Journal of Positive School Psychology http://journalppw.com
2023, Vol. 7, No. 1, 782-800

# International Legislative Framework Of Cybercrimes- A Comparative Study Of India, Israel, And Usa

**Nuruddin Khan[1], Dr. Shobha Gulati[2]**

**Abstract:**

The following research paper will be discussing the legislative framework of cybercrimes in India, Israel, and USA. As India being a developing country and Israel, USA are having next level of technology in order to combat cyber-crimes in their relevant countries. The paper will be discussing the laws present in USA and Israel and on that note how India can develop their cyber-crimes laws and develop and excellent cyber security infrastructure to combat cyber criminals. The critical infrastructure of India is vulnerable at the instant of cyber criminals a through study of cyber laws of one USA and Israel will help in determining the basis for a strong cyber security infrastructure in India.

**Keywords:** cybercrime, cyberlaws, Information Technology, cyber security, critical infrastructure.

## I. INTRODUCTION

Information societies rely heavily on information technology availability, which is proportional to cyberspace security[3].The availability of information technology is constantly threatened by a variety of state and non-state entities.

The cyber-attack on the available information technology straddles the border between cybercrime and cyberwar, both of which have disastrous consequences in the physical world. The recent revelation of 'cyber-attack vectors' such as Stuxnet, Duqu, Flame, Careto, Heart Bleed, and others only emphasizes the vulnerability of information technology resources' confidentiality, integrity, and availability.

The issue is complicated further by the nature of cyberspace, which manifests itself in anonymity in space and time, quickness of actions resulting in unequal results disproportionate to the resources used, non-attribution of activities, and the lack of international borders. Because of these characteristics, "the transnational dimension of cybercrime offence arises when an element or substantial effect of the offence, or where part of the modus operandi of the offence is in another territory," raising issues of "sovereignty, jurisdiction, transnational investigations, and extraterritorial evidence," necessitating international cooperation[4]. The effectiveness of multinational efforts to combat cybercrime will be examined in this chapter.

International cybercrime frequently puts domestic and international law, as well as law enforcement, to the test. Because many countries' present laws are not designed to cope with cybercrime, criminals are increasingly turning to the Internet to avoid harsher sanctions or the difficulty of being tracked. Governments and industry in both emerging and developed countries have increasingly grasped the enormous hazards that cybercrime poses to economic and political security and public interests. However, the variety of types and forms of cybercrime makes it more difficult to combat. In this regard, combating cybercrime necessitates international collaboration. On a regional and international basis, various organizations and governments have previously collaborated to establish global standards of laws and law enforcement. Because they are the top two source countries of cybercrime, collaboration between China and the United

States has been one of the most notable recent developments.

Information and communication technology (ICT) plays a critical role in ensuring worldwide standards-based interoperability and security. In order to combat cybercrime, general countermeasures have been implemented, such as legal measures to improve legislation and technical measures to track down crimes over the network, Internet content control, the use of public or private proxy servers, computer forensics, encryption, and plausible deniability, among others. Because different countries' law enforcement and technical countermeasures differ, this article will mostly focus on international cooperation legislative and regulatory activities[5].

## II. ROLE OF INTERNATIONAL TREATIES, CONVENTIONS AND PROTOCOLS CONCERNING CYBERSPACE

The role of international treaties, conventions and protocols concerning the cybercrime which is a part of the cyber space is immense as it provides for a regulatory framework for the relevant countries who are part of the treaty or conventions. This will bind the countries to cater with the rules and regulations of the treaties, conventions, and protocols. The following are the some of the treaties, conventions and protocols that is worldwide accepted by majority of the countries. The following treaties, conventions set a backdrop for the comparative study of the legislative framework for this chapter.

- The United Nations is the most well-known of all international organizations. The United Nations Commission on International Trade Law (UNCITRAL) is the organisation in charge of harmonizing and unifying international trade law. UNCITRAL, based in Vienna, is a global legal organisation that has specialised on commercial law reform for over 40 years. The mission of UNCITRAL is to modernize and harmonise international business rules.

