CENTRE FOR ACADEMIC LEGAL RESEARCH | JOURNAL OF APPLICABLE LAW & JURISPRUDENCE

Volume 1 | Issue 1

"Cyber Laws: Comparative Study of Indian and Foreign laws"

By: Yoshita Gwalani (4th Year, University of Mumbai Law Academy)

Abstract

With the recent outbreak of **the COVID-19** pandemic, we have seen a complete shift in dependency on electronic devices and the internet and a consequent surge in cybersecurity threats in India.

With the constant rise in cyberattacks such as phishing, Trojans, Malware attacks, and privacy concerns, it is important to shed light on the existing cybersecurity laws and legal remedies available to a victim of a cyberattack in India. Cyberattacks in India have gained great momentum since February 2020 as the percentage of cyberattacks has increased to 500% in 2020 alone with more expected in the near future. The paper aims at analyzing the current legislation of India concerning cyber laws, cybersecurity, and remedies available for cyberattack victims. The Article also sheds light on the upcoming cyber laws in India and their potential impact on cybersecurity and cyberattacks. The paper seeks to establish whether the existing laws in addition to the upcoming laws are sufficient to combat the current and future threats to privacy and cybersecurity while also focusing on analyzing the existing legislation concerning cyber laws in western countries such as the United States of America, United Kingdom, and Australia in comparison to that of Indian cyber laws.

Keywords: cyber laws, Cybersecurity, COVID 19, cyberattacks, cybersecurity threats

Introduction

In recent times, there is a trend of increasing reliance on technology not only in various industries but also in common households. The COVID-19 pandemic has accelerated this industry's shift to digital. Operations in various fields based in cyberspaces have been forced to evolve quickly.[1]The pandemic lays bare the many vulnerabilities created by society's dependence on the internet.[2] With this increasing dependence and use of electronic mediums by individuals, vast expansions in e-commerce industries and business, international trade gaining momentum, and the evolution of new crimes committed in cyberspace, it also managed to give rise to a variety of legal challenges and issues that have laid the groundwork for the implementation of Cyber Laws in India.

Cyber Law Legislations in India

The Government of India then passed its first cyber law, THE INFORMATION AND TECHNOLOGY ACT OF 2000, which provides a legal infrastructure for e-commerce in India. The IT Law takes into consideration, the legal semantics and know-how while also simultaneously governing relevant data, software, and details on the digital age.

Even though it's not under any particular ambit of law, it manages to cover vast areas of intellectual property, data protection, and privacy under its ambit. The Act protects the field of e-commerce, e-governance, e-banking while also covering penalties and punishments in the field of cybercrimes. The above Act was further amended in the form of the IT Amendment Act, 2008 [ITAA-2008][3].

- **Information Technology Act 2000**

  Information Technology Act, 2000 is the Primary legislature that regulates the use of computers and software, and networks while also overseeing digital or electronic information. It is multifold because it extends to digital signatures, crimes committed in cyberlaw, network service providers as well as digital authentication.

---

[1] Sankaranarayanan Krishnapuram Srinivasan on Covid-19: Dependence on digital banking underscores the need for efficient cybersecurity measures, Available at https://ciso.economictimes.indiatimes.com/news/covid-19-dependence-on-digital-banking-underscores-the-need-for-efficient-cybersecurity-measures/76155222

[2] Laura DeNardis and Jennifer Daskal on Society's dependence on the internet: 5 cyber issues the coronavirus lays bare, Available at https://theconversation.com/societys-dependence-on-the-internet-5-cyber-issues-the-coronavirus-lays-bare-133679

[3] Gupta, Rohit. (n.d.). *An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective - Privacy - India*. Www.Mondaq.Com. https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective

As objectives stated in the preface of the act itself, the Information Technology Act aims at giving legal recognition to e-commerce activities, facilitate e-governance, prevent cybercrime and amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. However the Act had certain shortcomings and with the rising security concerns, privacy concerns, and rapid development in the IT sector, the Government of India amended the Act in 2008 to accommodate new developments and regulations that the original bill failed to cover.

