IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

COMPARATIVE ANALYSIS OF CYBER LAWS – INDIA, US AND UAE

Diksha Jain
Student
New Law College
Bharati Vidyapeeth Deemed to be University, Pune, India

Abstract

The digital revolution has brought unprecedented connectivity and convenience, but it has also given rise to a new breed of criminal activities known as cybercrime. Cybercrime has emerged as a critical challenge in the digital age. It has become a pervasive and evolving threat in today's interconnected world. The rapid evolution of technology has brought about unprecedented challenges in the legal sphere, particularly in the context of cyberspace. As technology advances, so do the methods and tactics employed by cybercriminals, the legal framework governing cyberspace must adapt accordingly, prompting nations to enact comprehensive legislation to address and mitigate these threats. Nations around the globe have responded by enacting legislation to address and combat cybercrime. This research paper undertakes a detailed examination of cybercrime legislation in the United Arab Emirates (UAE), the United States(US), and India. This research paper also take a look on the procedure of filling of report by the victim of cybercrime in the United Arab Emirates (UAE), the United States(US), and India . In this research paper there will also be comparison between United Arab Emirates (UAE), the United States(US), and India with respect to the cyber legislation, agencies dealing with cybercrime, conventions on cyber laws, punishments or penalties. From the comparison we will look where does India lacks from other countries and how to overcome these shortcomings.

Keywords : cyberlaw, cybercrime

INTRODUCTION

Cybercrimes are those crimes in which electronic devices and internet are used to commit such crimes. Cybercrimes can be committed through various electronic devices like computers, laptops, mobile phones, etc. cybercrimes are of various types for example phishing, cyberstalking, PUPs (potentially unwanted programs), social engineering, identity theft. There was rise in rate of cybercrimes in recent years because of the sudden increase in the need of technology, internet and electronic devices. It is clear that the rate of data breaches are increasing. Since 2001, the victim count has increased from 6 victims per hour to 97 in 2021, a 1517% increase over 20 years[1]. Because of this rise the need for laws to curb the cybercrimes is felt by various countries. And subsequently countries started framing cyber laws and brought them into force. Cyber laws are the rules and regulations which controls and governs cyberspace. Cyber laws also prevents from online frauds, provides security for e-transactions, protects data of individuals i.e. data privacy and also provides for

[1] Charles Griffiths, The Latest 2023 Cyber Crime Statistics, AAG(04.01.24), https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=The%20Cost%20of%20Cyber%20Crime,hour%20worldwide%20has%20also%20increased., (last visited on jan 29, 2024)

right to legal action to victim if any cybercrime gets committed against him. Cyber laws also provide for cybersecurity. Cybersecurity is essential in today's interconnected and digital world due to the increasing reliance on technology and the pervasive nature of cyber threats. The need for cybersecurity is paramount in addressing the evolving landscape of cyber threats. By implementing robust cybersecurity measures, individuals, businesses, and nations can mitigate risks, protect sensitive information, and ensure the resilience of digital systems in the face of an ever-changing threat landscape. In India, the Information and Technology Act (IT Act) are the cyber laws governing in the country. The IT Act came into force in year 2002. The IT Act was the first cyber legislation in india and this law was further amended in 2008. In US there are 3 main cybersecurity laws, the laws are the regulations of the federal government of us. These main 3 laws are – health insurance portability and accountability act of 1996, gramm-leach-bliley act of 1999 and homeland security act which included the federal information security management act of 2002. Apart from these laws today in US there more laws on cybersecurity enacted by federal government as well as state government. In UAE the Federal Law No (2), 2006 is cyber legislation which prevents against the crimes of information and technology. In 2012, the amendment was brought through Federal Decree law no (5) on combating cybercrimes.

Cyber laws

India

The department of electronics in 1998 drafted the bill for cyber laws for the every first time. After this a new ministry was formed to deal with all the matters related to cybercrime, cyber law, cybersecurity, the ministry was IT Ministry, which later in 1999 introduced the bill in the house. In 2000 the bill was passed and became the Information and Technology Act (IT Act), 2000 and in 2000 only this act came into force. With passing years, as technology got evolved, this technology also started getting used for cybercrimes of new types for which the existing act was not sufficient. So in the year 2008 the amendment was done in IT Act and came in force in 2009. Digital signatures are a form of electronic signature that provides a way to verify the authenticity and integrity of digital messages or documents. Digital signatures continue to play a crucial role in facilitating secure and authenticated transactions in the digital realm.

Digital signatures are extensively used in various sectors, including business transactions, and electronic contracts. Digital signatures often rely on Digital Signature Certificates issued by trusted Certificate Authorities (CAs). These certificates play a crucial role in verifying the identity of the entity using the digital signature. Governments and regulatory bodies may accredit specific CAs to ensure the trustworthiness of digital signatures. In India section 2 (!) (q) of the IT act, 2000 defines digital signature. Through section 2 (1) (q) of IT Act only the digital signatures get legal recognition in India. In India, the eligibility and appointment of CAs is done under the IT (certifying authorities) rules, 2000. While the IT (certifying authority) regulations, 2001 gives procedure and technical standards which are to be maintained by CAs. In 2002 the electronic cheques concept got introduced in India through negotiable instruments (amendments and miscellaneous provisions) act. The Indian Evidence Act also got amendment and because of this amendment the digital data and information was also considered as admissible evidence in court. The first recent addition which is made to the cyber laws is the Information Technology Amendment Rules, 2023, through this rules government has tried to put censorship on social media platforms. In 2023 only the Proposed Digital India Act, 2023 was made public by the ministry of electronics and information technology. This new bill is aimed to replace the 24 year IT Act,2000. [2]This Act provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. This bill is not yet presented in any house of parliament, this is only a proposed draft of digital india act.

The complain against cybercrime in India can be filled by 3 ways: First way is that one can file complain through online portal of Indian government that is https://cybercrime.gov.in/ , the second way is through

[2] Tapanjana Rudra, Digital India Act Unlikely To Be Ready Before 2024 General Elections, inc42.com https://inc42.com/buzz/digital-india-act-unlikely-to-be-ready-before-2024-general-elections-mos-chandrasekhar/#:~:text=In%20March%20this%20year%2C%20the,online%20civil%20and%20criminal%20offences%E2%80%9D. (last visited on jan 28, 2024)

helpline number 1903, or the third way is you can go to the nearest police station to register complain physically.

[3]

United States (US)

In US federal laws for cybersecurity as well as state laws for cybersecurity. One of the federal cyber law in US is Federal Information Security Modernization Act (FISMA) which was passed in2002. This law was passed for federal agencies to maintain the confidentiality of their data. The other federal law which was passed in 2015 is cybersecurity information sharing act (CISA). The objective of this act was sharing of information between the government and private sector companies about the cyber threats with the department of homeland security(DHS). There are state laws also ; one of the state law is passed by California which is California consumer privacy act (CCPA) which was passed in 2018 but came into force in 2020. This law aims to give rights to individual about personal information which is collected by businesses. This right includes to know that information is collected, request to delete it and choose not to sale information by businesses. The other state is new York where a agency is formed which is New York Department of Financial Services (NYDFS) for the purpose of enforcing laws and regulation to financial service company in the new york. Other than these several other states have laws for cybersecurity and protection of personal information. Other than federal laws and state laws there are some agencies for example Department of homeland security (DHS), Federal bureau of investigation (FBI) and Cybersecurity and infrastructure security agency (CISA) is a department of DHS, the main objective of these agencies is to protect from cybercrime and cyberthreats and to ensure cybersecurity. There is one more agency which looks out to other federal agency if they are compels with federal cyberlaws which is Government Accountability Office (GAO)

To file complain against cybercrime there are different websites created by different departments. Complain can be file with the united states computer emergency readiness team (us-cert) created by the department's cyber security division through hotline (1-888-282-0870) or website www.us-cert.gov , one can also file complain of fraud through website www.ftc.gov/complaint to the federal trade commission, or complain can also be filed with internet crime complaint centre on the website www.ic3.gov.[4]

United Arab Emirates (UAE)

In UAE, Prevention of Information Technology Crimes, Federal Law No. (2) of 2006 was a legislation governing telecommunication sector and cybercrime. It was dealing with the unlawful access to website and the penalty for same was given under Federal Law No. (2) of 2006 . One of the key pieces of legislation governing cyber activities in the UAE is the Cybercrime Law, Federal Law No. 5 of 2012. This law aims to combat cybercrimes and provides a comprehensive legal framework to address offenses related to information technology and electronic communication. It covers a wide range of activities, including unauthorized access to computer systems, data interference, and online fraud. This law also repealed the , Federal Law No. (2) of 2006. Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes took effect in 2022. The law provides a comprehensive legal framework to address the concerns relating to the misuse and abuse of online technologies. It aims to enhance the level of protection from online crimes committed through the use of information technology, networks and platforms[5]. The UAE's Personal Data Protection Law, Federal Decree Law No. 45 of 2021, focuses on safeguarding personal data and ensuring its lawful and fair processing. It grants individuals certain rights over their data, such as the right to access, rectify, and erase their personal information held by data controllers.

[3] Ankita Deshkar, Victim of a cybercrime? Here's a step-by-step guide on how to file a complaint, THE INDIAN EXPRESS, https://indianexpress.com/article/explained/everyday-explainers/victim-cybercrime-guide-how-to-file-complaint-8970419/ (last visited jan 24, 2024)

[4] REPORTING A CYBERCRIME COMPLAINT TIP CARD, cisa.gov https://www.cisa.gov/sites/default/files/publications/Reporting%2520a%2520Cybercrime%2520Complaint_0.pdf (last visited jan 29, 2024)

[5] Cyber safety and digital security, U.AE, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security#:~:text=Dubai%20Cyber%20Index-,Law%20on%20combatting%20rumours%20and%20cybercrimes,and%20abuse%20of%20online%20technologies., (last visited jan 29, 2024)

The UAE computer emergency response team (CERT) is the agency who handles the cybersecurity cases in UAE.CERT also investigates the cases and take action on the complain. In UAE complain against cybercrime can be reported to UAE CERT on the email id cert@tra.gov.ae or by call on 800444 and the other way to report a complain is to Dubai police through their website https://www.dubaipolice.gov.ae/wps/portal/home/services/individualservices/cybercrimeService .[6]

Comparative analysis of cyber laws in India, US and UAE

In India, the primary legislation governing cyber-related issues is the Information Technology Act, 2000, and its subsequent amendments. The Act encompasses a wide range of cyber offenses, including unauthorized access, data breaches, and cyberterrorism. Additionally, the Indian Penal Code has provisions relating to cybercrimes. The United States lacks a comprehensive federal cyber law. Instead, cyber-related matters are addressed through a combination of federal and state laws. The Federal Information Security Modernization Act (FISMA) and Cybersecurity Information Sharing Act (CISA) are key federal statute, Various states also have their own cybercrime laws. In the UAE, cyber-related matters are primarily governed by Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes and Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes. This legislation criminalizes various cyber offenses, including hacking, online fraud, and identity theft. The UAE has also implemented data protection laws, such as the UAE Privacy Regulation.

Jurisdictional challenges in India arise due to the global nature of cybercrimes. The IT Act provides extraterritorial jurisdiction, enabling authorities to prosecute offenses committed outside India that affect computer systems within the country. However, practical challenges in cross-border enforcement persist because taking out data from foreign territory for investigating is not a esay task. The USA faces similar challenges in determining jurisdiction, especially in cases involving international cybercrimes. The Computer Fraud and Abuse Act (CFAA) has provisions for extraterritorial jurisdiction, allowing prosecution for offenses committed outside the country that impact U.S. computer systems. The UAE, with a smaller geographical scope, may have a more defined jurisdictional framework. The Combating Cybercrimes legislation in the UAE also provides for extraterritorial jurisdiction to address cybercrimes that have an impact on the country.

India has recently enacted the Personal Data Protection Bill, 2019, which is set to replace the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The new legislation aims to strengthen data protection and privacy rights. The United States lacks a comprehensive federal data protection law. Instead, it relies on sector-specific regulations and state-level laws. The California Consumer Privacy Act (CCPA) is a notable state-level legislation that grants California residents specific rights over their personal data. The UAE has implemented UAE's Personal Data Protection Law, Federal Decree Law No. 45 of 2021, including the UAE Privacy Regulation. These regulations govern the processing of personal data and provide individuals with certain rights regarding their information.

In India there is specific provision for cyber terrorism. This provision for cyber terrorism was introduced by the Information Technology (Amendment) Act, 2008, specifically to address cyber terrorism. Section 66F - Cyber Terrorism defines cyber terrorism and prescribes stringent penalties for offenses related to cyber terrorism. The penalty under this section for cyber terrorism is imprisonment which may extend to imprisonment for life[7]. In US there is no specific provision for cyber terrorism like in India. In US, there are provisions within the CFAA play a role in prosecuting cyber terrorists engaging in activities such as hacking, data breaches, and disruption of critical infrastructure. USA Patriot Act was enacted shortly after the 9/11 attacks, the USA PATRIOT Act expanded the government's surveillance and investigative powers. It includes provisions allowing the collection of information related to potential cyber threats with connections to terrorism. In UAE, Article 21 of Federal Law No. 5 of 2012 on Combating Cybercrimes is Penalties for Using

[6] Reporting cybercrime in UAE, cyber bell india, Mon/Oct/2023 https://cyberbellindia.com/reporting-cybercrime-in-uae/ (last visited on jan 28, 2024)

[7] THE INFORMATION TECHNOLOGY(AMENDMENT) ACT, 2008, § 66F, No. 10, Act of parliament, (India)

Electronic Information Systems for Terrorism. This article specifically addresses the use of electronic information systems for terrorist purposes, prescribing severe penalties for individuals engaged in such activities.

The Indian government has established organizations such as the Cyber and Information Security Division (CISD) and the Indian Computer Emergency Response Team (CERT-In) to address cybersecurity challenges. These agencies work towards enhancing the country's cybersecurity infrastructure. In the United States, various federal agencies, such as the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), play crucial roles in addressing cyber threats. Coordination between these agencies is essential to ensure a comprehensive approach to cybersecurity. The UAE has various government bodies, including the UAE Computer Emergency Response Team (aeCERT), tasked with addressing cybersecurity issues. The National Electronic Security Authority (NESA) also plays a role in formulating policies related to information security.

The Budapest Convention 2001, is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.[8] India actively engages in international cooperation to combat cybercrimes. The Budapest Convention on Cybercrime has not signed by India. The USA is a signatory to the Budapest Convention and collaborates with other nations to address transnational cyber threats. Bilateral agreements and international partnerships play a crucial role in fostering cooperation in the realm of cybersecurity. The UAE, being a member of the international community, participates in global efforts to combat cybercrimes. It collaborates with other countries through bilateral agreements and international forums to address transnational cyber threats. Similar to India, UAE has also not signed the Budapest Convention on Cybercrime.

Opinion

In my opinion, while all India, US and UAE recognize the importance of addressing cybercrimes, there are notable differences in their approaches. India's recent efforts to enact comprehensive data protection legislation demonstrate a commitment to enhancing privacy rights. The USA's reliance on a combination of federal and state laws creates a complex legal landscape that may benefit from greater harmonization. , while the UAE's comprehensive legislation reflects its commitment to combatting cybercrimes. However, challenges such as jurisdictional issues and the need for effective international cooperation persist in all countries. In India there is specific provision for cyber terrorism but in US and UAE there is no such specific provision for cyber terrorism it is included under terrorism provision or under cybercrime provisions. US have enough infrastructure to investigate the complain of cybercrime through various agencies and specialised department for cybersecurity while India and UAE need to develop infrastructure to investigate cybercrime.

Conclusion

The evolution of cyber law in India, USA and UAE reflects the dynamic nature of the digital landscape. As technology continues to advance, the legal frameworks in all three countries must adapt to effectively address emerging cyber threats. Collaborative efforts, both domestically and internationally, are crucial to creating a secure cyberspace for individuals and businesses alike.

while India has made significant strides in establishing a legal framework to address cyber issues, there is a need for continuous vigilance and adaptation to stay ahead of cyber threats. The government should focus on regular updates to existing laws and consider new legislation to tackle emerging challenges such as artificial intelligence-related crimes and the use of cryptocurrencies in cyber offenses. Furthermore, education and awareness programs should be prioritized to inform the public about cybersecurity best practices and the potential risks associated with online activities. Empowering individuals with knowledge about protecting themselves online is crucial in creating a safer digital environment. India's cyber laws have come a long way,

[8] Details of Treaty No.185, COUNCIL OF EUROPE PORTAL, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, (last visited jan 29, 2024)

but the journey is ongoing. The government, legal professionals, and technology experts must work hand in hand to ensure that the legal framework remains robust and effective in the face of evolving cyber threats. It is a collective responsibility to secure the digital future of the nation and safeguard the rights and privacy of individuals in the online realm.