  In 1996, the UNCITRAL issued a Model Law on Electronic Commerce in response to the expanding use of electronic commerce and advanced communications technologies in international trade. This was based on a resolution passed by the United Nations General Assembly in 19851 encouraging nations and international organizations to take steps to safeguard legal security in the context of the widespread use of automated data processing in international trade.

- A World Summit on the Information Society (WSIS) was conducted in two phases, one in Geneva from December 1 to 12, 2003, and the other in Tunis from November 16 to 18, 2005, under the auspices of the United Nations, with the International Telecommunication Union playing a prominent role. Realizing the enormous potential of information and communication technologies in human development, world leaders declared their "common desire and commitment to build a people-centered, inclusive, and development-oriented information society, where everyone can create, access, utilize, and share information and knowledge, enabling individuals, communities, and peoples to achieve their full potential in promoting their sustainable development" at the summit in Geneva in 2003. One of the goals of the WSIS was to alleviate the digital divide, or the unequal distribution of the advantages of the information technology revolution between developed and poor countries and within societies.

- The United Nations Commission on Trade and Development (UNCTAD) is the primary trade and development agency of the United Nations General Assembly. UNCTAD has been engaged in advocating for the role and importance of information and communication technologies in development since 1998, when the General Assembly allocated it a special grant to pursue and promote electronic commerce initiatives.

- Cybercrime Convention in Europe

  The European Convention on Cybercrime, held in Budapest on November 23, 2001, took the most major approach to cybercrime and international cyber law. It is one of the most important international conventions addressing cybercrime and electronic evidence. The Council of Europe, Canada, Japan, South Africa, and the United States of America collaborated on the document. This Convention is divided into four chapters with a total of 48 articles. This Convention is a global treaty on criminal justice that provides States with Computer and internet-based criminalization of specific behaviors; procedural law for investigating cybercrime and admitting electronic evidence in any criminal case; and international collaboration between law enforcement and judicial authorities in the areas of cybercrime and electronic evidence. India’s stand on the convention its status as nonmember of the convention but India voted for a separate convention. Similarly, data sharing with foreign bodies is against the national sovereign of the country as termed by the Intelligence Bureau. Due to a lack of a strong legislative framework, India's data protection regulations are currently set with challenges and discontent. The legal framework consists of the following elements:

  The Information Technology Act of 2000 (IT Act) comprises legislation relating to cyber and IT-related laws in India (for example, sections 43A and 72A).

  Compensation for data breaches under Section 43A.

  Section 72A: Any knowingly and intentionally disclosing of information without the consent of the person concerned is punishable by imprisonment for up to three years.

  However, these provisions do not, on the one hand, protect against data breaches and, on the other, do not impose a privacy framework based on rights[6].

- Around 67 countries have signed the Convention, and ten international organizations (the Commonwealth Secretariat, European Union, INTERPOL, International Telecommunication Union, Organization of American States, UN Office on Drugs and Crime, and others) participate in the Cybercrime Convention Committee as members or observers. The Signatories' implementation of the Convention is the responsibility of the Committee. However, because India is not a signatory to the Convention on Cybercrime, it is not compelled to change or execute its domestic laws in line with the Convention.

- Computer and Computer-Related Crimes Model Law

  The Commonwealth Secretariat drafted a "Model Law on Computer and

Computer-Related Crime" for the Commonwealth's 53 member countries in October 2002. The Model Law expanded the scope of criminal culpability for offenses involving the internet and computer systems, as well as the use of unauthorized computer-related devices and practices.

In the context of cybercrime, the Model Law also introduced the idea of dual criminality. It indicates that if a person commits an infraction outside of his nation, the offence is punishable if the person's acts would be punishable under any law of the country where the offence was done. This idea of dual criminality could lead to charges or extradition. The Model Law has been used to draft domestic cyber laws in some Commonwealth member countries.