The Act elaborates on the procedures relating to Certifying Authorities (for digital certificates as per IT Act, 2000 and since replaced by electronic signatures in the ITAA, 2008). Numerous offenses have been mentioned especially pertaining to data theft and the adjudication proceedings for such crimes. It also elucidates the popular and common crimes that are being committed daily along with their punishment. Moreover, emphasis has been placed on a few provisions, the role of intermediaries, and the importance of exercising due diligence to avoid such risks[4].

The Government under IT Act has laid down certain rules that focus on and regulates specific areas of collection, transfer, and processing of data which includes the regulations for registration of cyber cafes in India and also complies them to keep specific logs of daily internet users, it further prohibits the exhibition of improper content on various digital platforms while also requiring intermediaries to block and take down such content off the websites, this has gained great importance in recent times due to excessive use of social media. Moreover, the Privacy and security of user data have become a prime concern today, it is necessary that such data provided by the citizens be well protected and secured. Thus, the act Rules, which require entities holding user's sensitive personal information to maintain certain specified security standards, these rules were species in 2011 by the government, and failure to abide by the rules shall be punishable with hefty fine and imprisonment under the act.

[4] *Cyber Laws in India*. (n.d.). Retrieved August 18, 2020, from https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf

An Overview on Important Provisions under IT Act

- **Adjudication**

  Section 46 of the act describes the power of adjudication, accordingly, it specifies that the central government has the power to appoint an adjudicator and he shall be above the position of Director of Government of India or equivalent to an officer of State Government to adjudicate the matters in a prescribed manner [5].The act states the procedure of adjudication, in which the applicant shall be given a reasonable opportunity to argue his issues and after appropriate inquiry done by the appointed officer if the officer believes the offense has been committed then he shall award or impose such punishment as prescribed in the act. The act also lays down the procedure to establish Central Cyber Administrative Tribunal Every adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure[6].The first matter adjudicated in India was the ICICI Bank fraud controversy where the applicant complained that he lost money from this bank account due to lack of security by the bank, the amount was compensated to the applicant as per the order of the court.

- **E-commerce**

  The Indian e-commerce sector has shown impressive growth in the last couple of years. India has seen a major shift of businesses from local markets to digital platforms. The IT act provides a legal infrastructure to all the e-commerce activities which protect the customers as well as the sellers, the act legally validates and enforces digital Signature and electronic records and emphasizes to secure private data by the customers and the electronic records. Further, it also aims at reducing frauds and forgery to facilitate convenient e-commerce and providing stringent punishments for non-compliance[7] .

- **E-governance**

  In the IT Act of 2000, Chapter III discusses electronic governance issues, procedures and the legal recognition of electronic records dealt with in detail in Section 4 followed by the description of procedures on electronic records, storage and maintenance, and

---

[5] *Penalties and Adjudication in IT ACT 2000 - PATHLEGAL*. (2018, June 28). Www.Pathlegal. In. https://www.pathlegal.in/Penalties-and-Adjudication-in-IT-ACT-2000-blog-1831947

[6] Gupta, Rohit. (n.d.). *An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective - Privacy - India*. Www.Mondaq.Com. https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective

[7] Raj, Aijaj & Rahman, Wazida. (2016). E-commerce Laws and Regulations in India: Issues and Challenges. 1. 44-51.

according to recognition to the validity of contracts formed through electronic means. Procedures relating to electronic signatures and regulatory guidelines for certifying authorities have been laid down in the sections that follow.

- **Digital Signatures**

  Digital signature means authentication of any electronic record by a subscriber through an electronic method or procedure under the provisions of Section 3. Section 3 deals with conditions subject to which an electronic record may be authenticated using an affixing digital signature which is created in two definite steps. First, the electronic record is converted into a message digest by using a mathematical function known as 'Hash function' which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key that attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.[8]

  In today's scenario, information is supreme. Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case anyone breaks into their computer systems or network and causes damages or copies data network[9].

Cyber Security Policy 2013

With the rapid increase in the IT sector and frightening growth of cyberattacks, the Indian government took a step to introduce a policy in 2013 to provide a new framework and prevent cyberattacks. This policy provides a framework to create secure electronic transactions while also stating guidelines for safer cyberspace in India The policy also documents a roadmap to create a framework for a comprehensive, collaborative and collective response to deal with the issue of cybersecurity at all levels within the country.[10] The policy lays out 14 objectives, which include the adoption of practices to secure e-commerce transactions, the private data of citizens,

---

[8] *OVERVIEW OF CYBER LAWS IN INDIA Index*. (n.d.). Retrieved August 18, 2020, from https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf

[9] Dugal, P. (2001, September). *Cyberlaw In India: The Information Technology Act 2000 - Some Perspectives - Media, Telecoms, IT, Entertainment - India*. www.mondaq.com. https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technology-act-2000--some-perspectives

[10] Andrew, A. (2013, December 4). *National Cyber Security Policy 2013 – In a nutshell*. ClearIAS. https://www.clearias.com/national-cyber-security-policy-2013/

creating a better cyber ecosystem in India, and also effective cooperation between public and private sectors.[11] The policy also aimed at establishing a nodal agency for cyberattack crisis management and effective coordination. The Cert -In instituted Section 70 of IT act under the policy to collect analysis and disseminate information on cyber incidents, forecasts and alerts of cybersecurity incidents, and take emergency measures for handling cybersecurity incidents, etc. The role of CERT-In in e-publishing security vulnerabilities and security alerts is remarkable. The CERT-In helps in combating cybercrime with due processes of law.[12]

National Cyber Security Strategy 2020

Every single day there are new developments and reforms in the field of technology and with the rapid changes, there are requirements for more updated laws and stringent regulation. Taking into consideration the massive changes and the new challenges faced by the private and government sectors, the government of India announced a new cybersecurity policy known as the National Cyber Security Strategy 2020 for five years, i.e., 2020-25. This strategy was implemented to ensure a safe, secure, trusted, resilient and vibrant cyberspace for our Nation's prosperity.

Pillars of Strategy

a. **Secure** (The National Cyberspace)

b. **Strengthen** (Structures, People, Processes, Capabilities)

c. **Synergise** (Resources including Cooperation and Collaboration)

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

[11] PTI. (2013, July 2). *Govt releases National Cyber Security Policy 2013*. Livemint. https://www.livemint.com/Politics/DQ8gg6eCNeZwHJxt84rhMN/Govt-releases-National-Cyber-Security-Policy-2013.html

[12] *Cyber Laws in India.* (n.d.). Retrieved August 18, 2020, from https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf

virtual reality[13]. With the increasing dependency on the internet over the past few years for even basic human needs, cybercrimes have also evolved at a greater pace. Cybercrimes today are quite advanced as they occur almost every single day. It has now become so common that even the highly secured websites of government bodies get hacked, let alone the social media accounts of common people. Research has shown that every eight out of ten people have in some or the other way fallen into such traps of cybercrimes and have been victimized**[14].** Some of the most dangerous data breaches have been concerning government data. One such security breach was that involving India's unique citizen identification system- the Aadhaar, which got hacked in early 2018, compromising extensive personal information including bank details, address, and biometrics of over a billion Indians.[15]Along with economic losses, cybercrimes also impact public safety- especially for minors and vulnerable sections of the society through incidents of cyberbullying and exploitation. In 2018 alone, India recorded over two thousand cases of cybercrimes related to sexual harassment and over 700 cases of cyberbullying against women and minors. Perhaps these high number of cases led to increased awareness about the issue of cyberbullying as a large share of Indians felt that the responsibility for abusive behavior on social media lay with both the users as well as social media platforms[16]. The government in 2018 took the initiative to launch a National Cyber Crime Reporting Portal across the country which enables citizens to register complaints online.

Types of Cyber Crime

With the advent of technology and the ever-increasing advances in science, it has managed to also attract criminals who find new ways to defraud people on the internet. Some of the most common and equally terrifying cybercrimes committed regularly have been detailed below.

a) **Identity theft**: It simply refers to fraudulently cheating others by assuming another individual's identity. It involves stealing money or getting other benefits by pretending

---

[13] Joseph, V., & Ray, D. (2020, February). *Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence - Media, Telecoms, IT, Entertainment - India*. Www.Mondaq.Com. https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence?type=popular

[14] Varsha. (n.d.). *An Analysis on Cyber Crime in India*. Www.Legalserviceindia.Com. Retrieved August 19, 2020, from http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html

