DE JURE NEXUS LAW JOURNAL

Author:

Ashriya Kanojia

Symbiosis Law School, Noida

2nd Year, BA LL.B.

EFFECTIVENESS OF CYBER LAW ENFORCEMENT AGENCIES IN TODAY'S TECHNOLOGY DRIVEN WORLD

INTRODUCTION-

When the Internet was first conceived, the founders of the Internet had no idea that it would grow into an all-encompassing revolution that might be used for criminal purposes and would demand control. There are a lot of disturbing things going on in cyberspace these days. Because of the Internet's anonymous character, it is easy to participate in a wide range of criminal actions with anonymity, and those with intellect have been badly utilizing this aspect of the Internet to conduct illicit operations in cyberspace. As a result, India requires Cyberlaws.[1]

The legal difficulties involving the use of communications technology, notably "cyberspace," i.e. the Internet. It is an intersection of numerous legal topics, including intellectual property, privacy, freedom of expression, and jurisdiction, rather than an unique field of law like property or contract. In essence, cyber law seeks to reconcile the issues posed by human behavior on the Internet with the historical legal framework that governs the physical world.

[1] Harshit Agarwal, Cyber security laws in India, APKNOX (July 31st, 2021, 10:00 AM), https://www.appknox.com/blog/cybersecurity-laws-in-india

Cyberlaw is significant because it encompasses nearly all elements of transactions and activities on and with the Internet, the World Wide Web, and Cyberspace. At first glance, Cyberlaws may appear to be a highly technical area with little relevance to ordinary Cyberspace operations. The truth, on the other hand, is that nothing could be further from the truth.

THE HISTORICAL ASPECT OF CYBER CRIMES-

It is impossible to deny that the internet has had a profound impact on our lives. The Internet has evolved into a useful medium of communication that allows for speedier information transmission. Cybercrime, like any other type of crime, has a long and tumultuous history.

➢ **Between the 1870s until the early 1980s-**

- The first cases of superficial hacking can be dated back to the 1870s, when telephonic phreaking was used to manipulate the masses (Hacking long-distance telephone networks illegally in order to make free telephone calls). Because the internet began in the United States, it was here that the first computer-assisted crime occurred in 1969. It's also worth noting that Hesse passed the world's first computer-specific law (German state). To control cyber technology, the Data Protection Act of 1970 was enacted.[2]
- By the end of the 1970s, cyber pornography had progressed as well. This cybercrime poses a legal dilemma not only for India, but also for a number of other countries around the world. The Inter Networking Working Group was established in 1972 with the goal of regulating Internet standards. In a weekly class offered by author Len Adleman in 1983, the first known computer "virus" was designed and tested.

➢ **From the late 1980s to the early 1990s-**

- Two suspected hackers were engaged in the case of R. v. Gold ([1988] 2 WLR 984). They were journalists given access to British Telecom Prestel Gold's computer server, and they altered data without authorization.[3]
- Another noteworthy case is United States of America v. Jake Baker and Arthur Gonda [(1995) 890 F.Supp, 1375 (E.D. Mich)], in which the defendants were held responsible for threatening and abduction using offensive information. This became a landmark case because the entire episode was assisted by electronic means.[4]
- In the case of Yahoo, Inc v. Akash Arora [(1999) 19 PTC 229 (Delhi), India had its first brush with cyberrcrime in 1999. Yahoo essentially filed a lawsuit seeking a permanent injunction to prevent the defendants and their partners, agents, or servants from using the

[2] Isha Upadhayay,Cyber law:A comprehensive guide for 2021, JIGSAW ACADEMY (July 31st, 2021, 11:30 AM)
[3] R. v. Gold ([1988] 2 WLR 984
[4] United States of America v. Jake Baker and Arthur Gonda [(1995) 890 F.Supp, 1375 (E.D. Mich)

domain name 'Yahooindia.com' for commercial purposes. The Court clearly stated that other entities cannot use the Yahoo! trademark because it deludes customers.[5]

- **The Past Decade- since 2000-**

The Indian Parliament ultimately passed a law to tackle cybercrime in the year 2000. The Information Technology Act (ITA) of 2000 was enacted with the sole purpose of establishing a legal framework for business transactions conducted via the internet.

- The Indian judiciary, in Rediff Communications Ltd. V. Cyberbooth (AIR 2000 Bom 27), took note of the large number of instances involving trademark infringements and reaffirmed the Yahoo! decision. Before tackling cybercrime, it was realised that a slew of concerns needed to be addressed. However, between 2004 and 2005, data breaches became more common, posing a serious threat to businesses. By stealing data or gaining unauthorized access to client information, cybercriminals began causing massive losses to organisations. Some people began doing it professionally, as well as promoting it. As a result, the majority of cybercrimes performed during this period of time were aimed at enticing money as well as the development of professional skills.[6]
- In 2010, a large cyberattack known as "Operation Aurora" occurred. Google, as well as big corporations such as Yahoo, Adobe Systems, and Symantec, were also targeted.