- Members of the World Trade Organization (WTO) adopted a declaration on global electronic commerce on May 20, 1998, during their Second Ministerial Conference in Geneva, Switzerland, due to the growing importance of internet commerce in global trade. The WTO General Council was directed to prepare a thorough work programme to evaluate all trade-related concerns arising from electronic commerce, and to deliver a progress report to the WTO's Third Ministerial Conference, according to the Declaration.

- The Group of Eight consists of eight countries (G8)

  The Group of Eight (G8) was primarily focused on prosecuting high-tech criminals and supporting technical and legislative improvements to combat worldwide computer crimes at the Denver Summit in 1997[7].

- The Okinawa Charter on Global Information Society, adopted at the Okinawa Summit in 2000, adopted the concepts of international collaboration and harmonization for cybercrime. The Group of Eight agreed on the importance and principles of privacy protection, free flow of information, and transaction security.

- WIPO, the World Intellectual Property Organization, is situated in Geneva and has 179 member states. WIPO's mission is to "advance the protection of intellectual property around the world through international collaboration." (WIPO Convention, Article 3) WIPO is the custodian of 23 international treaties and serves as a platform for worldwide IP policy development and administration. The migration of intellectual property to the digital realm is the order of the day, as IP is well-suited to digitalization. Because an infinite number of perfect copies may be generated and readily distributed across digital networks around the world, IP on the internet is insecure. As a result, it's understandable that online content, such as information, music, software, films, business procedures, databases, and so on, needs to be protected[8].

- The United Nations Convention Against Transnational Organized Crime (UNCTOC) was adopted by the United Nations in 2000. The Palermo Convention requires state parties to create domestic criminal charges that target organized criminal groups, as well as new procedures for extradition, mutual legal assistance, and law enforcement cooperation. Even though the treaty does not specifically mention cybercrime, its provisions are extremely pertinent.

- Article 34 of the 1989 Convention on the Rights of the Child mandates that states protect children from all forms of sexual exploitation and abuse, including prostitution and pornography.

- Protocol to the Convention on the Rights of the Child (Optional Protocol) (2001) – The sale of children, child prostitution, and child pornography are all addressed in this protocol, which is based on the CRC Convention. The production, distribution, dissemination, sale, and possession of child pornography are all prohibited under Article 3(1)(c). The Internet is mentioned in the Preamble as a source of child pornography distribution. Article 2(3) contains a definition of child pornography that is wide enough to include virtual images of minors[9].

## III. LEGISLATIVE FRAMEWORK OF CYBERCRIME IN INDIA

### India's Cyber Laws Statute

The Information Technology Act, 2000 ("IT ACT") governs cyber laws in India. The act's principal goal is Protection of private data and personal information of persons has become increasingly important in today's digital world as the number of IT-enabled services grows. In a broader sense, sensitive and vital information that is critical to national security need protection as well. The IT Act provides the infrastructure required to set up a secure system and limit access to confidential information.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Signatures in 2001. The general assembly's recommendations urged all states to integrate the Model Law on Electronic Signatures into their own state laws. The provisions on digital signatures are incorporated into the IT Law, which is in line with the UNICITRAL Model Law.

Crimes have also made their way into the digital sphere as a result of the advancement of information technology. Hacking, voyeurism, identity theft, and other cybercrimes and e-commerce frauds are becoming an increasing concern around the world. The IT Act identifies these offences and imposes appropriate penalties in order to deter them.

The Act also includes provisions that allow service providers to set up, maintain, and improve computerised facilities while also allowing them to collect and retain adequate service costs if the State and Central Governments give them permission[10].