[15] cycles, T. text provides general information S. assumes no liability for the information given being complete or correct D. to varying update, & Text, S. C. D. M. up-to-D. D. T. R. in the. (n.d.). *Topic: Cybercrime in India*. Statista. Retrieved August 19, 2020, from https://www.statista.com/topics/5054/cyber-crime-in-india/#:~:text=In%20fact%2C%20according%20to%20a

[16] cycles, T. text provides general information S. assumes no liability for the information given being complete or correct D. to varying update, & Text, S. C. D. M. up-to-D. D. T. R. in the. (n.d.). *Topic: Cybercrime in India*. Statista. Retrieved August 19, 2020, from https://www.statista.com/topics/5054/cyber-crime-in-india/#:~:text=In%20fact%2C%20according%20to%20a

to be someone else. Information Technology (Amendment)Act, 2008 has defined the crime of identity theft under Section 66-C as - Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, known as identity theft for which the criminal shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.[17]

b) **Unauthorized access to computer systems or networks:** This activity is commonly referred to as hacking but the Indian law indicate hacking as part of unauthorized accesses giving unauthorized access a broader view, however, hacking does occur by default if there is authorized access .'Hacking' means destruction or alteration of any information residing in a computer resource, that is destruction or alteration of tangible and/or intangible assets of a computer resource.[18] As per Section 66, a person with the intention to cause or with the knowledge that he will cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in computer resources or diminishes its value or utility or affects its injuriously by any means commits hacking. Punishment for hacking is imprisonment up to 3 years or a fine which may extend to 2 lakh rupees or both.

c) **Cyber Terrorism:** After the horrifying case of 26/11 in India, the Government of India specifically added 'Cyber Terrorism' in Indian legislation under Section 66F of the IT Act, as inferred by the definition under section 66F. Cyber terrorism is an act to hack, contaminate or prevent a legally authorized person to access the necessary information. Cyber terrorism aims at attacking and gaining access to critical data from the government which shall be restricted data for security of the state, or foreign relation, etc. These are gruesome acts done to extort money from the government, threaten the security of the nation, disrupt public peace, or strike terror in the minds of people in India. It may result in death and injury of people, damage to properties, disruption of civil services which are essential to the life of a community while also affecting the critical information infrastructure.[19]

d) **Cyberstalking**: Cyberstalking means to harass, follow and stealthily try to approach a person using the internet or any other electronic means. It involves the conduct of

---

[17] Kumar, S. (2015). *Present scenario of cybercrime in INDIA and its preventions.*

[18] *OVERVIEW OF CYBER LAWS IN INDIA Index*. (n.d.). Retrieved August 18, 2020, from https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf

[19] https://www.researchgate.net/publication/228192670_Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review

harassing or threatening an individual repeatedly over publishing obscene material in "electronic form". Section 67 of the Information Technology Act Of 2000 covers online stalking, according to the section any person who deliberately bullies or pesters any individual on social media, sends or uses 'Sexually explicit, or publishes any obscene content about the victim shall be punishable with imprisonment and fine under this section. Moreover, with the gaining popularity of social media platforms Section 67B of the Information Technology Act, 2000 is introduced in order to protect children below the age of 18 years from online bullying and stalking. The section also focuses on punishing any person who is engaged in promoting any content on such platforms that would terrorize the minds of children [20].

Cyberattacks In India

Cyberattacks are defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." Cyber Attacks are quite dangerous they can be as simple as hacking a website to stealing intellectual properties, private data, and disrupting essential and civil services[21]. According to reports released by Subsex in 2019, India beat the USA and became the country with the Highest Cyberattacks in 2019. This has alarmingly increased after the outbreak of the COVID-19 pandemic in 2020. According to Cyberlaw expert Pavan Dugaal, cyberattacks in India have increased up to 500 % since February 2020. Since the outbreak, there have been reports of scams impersonating public authorities (e.g. WHO) and organizations (e.g., supermarkets, airlines), targeting support platforms, conducting Personal Protection Equipment (PPE) fraud, and offering COVID19 cures. These scams target members of the public generally, as well as millions of individuals working from home. Working at home en-masse has realized a level of cybersecurity concerns and challenges never faced before by industry and citizenry. Authorities in India declared a High Alert in June 2020 due to a massive increase in cyberattacks. Many companies and banks in India faced financial losses and data infringement. Some of the most recent cases of cyberattack In India are -

[20] Keswani, M. (n.d.). *CYBER STALKING: A CRITICAL STUDY*. Retrieved August 19, 2020, from http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf

[21] *Cyber Attacks | Data Security Council of India*. (n.d.). Www.Sci. In. https://www.dsci.in/content/cyber-attacks

The malware attack on the servers of Pune-based Cosmos Bank shook the Indian Banking sector when hackers, for years, stole nearly $13 million. Hackers siphoned this money from the bank's ATM servers and hacked online transfers and transferred and withdrew it outside India.

- Recently Two Mumbai-based hackers were caught committing a major money fraud involving Rs 540,000, the culprits would hack and gain access to the sim cards and fraudulently divert money from one bank account to another by presenting fake documents.
- In mid-2018, criminals attacked the ATM servers of Canara Bank of India and skimmed Rs 270,000 from it, while also gaining data accesses of 300 users of the banks
- One of the most serious cyber attacks in India that shook the government was the data leak of adhar cards of thousands of Indians which raised major concerns about a breach of Private data and violation of the Right to Privacy granted under the Indian Constitution.
- Other major cyber attacks were on a health care website that resulted in the breach of private data of 7 million patients in India
- In 2016, the Union Bank of India faced a giant phishing attack and lost 17 million marking it one of the biggest financial frauds in India.
- India was, according to an *Analytics in India Piece*, among "the top nations which came under ransomware attacks in 2019." Ransomware demands were as high as $5 million[22].

It is pertinent to point out that cybercriminals target individuals just as easily as they don't tend to update their cybersecurity system and it's much easier to hack into their devices, knowingly or unknowingly via trojans or mobile applications to extract personal as well as work-related confidential information. There are innumerable ways of cyber-attacking individuals other than the ones mentioned above such as web attacks which include SQL Injection and Cross-Site Scripting whereas other cybersecurity threats include DDoS attacks, Password Attacks, Eavesdropping Attack, Birthday attack, Insider threats, etc. With the escalating increase in crimes, the Indian government has taken robust steps by introducing a new cybersecurity policy to combat cybercrimes and ensure better and safer infrastructure in India.

[22] *Notorious Cyber Security Attacks in India to Date*. (2020, March 30). Express Computer. https://www.expresscomputer.in/security/notorious-cyber-security-attacks-in-india-to-date/51714/

Remedies for Cybercrime Victims in India

If any individual or company is a victim of cybercrime shall lodge a complaint with the cyber cell in the nearest Police Stations, the cyber cell then looks into the complaint within 24hrs and also take immediate measure to block websites to avoid further access and try to retrieve data Further One finds laws that penalize cyber-crimes in several statutes and even in regulations framed by various regulators. The Information Technology Act, 2000 ("IT Act") and the Indian Penal Code, 1860 ("IPC") penalize many cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other.

Sections Under IT Act 2000	Offenses	Penalties
43	Damage to computer, computer system, etc.	Compensation not exceeding one crore rupees to the person so affected
43A	Body corporate failure to protect data	Compensation not exceeding five crore rupees to the person so affected
45	Where no penalty has been separately provided	Compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees
66	Hacking with Computer systems, Data alteration, etc.	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both
66A IPC 378	Sending offensive messages through communication services etc.	Imprisonment for a term which may extend to three years and with fine IPC: imprisonment of up to 3 (three) years or a fine or both
66C	Fraudulent use of electronic signature	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh
66F	Cyber Terrorism	Imprisonment which may extend to imprisonment for life

66D	Cheats by personating by using computer resource	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees
70	Unauthorized access to the protected system	Imprisonment for a term which may extend to ten years and shall also be liable to fine

The mirroring remedies under the Indian Penal Code for Cyberattacks are as follows

Cyber sending threatening messages by email	Sec.503 IPC
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec.463 IPC
Bogus websites, Cyber Frauds	Sec.420 IPC
Data theft	Sec.378 IPC
Sharing obscene material	Sec.292
Cyber Terrorism	Sec.121 IPC
Cheating by Personification	Sec.419 IPC
Email spoofing	Sec.463 IPC
Web-Jacking	Sec.383 IPC
E-Mail Abuse	Sec.500 IPC

