bodies. Despite this, in the absence of adequate legislation, the government, law enforcement agencies, and district magistrates are increasingly making use of the expansive authority granted to them by the Code of Criminal Procedure 1973 in an effort to stop individuals from committing acts that would violate the peace or disrupt the tranquilly of the public.[19]

The most challenging class for the enforcement of Cybercrimes are the law enforces or the investigators. Securing conviction in the real-world crime is still not the total success of law enforcers; the intangible crime has left the bewildered. The first thing which is required by them are the law provisions giving them more and more powers enlarged on technical lines to investigate such crimes. The second thing is technical training which is lacked by a good many. The internet has a global face. It is junction where all the national laws of various nations intermingle. It is often said and rightly, so that the cyberspace with its queer features call for a legal regime of its own legal principles, cyber jurisprudence and sanction of its own. But that is not easy. Though invisible by nature and committed in unseen surroundings, the effect of cybercrime is felt in the physical world. More importantly the human hand is responsible for the illegal automated activities which call for booking the culprit and the wrongdoer to face the legal consequences. Nations have reacted towards the illegal conduct online by legislating some in a lukewarm manner and some vigorously.[20]

The most possible way to tackle these crimes is not to let them take place at all, in other words, preventing these crimes is an easier and better option though "it should not appear that crime prevention is a complete solution. It is one of the strategies, for total crime prevention that is infeasible and unachievable. Such prevention falls under technological prevention, better policing and an educated approach.

CONCLUSION:

As was made abundantly clear in the pages that came before this one, cyberattacks aimed at vital information infrastructures in India, such as those in the energy sector, the financial

[19] Bharuka, Devashish. “INDIAN INFORMATION TECHNOLOGY ACT, 2000 CRIMINAL PROSECUTION MADE EASY FOR CYBER PSYCHOS.” Journal of the Indian Law Institute, vol. 44, no. 3, 2002, pp. 354–79.
[20] Bharuka, Devashish. “INDIAN INFORMATION TECHNOLOGY ACT, 2000 CRIMINAL PROSECUTION MADE EASY FOR CYBER PSYCHOS.” Journal of the Indian Law Institute, vol. 44, no. 3, 2002, pp. 354–79.

services sector, the defence sector, and the telecommunications sector, have the potential to have a negative impact on the economy of the country as well as on public safety. The protection of the essential information infrastructure has emerged as a primary concern with respect to national security, and this shift in emphasis is consistent with the policies that have already been implemented by other digital nations. Indeed, the ever-increasing interdependence of the digital sphere, across borders, has prompted the emergence of cybersecurity as a major component of national security strategies in states across the globe. India should not wait to follow in the footsteps of other nations and should immediately begin implementing cybersecurity measures.

References:

Allen, Jeffrey. "TECHNOLOGY AND ETHICS: A DOUBLE-EDGED SWORD." GP Solo, vol. 27, no. 7, 2010, pp. 34–39.

Bharuka, Devashish. "INDIAN INFORMATION TECHNOLOGY ACT, 2000 CRIMINAL PROSECUTION MADE EASY FOR CYBER PSYCHOS." Journal of the Indian Law Institute, vol. 44, no. 3, 2002, pp. 354–79.

Bharuka, Devashish. "INDIAN INFORMATION TECHNOLOGY ACT, 2000 CRIMINAL PROSECUTION MADE EASY FOR CYBER PSYCHOS." Journal of the Indian Law Institute, vol. 44, no. 3, 2002, pp. 354–79.

C. Satapathy. "Role of the State in the E-World." Economic and Political Weekly, vol. 35, no. 39, 2000, pp. 3493–97.

FATIMA Tatat, Cyber Crimes, EASTERN BOOK COMPANY 2012

Hathaway, Melissa E., and John N. Stewart. "Taking Control of Our Cyber Future." Georgetown Journal of International Affairs, 2014, pp. 55–68.

O'Neil, Michael. "Cyber Crime Dilemma: Is Possible to Guarantee Both Security and Privacy?" The Brookings Review, vol. 19, no. 1, 2001, pp. 28–31.

Reidenberg, Joel R. "Technology and Internet Jurisdiction." University of Pennsylvania Law Review, vol. 153, no. 6, 2005, pp. 1951–74.

SESHU, GEETA. "Poor Guarantee of Online Freedom in India." Economic and Political Weekly, vol. 47, no. 24, 2012, pp. 14–16.

WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA