International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 23-10-2023, Accepted: 08-11-2023, Published: 24-11-2023
Volume 9, Issue 6, 2023, Page No. 88-91

Comparative analysis of cyber security laws of India United States and United Kingdom

Ekadshi, Deepti Monga
[1] LLM Student, University Institute of Legal Studies, Chandigarh University, Punjab, India
[2] Associate Professor, University Institute of Legal Studies, Chandigarh University, Punjab, India

Abstract
With the swift development in innovation and growing dependency on technical gadgets, cyber frauds are becoming common rampantly. Technology has entirely dominated the lives of people, which has led to some serious repercussions. Crimes of all kinds are perpetrated online. Due to free flow of information in the cyberspace, countries are becoming more vigilant regarding data protection as a part of national defense and public welfare. By developing and putting into practice the cyber security policies and proper procedures, the associated risk with cyber crime can be mitigated to certain extent. This paper is an attempt to analyze the existing legislation concerning cyber laws. It aims to emphasize on those nations that are widely recognized for their vigorous participation in the cyber security arena, namely the United States, United Kingdom, and India.

Keywords: Cyber security, cyber laws, cyber crimes

Introduction
Cyber security is a domain which is evolving constantly. The main causation for this is the growth of new hazards and advances in technology. The requirement is to be one step ahead of cyber criminals by becoming more vigilant. Cyber security has become a more crucial technology in this era of digitization for both individuals and commercial safety. Cyber security is the area of safeguarding the networks of computer system and online data from fraudulent activities like theft, phishing, Trojans, malware attacks, unauthorized access of data and damage. The main object of cyber security is to maintain secrecy of digital assets because people, businesses and governments are more prone to cyber attacks owing to increasing dependency on internet.

Objective
The objective of this paper is to do a comparative analysis of the existing legislations related to cyber security. This paper aims to emphasize on those nations that are widely recognized for their vigorous participation in the cyber security arena, namely the United States, United Kingdom, and India.

1.3 Methodology of data analysis and interpretation
To carry out the study, secondary data analysis approach will be adopted. Data from different websites, articles, journals and other materials has been browsed for the same. The secondary data explored the various cyber crimes that are common in India as well as in western countries.

1.4 Meaning of Cyber Crimes
The term "cyber-crimes" is not defined in any statute or law in India. The word "cyber" is used in the context of computers, Information Technology, etc. Therefore, it stands to reason that "cyber-crimes" are offenses relating to computers, information technology, the internet, and virtual reality[1]. The attacks target the corporate or personal virtual body, which is the collection of informational characteristics that characterise individuals and organisations on the Internet, rather than a physical body. Cybercrime affects more than just one person. Cybercrimes, such as financial theft, espionage, and other cross-border crimes, are committed globally by both state and non-state actors. Cyber warfare is the term used to describe cybercrimes that involve a minimum of one nation-state and cross international borders. Odumesi (2014) define Cybercrime as "a crime that has to do with the abuse of digital resources in a cyberspace or via the internet or network networks, wither through wired or wireless communication."

Kinds of Cyber Crimes
There has been a paradigm change in behavioral patterns of individuals from offline to online since the COVID-19 outbreak worldwide. This has made a profitable target for criminals in 2022 which amounts to $7.1 trillion, up from $1.2 trillion in 2019. There are copious cyber crimes that are common not only in India but also in other western countries like USA, UK, Germany and Russia.

Phishing
Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website. Phishing is a technique in which the attacker sends the bogus emails that seems to be come from reliable sources. Generally, E-mail source is used for it. The main object behind this is to steal the sensitive data like credit card number and login credentials by infecting the victim's computer with malware.

Ransomware
Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the

system that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations to prevent attacks that can severely impact business process and leave organizations without the data they need to operate and deliver mission-critical services. The cost or exchange rate varies depending on the type of ransomware. In present times, ransomware authors frequently request Bitcoin payments in exchange for ransomware. According to FBI, Globally, According to statistica, there were about 623 million ransomware attacks in 2021 and 493 million in 2022.

Cyber Pornography

Cyber pornography is the act of using cyberspace to create, display, distribute, import or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. The literal meaning of the term 'Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." Younger generation consider it as a source of instant satisfaction and a form of rebellion. Whereas, the senior generation see it as an abuse of cultural, ethical ands moral principles.

Cyber Terrorism

Cyber terrorism is also known as a Digital terrorism. It is a disruptive attack by recognized terrorist organizations against computer system with the intent of generating alarm, panic or physical disruption of the information system. Some examples of cyber terrorism are –

- Virus introduction to data networks.
- Server hacking to steal sensitive information
- Making website inaccessible by defacing them
- Causing terror by attacking financial institutions to transfer money

Identity Theft

Identity theft occurs when the personal information of some individual such as name, phone number, birthday and credit card number obtained by someone without the consent and uses it to perpetrate fraud or other crimes. Computer-related identity theft is the intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right.

Cyber Stalking

Cyber stalking means to harass, follow and stealthily try to approach a person using the internet or any other electronic means. It involves the conduct of harassing or threatening an individual repeatedly over publishing obscene material in "electronic form". Although cyber stalking is a broader term for harassment which is being committed online, still it can include false accusations, defamation, teasing and even extreme threats.

Cyber law legislations in India

Information Technology Act, 2000

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology "INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008]. With an attempt to safeguard the cyberspace and to empower internet users against cyber frauds, below written are some of the important provisions of the act.

Section 65:-**Tampering with computer source documents**

When a programme, computer command, design and layout is required to be maintained by law, is deliberately destroyed, conceal or altered by any person, then that person commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both.

Section 66: - Using password of another person

If the password, digital signature or other unique identification of a person is used by another person fraudulently, then that person can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.

Section 66D: - Cheating using computer resource

Cheating using a computer resource or a communication device by a person is also a type of cyber crime and covered under this section. He/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR.

Section 66E: - Publication of private pictures of others

Capturing, transmitting or publishing images of a private parts of a person without his/her consent or knowledge is a cyber crime and punishable by law. That person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both

Section 66F: - Cyber Terrorism acts

If an authorized person gets denied by some other person, the access to computer resources or if a person attempts to access a computer resource without sanction, with motive to endanger the integrity, security, unity and sovereignty of the nation, then that person can face life imprisonment. The offence covered under this section is a non-bailable offence.

Section 67: - Child Pornography

Capturing, publishing or transmitting photographs of a young boy/girl in a sexually explicit act or persuade any minor (under the age of 18) boy or girl into a sexual act is an offence in the eyes of law and punishable by imprisonment up to 7 years or fine up to 10 Lakhs INR or both.

Section 69: - Power to Block websites by Government

The government, in order to protect the interest of sovereignty and integrity of India, can seize, observe or decrypt any information obtained, broadcasted, received or reserved in any computer resource. Proper procedure has to be followed for exercising this power. Under section 69A, any information can be blocked by the central government from public access.

Section 43A: - Protecting data at corporate level
Any wrongful loss or gain, caused to any person, due to the negligence of a corporate body in administering the suitable safety procedures, such body corporate shall be liable to pay compensation to the affected person.

National cyber security policy, 2013
Because of alarming spike in the cyber attacks and the rapid development of technology industry, the Indian Government attempted to introduce an updated framework. To prevent cyber attacks in 2013, this act has been established. This act offers a foundation for safe and secure electronic transactions.
The National Cyber Security Policy document outlines a roadmap to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country. Few important objectives of this policy are –

a. Adoption of practices to secure E-Commerce transactions, private data of citizens.
b. Creating a better cyber ecosystem in India.
c. Effective cooperation between private and public sector.
d. Establishing a Nodal Agency for cyber attacks crisis.

National Cyber Security Strategy, 2020
New impediments observed by both public and private sector, the Government of India launched the National Cyber Security Strategy, 2020. It is a five year cyber security policy that will operate from 2020-2025. Because of the new developments in technology and improvements that occur on daily basis, stricter regulations and more recent legislation are needed. This policy guarantees a reliable, dynamic, safe, secure and robust cyber space for financial development of country. There are certain foundations of strategy-

a. Secure (National Cyberspace)
b. Synergize (People, Process, Capability)
c. Strengthen (Resource, such as teamwork and collaboration)

Cyber law Legislations in United States of America
The United States of America is facing the highest number of cyber-attacks and cybercrimes in the world today the legislation which covers cyber security concerns are quite complex in America, each federal agency has its own cyber security regulations to be followed and there are many sector-specific cyber laws for critical infrastructure. Some of the important provisions are written below.

The Counterfeit Access Device and Computer Fraud and Abuse Act, 1984
Attacks on computer system which have private information relating to international trade and global e- commerce owned by Government and interstate entities are controlled by this act.

The Computer Security ACT, 1987
An agency named as National Institute of Standards and Technology (NIST) has been introduced by this act. The main objective of introduction of this agency is the development of security system and to maintain proper security standards. Also, reduction of cyber crime along with creating cyber awareness is objectives of this act. But, the main point is that this act has no application on military and defense matters.

The Homeland Security Act, 2002 (HSA)
This act was initiated with the aim of handling responsibility to homeland security agency for the establishment of security standards of cyber security along with several other general security concerns.

The Cyber Security Research and Development Act, 2002
This act was enacted with an objective of establishing a research agency. The main motive of this agency was to restraint the cyber attacks along with developing a comparatively better infrastructure in state of America. Two institutions namely- NATIONAL SCIENCE Foundation (NSF) and National Institute of Standards and Technology (NIST) given the responsibility of this objective.

E- Government Act, 2002
It is one of the most significant legislation. This act provides the strict rules that must be followed for cyber security in the country. It also provides the framework on federal information technology. In present scenario, the government of United States is taking steps to further strengthen the cyber security laws by amending the older ones and by making new laws. Following are examples of such laws: -

Federal Exchange Data Breach Notification Act, 2015
This act is enacted for providing guidelines to the health insurance sector in provinces. According to this act, the patients should be provided with notification regarding the case of data breach within 60 days of breach. Moreover, the victims should also provide with compensation in such cases of breach. The failure to do compliance with this provision can lead to strict punishments under the act.

Cyber Security Enactment Act, 2014
Few objectives of this are-

a. Development of better rules for cyber security matters.
b. Enhancement of cyber infrastructure.
c. To create awareness about different cyber attacks.
d. To provide help to cyber attack victims and use preventive measure against crime.

Cyber Security Information Sharing Act, 2015 (CISA)
This act was established with a view of sharing matters among various federal agencies operating in country. Instant transferring of difficulties of cyber security, glitches, and some other concerns are the main objectives of this act.

Cyber Security Laws in United Kingdom
The rampant increase in the digital threats in the current times arise the need that the businesses should change their IT systems as they take an indispensable shift towards digitalization and cloud migration in UK's digital landscape. There is a dire need that companies must comply with the latest cyber security laws and regulations in the UK. Here are some of the important acts that are in operation in UK for protection against cyber crimes.
Data Protection Act, 2018

It is the primary legislation enacted by UK Government on processing of personal data in UK, which was enforced along with the UK-GDR. This act regulates all the aspects of how government bodies and organizations control and manage personal data by providing the data protection work. DPA, 2018 requires all the data controllers of UK to maintain and implement accurate safety measures for personal data securitization.

Penalty for Non- Compliance with provisions of act - Fine up to 17.5 million euro or 4% of annual global turnover.

United Kingdom General Data Protection Regulation (UK-GDPR): - The rules and regulations of this apply to every country in United Kingdom – England, Wales, Scotland and Northern Ireland. Under this, Businesses are obliged to protect all personal data. Moreover, it also protects the rights of people whose data is held.

Penalty for Non- Compliance with provisions- Non-compliance with UK- GDPR may be penalized up to 20 million pound or 4% of their annual turnover.

Network and Information System (NIS) Regulation, 2018

This is one of the most important legislations, which was transposed from EU cyber security directive. The primary objective of these regulations is to manage and detect the network security threats in information system. It works in acceptable and proportional manner.

Additionally, it also covers the non- cyber threats like disruptive events, power outrages etc.

Penalty for Non- Compliance with provisions- Non-compliance with NIS Regulations can lead to penalty of 19 million pound and 4% annual global turnover.

Conclusion

The distinct legal, cultural, and technological landscapes of the United States, the United Kingdom, and India are reflected in their respective cyber security legislation. Information technology Act, 2000 and National Cyber Security Policy has made noteworthy efforts to elevate cyber security in India. Still, concerns with allocation of resources, implementation, and the dynamic nature of cyber threats continue to exist**.**

Cyber security dangers are addressed by a comprehensive legal framework in the United States, which includes important laws like the Federal Exchange Data Breach Notification Act and the Cyber security Information Sharing Act (CISA). The American strategy places a strong emphasis on sector-specific attention, information sharing, and public-private partnerships. The UK has created a strong legislative framework for cyber security. The legal strategy adopted by the UK demonstrates a dedication to working with foreign partners, enforcing laws, and safeguarding vital infrastructure. Its legal system clearly strikes a compromise between the needs of national security and individual privacy.

Privacy and data protection are important issues in all three nations, although the details differ. The Data Protection Act of the United Kingdom is in line with European norms and underscores the significance of protecting personal data. Although every nation has made progress in tackling cyber security issues, several themes come up again and time again: public awareness, international cooperation, and constant adaptability to new threats. These countries must jointly confront the difficulty of striking a balance between the demands of individual privacy rights protection and national security.

References

1. Yoshita Gandhi," Cyber laws: Comparative study of Indian law & Foreign laws," 1 Journal of Applicable law & Jurisprudence 7
2. Cybercrime, *available at*: http://www.britannica.com (last visited on November 3, 2023)
3. Cyber crime, *available at*: http://www.byjus.com (last visited on November 3, 2023)
4. Nte, N. D., Enoke, B. K., & Teru, V. A., "A Comparative Analysis of Cyber Security Laws and Policies in Nigeri and South Africa" 8(2) Law Research Review Quarterly 238 (2022)
5. Phishing attacks: Defending your organization, available at: http://www.ncsc.gov.uk (last visited on November 3, 2023)
6. Stop ransomware, *available at:* http://www.cisa.gov (last visited on November 3, 2023)
7. Ransomware, *available at*: http://en.wikipedia.org (last visited on November 3, 2023)
8. Mr. Razit Sharma and Miss. Bhavika Sinha, "Cyber Pornography in India- A Legal Insight" 5 Journal of Emerging Technologies and Innovation Research 204 (2018)
9. Cyber Terrorism, *available at*: http://wigan.gov.uk (last visited on November 3, 2023)
10. Anti Cybercrime Group, *available at*: https://acg.gov.ph/main (last visited on November 3, 2023)
11. Yoshita Gandhi," Cyber laws: Comparative study of Indian law & Foreign laws," 1 Journal of Applicable law & Jurisprudence 10
12. An Overview of Cyber Laws vs. Cyber Crimes: Indian Perspective, *available at*: http://www.mondaq.com (last visited on November 7, 2023)
13. National Cyber Security Policy 2013 – In a nutshell, *available at:* - http://www.clearias.com (last visited on November 7, 2023)
14. Federal Laws Relating to Cyber security: Overview of Major Issues, Current Laws, and Proposed Legislation, *available at,* https://fas.org/sgp/crs/natsec(last visited on November 7, 2023)