Cyber Laws in Western Countries

Today in the age of computers, smartphones and the use of the internet and technology in all walks of life has inevitably led to an increase in cybersecurity concerns around the globe, all the countries are trying to have a safer cyber ecosystem and facilitate better international trade and e-commerce activities, here is an overview of cyber laws in western countries such as

a) **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 cybersecurity concerns are quite complex in America, each federal agency has its own cybersecurity regulations to be followed and there are many sector-specific cyber laws for critical infrastructure.[23] Moreover, the legislation covers a large number of federal as well state laws Some noteworthy provisions are in the following acts:

• The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 regulates the frauds or any attacks committed on the federal computer system or any banks, interstate having access to sensitive information relating to foreign commerce and international trade

• The Computer Security Act of 1987 introduced an agency known as the National Institute of Standards and Technology (NIST) to develop healthy and safer security systems and maintain such security standards and take effective measures to considerably reduce cybercrime and initiate steps to create more cybersecurity awareness, however, this does not apply to military and defense-related concerns.

• The Paperwork Reduction Act of 1995 was initiated to develop better cybersecurity policies

• The Homeland Security Act of 2002 (HSA) was initiated to give responsibility to homeland security agency to develop cybersecurity standards along with other general security concerns

• The Cyber Security Research and Development Act, of 2002 was introduced to develop a research agency to curb cyber-attacks and bring better cyberspace infrastructure in America The responsibility was given to NSF and NIST.

• The E-Government Act of 2002 is one of the most important legislation it provides guidelines and regulations for federal information technology in the country and also lays down stringent rules to be followed for cybersecurity

In a recent effort to strengthen its cybersecurity laws, the federal government is introducing several new cybersecurity laws as well as amending the older ones for a better security ecosystem. Below are a few of them:

[23] Fischer, E. (2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*. https://fas.org/sgp/crs/natsec/R42114.pdf

Cybersecurity Information Sharing Act (CISA) -The act was introduced in 2015 to enable sharing of cybersecurity concerns between different federal agencies. Its main aim was to build a strong cyber infrastructure by allowing prompt sharing of cybersecurity difficulties, glitches, and any other concerns between different agencies of the government

Cybersecurity Enhancement Act of 2014: As the name suggests, this act was initiated to enhance the cyberinfrastructure, develop better regulation for cybersecurity concerns, create more awareness about cyberattacks, help the cyberattack victims, use preventive measures against cybercrimes, encourage voluntary public-private relationships as well as research and development in this field

Federal Exchange Data Breach Notification Act of 2015: The act regulates and provides stringent guidelines for the health insurance sector to notify the patients in case of a data breach within 60 days of the breach and compensate the victim for the same, failure to do so shall lead to severe punishments under the act.

There are 50 statues currently in the United States Of America under Federal and state laws and it's quite evident that the country is constantly working on updating new cyber policies and better infrastructure. However, despite constant efforts the government is still not able to curb cyber attacks in America, this stands true for private sectors as well, even after having the best systems in place data breaches and phishing attacks occur every single day in the private sector. [24]

b) **United Kingdom**: No umbrella legislation governs information technology or cybersecurity in the UK, and its various agencies operate under distinct legislative mandates, such as the Civil Contingencies Act of 2004, or the Security Services Act of 1989. Therefore, executive agencies tasked with maintaining cybersecurity have a great degree of flexibility in developing different approaches towards cybersecurity. The Office of Cyber Security was formed in 2009 and became the Office of Cyber Security and Information Assurance (OCSIA) in 2010. The OCSIA is both responsible for developing and coordinating cybersecurity policy across various wings of the UK government, and also works in tandem with the private sector for information exchange and standard-setting. The National Cyber Security Centre (NCSC) is the authoritative

[24] Hardeep Singh. (2015). *A Glance At The United States Cyber Security Laws*. Appknox.Com. https://www.appknox.com/blog/united-states-cyber-security-laws

agency for implementing a cybersecurity policy. It is responsible for advising on and coordinating cybersecurity responses across the government and industry. The NCSC, set up in 2016, incorporates the roles and functions of the Communications-Electronics Security Group, which was the intelligence wing of the UK National Security agency, the GCHQ, and is also in charge of the functioning of the CERT-UK, as well as the Centre for Cyber Assessment and the cyber-related functions of critical infrastructure protection which were undertaken by the Centre for the Protection of National Infrastructure.[25] The most recent legislative measures applicable to businesses in the UK, namely the General Data Protection Regulation ("GDPR") and the Network and Information Security Regulations 2018 (the "NIS Regulations"). Other laws and regulations that may be relevant include the Computer Misuse Act 1990, Communications Act 2003, Privacy and Electronic Communications (EC Directive) Regulations 2003, the FCA Handbook, the PRA Rulebook, and the common law tort of misuse of private information.