CYBER LAWS IN INDIA-

It was critical to comprehend the historical context in which India's government was urged to pass the Information Technology Act of 2000.

The main goals of the Act are stated in the preface. They are as follows:

- to offer the legal status that electronic business activities carried out through electronic communications require. Electronic storage facilities are used as a substitute to the paper-based documentation storage system in such transactions.
- to make it easier to file documents electronically with government entities as well as in a court room

[5] , Inc v. Akash Arora [(1999) 19 PTC 229 (Delhi), India
[6] Rediff Communications Ltd. V. Cyberbooth (AIR 2000 Bom 27)

- to alter India's existing criminal laws as well as a few particular laws The Indian Penal Code, the Bankers' Books Evidence Act, 1891, the Indian Evidence Act, 1872, and the Reserve Bank of India Act, 1934, were all updated by the IT Act of 2000.[7]

The IT Act focuses mostly on the following areas:

- Legal identification of electronic documents.
- Justice Dispensation Systems for cyber crimes
- Legal Recognition of Digital Signatures
- Offences and Contraventions [8]

It's worth noting that the Information Technology Act of 2000 doesn't give a clear overview to the word "cybercrime." This aspect was overlooked even after the modifications.

EFFECTIVENESS OF CYBER LAWS IN INDIA-

We talk about privacy and its importance on a daily basis in contemporary era. Cybercrime is defined as any crime that involves the use of a computer or network system as the object of the crime or as a tool for committing the crime. Cybercriminals may utilise any method to obtain personal details, trade secrets, or for other harmful objectives. The most basic educational question is what to do if a cyberattack occurs, which may include financial fraud, cyber bullying, or any other type of cybercrime. We've seen a tremendous spike in cyber-crime in India, due to increased internet and smartphone use, which has resulted in a number of unsolved instances. In India, the Community Emergency Response Team (CERT) is the institution in charge of collecting, analyzing, forecasting, and alerting for cyber occurrences. The incident could be reported on their website.[9]

The “Aurora Generator Test,” a 2007 experiment in which researchers discovered that by remotely modifying the software of a power generator, they could cause the turbines to catch fire, causing catastrophic damage to the generator. Cyber terrorists pose a serious threat to Industrial Control Systems (ICS) and Building Control Systems (BCS) in situations like these. The question then becomes what kind of forensics could be performed and how similar cyber-attacks may be avoided in the future.

[7] I. Prateek Singh, Cyber Law in India: It Act 2000, LEGAL SERVICE INDIA E-JOURNAL, (July 31st, 2021, 1:00 PM) https://www.legalserviceindia.com/legal/article-836-cyber-law-in-india-it-act-2000.html

[8] Hardik Mishra, Cyber Law in India – Meaning, Introduction, History, Need, Important terms and Amendments, LEGAL DESIRE. COM (July 31st, 2021, 3:00 PM) https://legaldesire.com/cyber-law-in-india-meaning-introduction-history-need-important-terms-and-amendments/

[9] Vinit Verma, Importance of Cyber Law in India, LEGAL SERVICE INDIA E-JOURNAL, (July 31st, 2021, 4:00 PM) https://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html

Cyber terrorism is the fastest-growing concern, posing a threat not just to individuals or organisations, but also to nations as a whole. We must ensure that the proper prevention strategies are considered. Because there are no quick answers, and depending on the intensity of the cyber-attack, determining the solutions to these two questions could take weeks or even months.[10]

This is due to a lack of resources or desire on the part of the individual or the organisation. The answers could be discovered through a variety of in-depth vulnerability assessment techniques. This entails doing reconnaissance on possible risks as well as handling existing hazards appropriately.

Creating a security culture is an effective strategy to address these issues. The term "security culture" refers to a set of principles that everyone in a business share in terms of cyber security. This influences how one should think about it. Building a strong security culture will result in a more security-conscious workforce and promote the desirable security behaviors among employees.[11]

A brief checklist of dos and don'ts that might assist the organisation in developing a safety culture. As previously stated, culture swallows' strategy for breakfast, and once fully applied, 80-90 percent of attacks might be avoided.

Government and legislators are working hard to ensure that technology progresses in a rational manner and is used for moral and constitutional corporate growth rather than criminal activity. It takes real effort to change human behavior, which is easier said than done.

To begin, government and business leaders should form partnerships and begin creating recognition, as well as organise events such as Capture the Flag (CTF) activities and problem statements for hackathons on cyber security.

Cybercrime and Effective Cyber Law Enforcement

It's uncommon these days to open a newspaper (printed or digital) and not come across a piece concerning cybercrime. Cybercriminals are hacking into databases, stealing credit and debit card account, compromising people's identities, and shutting down legal websites numbers, compromising individuals' identities, and shutting down legitimate websites. Despite the fact that data security costs are increasing and computer users are becoming more aware of security standards, cybercrime continues to rise. Local law enforcement agencies appear powerless to

[10] Swati Shalini, How effective are Cyber Laws in India?, MY ADVO (July 31st, 2021, 6:30 PM) https://www.myadvo.in/blog/How-effective-are-Cyber-Laws-in-India/

[11] Pavan Duggal, India needs a dedicated cyber security law, THE TRIBUNE, (July 31st, 2021, 8:45 PM), https://www.tribuneindia.com/news/punjab/india-needs-a-dedicated-cyber-security-law-216669

combat this form of crime or criminal, and even the most advanced national and international crime-fighting organisations find it difficult to combat cybercrime.[12]

The Police Executive Research Forum recently released a research that examines the tactics, attitudes, and performance of nearly 230 law enforcement departments. Taken as a whole, it's hardly an image that inspires trust. Local and state governments must acknowledge that the last 50 years of crime-fighting triumphs are not training us for the criminal acts of this millennium, the paper states.

Traditional crimes, like everything else in the modern world, have moved online, from robberies to tax fraud, from sex and drug trafficking to intimidation and larceny. As a result of cybercriminal behavior, untold millions of citizens across the country and around the world have already experienced delays, inconveniences, and economic difficulties.

In fact, cybercrime is so widespread that law enforcement organisations are compelled to concentrate almost solely on the rare "high-loss" cases, or situations in which a pattern of pretty trivial offences points to a major instigator or mastermind. Single-instance crimes, such as falsified concert or game tickets and petty thefts, are usually investigated by local police. As a result, local gangs and small-time criminals are increasingly discovering that internet illicit activities pay better and have a lower risk of detection and penalty than traditional street crime.[13]

The reimbursement gap between cybercrime and street crime is significant. When a thief steals your wallet, you almost always have to absorb the loss on your own. However, if the same criminal steals your card number online, your bank will usually protect you from the crime. As a result, people are sometimes less compelled to protect and safeguard their online actions than they might otherwise be.[14]

Other differences are also important. However, there is no necessity for proximity in cybercrime. This poses jurisdictional issues and necessitates much more law enforcement resources. Cybercrime is also quite easy to scale. A lone hacker has the ability to assault millions of computers all around the world. As a consequence, a huge cybercrime binge can occur before authorities notice, and the criminal can vanish before authorities notice.[15]

Local police departments are increasingly using "training up" to better educate their sworn officers on how to combat internet crime as a response to this scenario. However, it appears that

[12] Karnika Seth, Evolving Strategies for the Enforcement of Cyberlaws, KARNIKASETH.COM, (August 1st, 2021, 12:30 PM), https://www.karnikaseth.com/evolving-strategies-for-the-enforcement-of-cyberlaws.html

[13] Adv. Partha Misra, Cyber Investigation - How Prepared are the Indian Police?, HG LEGAL RESOURCES. ORG, (August 1st, 1:45 PM)

[14] Karnika Seth, Cyber crimes and the arm of Law – An Indian Perspective, SETH ASSOCIATES, (August 1st, 2021, 3:00 PM)

[15] Nalini R, Prevention of Cyber Crime : A Legal Issue, LEGAL SERVICE INDIA E-JOURNAL, (August 1st, 2021, 5:45 PM)

this is the exception to the rule. It's unclear whether cyber law enforcement officers will ever be as vigilant in cyberspace as standard law enforcement officers are in offline financial districts.

CONCLUSION-

People can use the internet and cyberspace to conduct a wide range of transactions that can help them do business, save time, and gain access to a vast amount of information. Despite some flaws, these cyber laws give enough security against cybercrime. Nonetheless, the Acts have a large opportunity for change, and there is a need for effective provisions as well as successful implementation of these provisions. The battle against cybercrime has begun, but legal instruments are required to effectively combat the problem. While some issues will always exist because cyberspace is relatively open and some level of vulnerability will always be present, they cannot be completely eliminated. As a result, ethical use of cyberspace is promoted. The legal machinery's efforts must be in step with the instances and meet the public's aspirations. In order to check the offences rate, the conviction rate needs to be improved.

As a result, it will be up to legislators to assure that the regulatory rules of technology maintain pace with rapid trends and emerging cybercrimes.