It encompasses a wide range of topics, including data protection, data security, digital transactions, electronic communication, freedom of expression, and online privacy, to name a few. Regulation Of Information Technology Regulation Of Information Technology

The Information and Technology Act. It is based on the United Nations Model Law on Electronic Commerce (UNCITRAL Model), which was recommended by the United Nations General Assembly in a resolution dated January 30, 1997." In India, the legislation establishes a legal foundation for e-commerce. It focuses on and addresses digital crimes, sometimes known as cybercrime, as well as electronic trade. The legislation was passed in order to update some outdated laws and to give cybercrime jurisdiction. These laws have addressed issues such as electronic authentication, digital (electronic) signatures, cybercrime, and network service provider liability. In addition, the Information Technology Amendment Bill of 2008 amended the statute. The Indian Penal Code of 1860 and the Indian Evidence Act of 1872 were amended by the IT Act of 2000 to take into account the fast-changing technological landscape[11].

On October 17, 2000, the Cyber Law IT Act 2000 was enacted in India to address e-commerce and cybercrime. After the Indian Constitution was drafted, cyber legislation was enacted. As a result, it is a residuary topic managed by the Central Government that is not included in the three lists: Union, State, and Concurrent. The following is a list of characteristics of Cyber Law as defined by the act[12]:

- All electronic contracts entered into through secure electronic channels are legally binding.
- E-records and digital signatures are protected by security mechanisms.
- The Cyber Law Act establishes a procedure for appointing an adjudicating officer to conduct investigations.
- Digital signatures are legally recognized under the IT legislation act. The employment of an asymmetric cryptosystem and a hash function is also required for digital signatures.
- Without a warrant, top police officers and other officials are able to search any public case
- The act includes a provision to create a Cyber Regulation Appellate Tribunal. This tribunal hears appeals from the Adjudicating Officer's or the Controller's final orders. However, the only way to challenge the tribunal's decision is to go to the High Court.
- The act also establishes a Cyber Regulations Advisory Committee, which will advise the Controller and the Central Government.
- The Cyber Law Act's nature also applies to online crimes or offenses committed outside of India.
- There is also a provision for the Controller of Certifying Authorities to be established, which will license and regulate the Certifying Authorities' operations. In this situation, the Controller stores all of the digital signatures.

Areas where cyber law is not applicable

- The Central Government has started a number of initiatives and papers.
- Financial and legal acts performed by a person who has been lawfully designated as a Power of Attorney.
- Contract for the sale or transfer of real estate

Some of the most important sections under Information Technology act 2000

Section 3 - Authentication of electronic records

Section 4 - Legal recognition of electronic records

Section 5 - Legal recognition of Digital signature

Section 6 - Use of electronic records and digital signature in Government and its agencies

Section 17 - Appointment of controller of certifying authorities and other officials

Section 18 - Functions of controller of certifying authorities

Section 43 - Penalty for damages to Computer, Computer systems, unauthorized access, download of data, infecting with virus, denial of access etc

Section 44 - Penalty for failure to furnish information returns etc to the certifying authority

Section 48 - Establishment of Cyber appellate tribunal

Section 65 - Penalty for tampering with Computer source documents

Section 66 - Penalty for hacking of computer system

Section 66B - Penalty for receiving stolen computer or communication devices

Section 66C - Penalty for identity theft

Section 66D - Punishment for cheating by personation by using computer resources

Section 66E - Penalty for capture, transmit of publish images of a person without consent

Section 66F - Penalty for cyber terrorism

Section 67 - Punishment for publishing information which is obscene in electronic form

Section 67A - Penalty for publishing images containing sexual act or conduct

Section 67B - Penalty for child pornography

Section 70 - Penalty for securing access or attempting to secure access to a protected system

Section 71 - Penalty for misrepresentations

## Recent development in the cyber law in the year 2021[13]

The government of India has introduced new guidelines to regulate social media and OTT (over-the-top) platforms, as social media has become a newfound arena for everyone to communicate and express their ideas. It was set up to prevent hate speech from being used and spread. Another important motivation is to address people's grievances. They'll also track down the original sender of offensive remarks and tweets. This will be done either by the government or by a court order directed at that platform. The government has also stated that they will not support anything that could pose a threat to national security.

The requirement for social media and Over-the-Top (OTT) directions[14]

- Hate speech and defamation- Due to the unexpected surge in visibility on social media, it is critical to prevent hate speech and defamation, which can have serious consequences for the public.

