EMERGING TECHNOLOGIES AND LAW WITH SPECIAL REFERENCE TO CYBER CRIMES

Author: Akshaya Desai
Amity Law School
Amity University

Abstract

New technologies and so-called communication and information technologies are trans- forming our society, the way in which we relate to each other, and the way we understand the world. By a wider extension, they are also influencing the world of law. That is why technologies will have a huge impact on society in the coming years and will bring new challenges and legal challenges to the legal sector worldwide. On the other hand, the new communications era also brings with it a number of new legal concerns, like those resulting from e-commerce and payment services, intellectual property, or the issues resulting from young people's use of new technology. Undoubtedly, this will have an impact on how law develops, changes, and is understood. This Special Issue has evolved into a window into the fresh legal issues presented by emerging technologies.

Keywords: Technology, Law, Cyber Security, Cyber Crimes

Introduction

The development of new knowledge technologies across all disciplines, as well as its application for economic or social advantage, are crucial steps in the advancement of society at large. Its growth has been crucial for the convergence of the social and economic spheres globally. However, all nation's legal systems need to address the regulation and legal ramifications of these new technology. Therefore, legal systems should pay special attention to the legal challenges that new technologies can provide in order to regulate the fundamental principles that ensure people's equality and rights. This includes, for example, Cyber Security, Cyber Bullying, blockchain technology in the future of contracts, and the protection of personal data;

Research Methodology

For the conducted research, the qualitative research methodology is applied. The primary source of information for the study is secondary data. A lot of research and studies are being conducted globally to identify the full range of repercussions of cybercrime because it is an increasingly serious danger. As a result, the study topic (Cybercrime) has access to the pertinent literature, which contributes to the generation of pertinent secondary data. The descriptive research method is quite beneficial for this study because it aims to describe the cybercrime phenomena in great detail. Similar to this, a thorough study is done on the many sorts of crimes, difficulties, anti-cybercrime tactics, and the state of cybercrime globally. Numerous journal papers are employed as the secondary information source to research the phenomena of cybercrime. The qualitative research method is chosen instead of the quantitative research method. However, it attempts to examine the current state of knowledge regarding cybercrime and make relevant conclusions based on the readily available secondary data. The study's findings are supported by secondary data.

Types of Cybercrime

Cybercrime is "unlawful conduct wherein the computer is either a tool or target or both". Cyber criminals are those who intentionally conduct a cybercrime. Cybercriminals include motivated criminals, organised hackers, disgruntled employees, and cyber terrorists. Cybercrime includes non-delivery of products or services, computer intrusions (hacking), intellectual property rights abuses, economic espionage (stealing of trade secrets), online extortion, international money laundering, identity theft, and a growing number of Internet-facilitated offences. The crime method and where and when it was committed are also difficult to determine. Internet anonymity makes it ideal for organised crime.[1]

1) Hacking & Cracking

Hackers are computer and programming experts who know every aspect of a system. Hacking is lawful. A cracker is an illegal hacker. Data theft, bank account changes. Thus, all crackers are hackers but not all hackers are crackers.

Hacking is breaking into computers and networks. Hackers attack target computers with custom or pre-made programmes. Destructiveness thrills them. Some hackers steal credit card information, move money from bank accounts to their own account, and withdraw money. Crackers can steal data or install viruses or worms that damage the system. Web hijacking involves hacking a website and gaining control.

2) Unauthorized Access

Unauthorized Access occurs when a user without permission enters a system. Hacking is the common term. Access means entering, instructing, or communicating with a computer, computer system, or computer network's logical, arithmetic, or memory function resources. Thus, any access without permission from the owner or manager of a computer, computer system, or computer network is unauthorized.

3) Phishing

Phishing is a cybercrime in which someone pretends to be a legitimate institution and contacts a target by email, phone, or text to get personal information, banking and credit card details, and passwords. Accessing important accounts with the information can lead to identity theft and financial loss. Emailing a fake company. Usually with a threat or request for information. An account will close, a balance is due, or account information is missing.

Responding to a phishing email that requires immediate action is phishing. Phishing emails request: Attaching. Word macros.

[1] Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security, 30(8), 803– 814.

4) Software Piracy

Software piracy is the purposeful or unintentional copying, distributing, sharing, selling, or using of software. Copying and selling. "Software piracy" is this. Most countries consider this copyright violation and doubtful fair use or fair dealing if the content is commercially available. Some nations allow the sale of versions customised for blind persons, students (for educational products), or similar. Some jurisdictions' copyright laws may also invalidate it. Renting original software. Software licences restrict a buyer's right to lend a copyrighted material. Some nations require authorization from the copyright owners to rent software. Piracy is a crime because a software pirate steals software without permission.

5) Forgery

Advanced computers, printers, and scanners can forge currency notes, postage and revenue stamps, mark sheets, and more. Forgery includes impersonation.

6) eCommerce/Investment Fraud

Sales/Investment scams. An offering that uses false or fraudulent claims to solicit investments or loans or that sells, uses, or trades counterfeit securities. Online orders never arrive. Internet auction site fraud caused by misrepresentation or non-delivery of products. This scam promises abnormally high earnings to investors.

7) Crime Against Individuals:

Cybercrimes against individuals include transmission of child pornography, harassment of anyone via computer, cyber defamation, hacking, indecent exposure, email spoofing, Net Extortion, Malicious code, trafficking, distribution, posting, phishing, credit card fraud, and dissemination of obscene material, including software piracy. Such a crime could injure an individual more than anything else.

8) Crime Against Property:

Cybercrimes against all property are another category. These crimes include computer vandalism, IP theft, threatening, and salami attacks. Financial institutions and financial crimes often commit this type of crime. This offence is notable because the amendment is so small that it would normally go unnoticed.

9) Crime Against Government:

Treason betraying a nation or sovereign by committing acts that endanger security. Most crimes target specific people or property, but some target the federal government or country as a whole. These crimes violate federal law and are tried in federal court. Treason, espionage, voter intimidation, and terrorism are covered in FindLaw's Government Crimes section. Convictions for these acts can be severe because they may threaten national security. Continue reading about government crimes.

Impact of Cybercrime

Computer technology has downsides. Though it makes life faster and easier, it's threatened by the deadliest sort of crime, cybercrime. Without computers, businesses and governments would nearly cease to function. Cheap, powerful, user-friendly computers have allowed more people to utilise and, more significantly, depend on them. Criminals use them more as enterprises, government entities, and individuals do. Cybercrime may be limited through analysing their behaviour and comprehending their effects on society.[2]

Challenges in Cybercrime:

- Cybercrime pros and downsides are often debated. We face several cybercrime challenges. Below are some:
- Lack of individual and corporate cyber security awareness and culture.
- Untrained personnel to implement countermeasures.
- No email accounts for military, police, and security professionals.
- Terrorists and hostile neighbours have launched cyberattacks against us.
- Police are almost ignorant in cybercrime because they don't need computer skills to join.
- Cyber technology advances faster than the government sector, making it impossible to trace cybercrimes.
- Security and law enforcement cannot handle high-tech crimes.
- Current protocols are unable to investigate international crimes.[3]

Monitoring and preventing these issues is possible. Online space must govern data use and clearly identify when user data will be shared to solve data theft. The user can opt out, limiting personal data to the intended space. Cybercriminals can steal personal data from software with bugs or viruses. Large technology firms should collaborate on customer security solutions. Security measures should start at the application level, where such scams are quickly detected. Firms are susceptible without coordinated monitoring. Data may be protected by monitoring every network for changes.[4]

Laws concerning Cybercrimes in India?

1) Information Technology Act

The Information Technology Act, written in 2000, oversees Indian cyber law. The main driving force behind this Act is to provide trustworthy legal inclusivity to eCommerce, making it easier to register real-time records with the government. But as cyberattackers became more cunning and people began to abuse technology, a number of changes were made. The ITA, passed by the Indian Parliament, emphasises the severe fines and punishments protecting the e-government, e-banking, and e-commerce industries. The scope of ITA has now been expanded to include all contemporary communication technologies. The key piece of Indian law that directs strict regulation of cybercrimes is the IT Act:

- People who harm computer systems without the owner's consent are subject under Section 43.
- If someone is discovered to have committed any of the acts listed in section 43 dishonestly or fraudulently, section 66 may be applicable.

[2] Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74

[3] Speer, D. L. (2000). Redefining borders: The challenges of cybercrime. Crime, lawand social change, 34(3), 259-273.

[4] Ibid

- According to Section 66B, receiving stolen computers or communication equipment fraudulently carries a sentence of imprisonment.
- Section 66C - This section examines identity frauds including fake digital signatures, compromised passwords, or other distinguishing characteristics.
- Section 66 D - This on-demand addition focuses on punishing cheaters who use computer resources to impersonate others.

2) Indian Penal Code (IPC)

Invoked in conjunction with the Information Technology Act of 2000, the Indian Penal Code (IPC), 1860, defines identity theft and related cyber offences. The IPC's most pertinent section addresses cyber frauds: Forgery (Section 464) (Section 464). Planned forgery used to cheat (Section 468) falsified records (Section 465) posing a fake paper as a real one (Section 471) reputational harm (Section 469). [5]

Recommendations

- Intrusion Management Process prevents computer intrusions and provides effective security control.
- Self-restraint by computer and net druggies and service providers creates a healthy code of behaviour.
- Use of voice-recognizer, sludge software, and collar-ID for protection Computers used for life conditioning should have some safety and security bias to prevent unauthorised use.
- Antivirus software detects, prevents, and removes viruses and other dangerous software.
- Use encryption technology to appoint well-trained Information Security Officers to protect computer reserves and address security breaches.
- Use of international treaties and agreements to present a united front ensures that local laws are in accordance with international laws and conventions.
- Rigorous capacity building programmes for national law enforcement agencies.
- Firms, government, and civil society working together to tighten cyber-security laws.

Conclusion:

Indian and global cybercrime is rising rapidly. The research compared new cyber security concerns in electronic networks. In the digital age, people who can best use technology and information can grow, thus the Indian legal system must keep up with cybercrimes and international law. Statutory legislation, government policies, and specialised investigating agencies will secure India's cyberspace. Legal awareness programmes should empower people to protect themselves against cybercrime.

Cybercrime threatens society. Digital India could increase such a crime. A strategy to raise awareness is needed since crime affects all ages and education levels. Thus, cybercrime will continue to rise. So, a better way to stop cybercrime is to construct a robust system with a regular maintenance.

[5] Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: trends andchallenges. Handbook of Asian criminology.