The GDPR and the 2018 Act requires the Private business sector in the UK to adopt stringent measures to prevent security breach of data by third parties, it also encourages the private sector to enable and maintain more cyber hygienic systems in order to prevent cybercrimes. It also imposes cybersecurity regulations for all the essential service providers such as health, online market, transport, etc.[26].

c) **Australia:** Cybercrime Act offers comprehensive regulation of computer and Internet-related offenses such as unlawful access and computer trespass, damaging data and impeding access to computers, theft of data, computer fraud, cyberstalking and harassment, and possession of child pornography. Other legislation such as The Spam Act established a scheme for the regulation of commercial email and other types of electronic messages. It restricts unauthorized, unsolicited, electronic messages with some exceptions. This act is regulated by the "Australian Communications and Media Authority[27].As far as data privacy of the public is concerned the Australian government

[25] Joshi, D. (n.d.). *A comparison of legal and regulatory approaches to cybersecurity in India and the United Kingdom Shared under Creative Commons Attribution 4.0 International license*. Retrieved August 20, 2020, from https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf

[26] Timmsons, J., & Chabinsky, S. (2019, May). *Cybersecurity and the UK legal landscape | White & Case LLP*. Whitecase.Com. https://www.whitecase.com/publications/alert/cybersecurity-and-uk-legal-landscape

[27] Appknox, T. (n.d.). *A Glance At Australia's Cyber Security Laws*. Www.Appknox.Com. Retrieved August 20, 2020, from https://www.appknox.com/blog/glance-australias-cyber-security-laws

has a comprehensive framework in the place known as the Protective Security Policy Framework and Information Security Manual. The Australian Government has most recently announced its Cyber Security Policy for 2020 which aims at providing 247 cyber assistance, helping small and large businesses to set up better cybersecurity infrastructure, and to ensure reduction and awareness concerning cybercrimes. Australia has effective general regulatory cyber law but unlike the United States of America, it lacks regulatory laws in many sectors such as health, private business insurance, etc.

Conclusion

The cyber law framework in India, even though thought to suffice the need of the hour, lacks in some ways. Especially the cybersecurity frameworks of certain industry regulators need to be updated to stand the test of time with the ever-evolving technological advancements. Indian authorities, acknowledging this need, are coming up with certain new policy frameworks to sustain these said changes. The provisions of this new policy framework are thought to be adequate to sustain the adversities of these advancing developments. Having said that, the efficacy of these policies lies in the implementation, cautious and corruption-free, of these policies by the respective authorities considering India, as can be seen from precedence, is one of the most likely targets for cybercriminals. When these current and upcoming cyber laws are compared to certain countries around the world, it is found that the United States of America, despite having a multitude of policies and statutory frameworks to ensure cybersecurity, is struggling with the correct implementation. Moreover, all these countries show a trend of lacking sufficient policy frameworks for certain industries including the health sector, insurance sector, and private businesses. And in the case of all the countries including India, the implementation of the carefully framed policies needs to be strict, otherwise, the policies end up rendered futile.

Research/Scholar Index

- Sankaranarayanan Krishnapuram Srinivasan on Covid-19: Dependence on digital banking underscores the need for efficient cybersecurity measures, Available at https://ciso.economictimes.indiatimes.com/news/covid-19-dependence-on-digital-banking-underscores-the-need-for-efficient-cybersecurity-measures/76155222
- Laura DeNardis and Jennifer Daskal on Society's dependence on the internet: 5 cyber issues the coronavirus lays bare, Available at https://theconversation.com/societys-dependence-on-the-internet-5-cyber-issues-the-coronavirus-lays-bare-133679
- Gupta, Rohit. (n.d.). *An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective - Privacy - India*. Www.Mondaq.Com. https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective
- *Cyber Laws in India*. (n.d.). Retrieved August 18, 2020, from https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf
- *Penalties and Adjudication in IT ACT 2000 - PATHLEGAL*. (2018, June 28). Www.Pathlegal. In. https://www.pathlegal.in/Penalties-and-Adjudication-in-IT-ACT-2000-blog-1831947
- Gupta, Rohit. (n.d.). *An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective - Privacy - India*. Www.Mondaq.Com. https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective
- Raj, Aijaj & Rahman, Wazida. (2016). E-commerce Laws and Regulations in India: Issues and Challenges. 1. 44-51.
- *OVERVIEW OF CYBER LAWS IN INDIA Index*. (n.d.). Retrieved August 18, 2020, from https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf
- Dugal, P. (2001, September). *Cyberlaw In India: The Information Technology Act 2000 - Some Perspectives - Media, Telecoms, IT, Entertainment - India*. www.mondaq.com. https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technology-act-2000--some-perspectives
- Andrew, A. (2013, December 4). *National Cyber Security Policy 2013 – In a nutshell*. ClearIAS. https://www.clearias.com/national-cyber-security-policy-2013/
- PTI. (2013, July 2). *Govt releases National Cyber Security Policy 2013*. Livemint. https://www.livemint.com/Politics/DQ8gg6eCNeZwHJxt84rhMN/Govt-releases-National-Cyber-Security-Policy-2013.html
- *Cyber Laws in India*. (n.d.). Retrieved August 18, 2020, from https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf
- Joseph, V., & Ray, D. (2020, February). *Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence - Media, Telecoms, IT, Entertainment - India*. Www.Mondaq.Com. https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence?type=popular
- Varsha. (n.d.). *An Analysis on Cyber Crime in India*. Www.Legalserviceindia.Com. Retrieved August 19, 2020, from http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html
- cycles, T. text provides general information S. assumes no liability for the information given being complete or correct D. to varying update, & Text, S. C. D. M. up-to-D. D. T. R. in the. (n.d.). *Topic: Cybercrime in India*. Statista. Retrieved August 19, 2020, from https://www.statista.com/topics/5054/cyber-crime-in-india/#:~:text=In%20fact%2C%20according%20to%20a
- cycles, T. text provides general information S. assumes no liability for the information given being complete or correct D. to varying update, & Text, S. C. D. M. up-to-D. D. T. R. in the. (n.d.). *Topic: Cybercrime in India*. Statista. Retrieved August 19, 2020, from https://www.statista.com/topics/5054/cyber-crime-in-india/#:~:text=In%20fact%2C%20according%20to%20a
- Kumar, S. (2015). *Present scenario of cybercrime in INDIA and its preventions*.
- *OVERVIEW OF CYBER LAWS IN INDIA Index*. (n.d.). Retrieved August 18, 2020, from https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf
- https://www.researchgate.net/publication/228192670_Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review
- Keswani, M. (n.d.). *CYBER STALKING: A CRITICAL STUDY*. Retrieved August 19, 2020, from http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf

- *Cyber Attacks | Data Security Council of India*. (n.d.). Www.Sci. In. https://www.dsci.in/content/cyber-attacks
- *Notorious Cyber Security Attacks in India to Date*. (2020, March 30). Express Computer. https://www.expresscomputer.in/security/notorious-cyber-security-attacks-in-india-to-date/51714/
- Fischer, E. (2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*. https://fas.org/sgp/crs/natsec/R42114.pdf
- Hardeep Singh. (2015). *A Glance At The United States Cyber Security Laws*. Appknox.Com. https://www.appknox.com/blog/united-states-cyber-security-laws
- Joshi, D. (n.d.). *A comparison of legal and regulatory approaches to cybersecurity in India and the United Kingdom Shared under Creative Commons Attribution 4.0 International license*. Retrieved August 20, 2020, from https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf
- Timmsons, J., & Chabinsky, S. (2019, May). *Cybersecurity and the UK legal landscape | White & Case LLP*. Whitecase.Com. https://www.whitecase.com/publications/alert/cybersecurity-and-uk-legal-landscape
- Appknox, T. (n.d.). *A Glance At Australia's Cyber Security Laws*. Www.Appknox.Com. Retrieved August 20, 2020, from https://www.appknox.com/blog/glance-australias-cyber-security-laws