- Misuse of content and misinformation- Misuse of personal content, including obscene content, on the same platforms is another important issue.

- Online Protection- There is a pressing need to safeguard women and men from sexual assaults that take place on online platforms.

There were no effective controls in place earlier to ensure that content on OTT Platforms was being watched by an appropriate age group. However, with the new rules and strong parental controls in place, content will now be sent to the appropriate audience.

As amendments where it had some drawbacks also

- Concerns about privacy- Any information can be exploited, and propaganda of any kind can harm digital publishers.

- Infringing on the Right to Freedom of Expression and Speech- This right, according to Article 19(a), empowers citizens to express any opinion through any means of communication, including speech and writing. Curbing and regulating social media is essentially depriving citizens of their First Amendment right to free speech and expression.

- ❖ Tracking problems- Personal data, such as WhatsApp communications, is essential for the government to trace hate speech and original originators of tweets. However, given WhatsApp's encryption, it's unclear how they'll be able to extract such information.

The government periodically publishes sets of Information Technology Rules (the IT Rules) under various parts of the IT Act to widen its scope. These IT Rules are focused on and regulate specific areas of data collection, transfer, and processing, and include the following, most recently:

- ❖ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[15], which mandate that companies holding sensitive personal data or information of users adhere to particular security requirements;

- ❖ 2021 Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, which ban content of a particular sort on the internet and restrict the role of intermediates, particularly social media intermediaries, in keeping their customers' personal data safe online;

- ❖ The Information Technology (Guidelines for Cyber Cafe) Rules[16], which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage; and the Information Technology (Guidelines for Cyber Cafe) Rules, which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage.

- ❖ The government can specify that certain services, such as applications, certificates, and licenses, be delivered electronically under the Information Technology (Electronic Service Delivery) Rules[17], which allow the government to specify that certain services, such as applications, certificates, and licenses, be delivered electronically.

And the most important one the compliance regulators which look after the compliance part

## CERT-In

The government established CERT-In under Section 70B of the IT (Amendment) Act 2008, which the Ministry of Electronics and Information Technology refers to as the "Indian Computer Emergency Response Team." CERT-In is a national nodal agency that handles computer security events as they happen. The following are the functions of the agency as defined by the Ministry of Electronics and Information Technology:

- Information about cybersecurity incidents is collected, analyzed, and disseminated.

- Cybersecurity incident forecasting and notifications;

- actions should be taken in the event of a cyber-attack;

- actions for cybersecurity incident response cooperation; and

- issuing guidelines, advisories, vulnerability notes, and white papers on information security practices, processes, cybersecurity incident prevention, response, and reporting[18].

## Appellate Tribunal for Cyber Regulations (CRAT)

In October 2006, the Ministry of Electronics and Information Technology formed CRAT

under Section 48(1) of the IT Act 2000. The Cyber Appellate Tribunal was renamed as a result of the IT (Amendment) Act 2008. (CRAT). Any individual who is aggrieved by an order made by the Controller of Certifying Authorities or an adjudicating officer under this Act may file an appeal with the CAT under the IT Act. According to Section 49 of the IT Act 2000, the CRAT is led by a chairperson who is selected by the central government by notification.

The chairperson was previously known as the presiding officer until the IT (Amendment) Act 2008. The modified Act specifies that the CRAT will consist of a chairperson and as many other members as the federal government may notify or appoint[19].

## Legislative framework of cybercrime In Israel

The key statutory and regulatory provisions that address cyber issues under Israeli law are:

- **The Computer Law, 1995[20];**

  The main law that deals with cybercrimes is the Computer Law (1995). This Law forbids the illegal access to computer material (Article 4), data and system interference (Article 2) and the misuse of devices (Article 6) alongside other offences.

  Some of the important sections in Computer Law 1995.

  Section 4 – unlawful penetration into computer material -," A person who unlawfully penetrates computer material located in a computer, shall be liable to imprisonment for a period of three years; for this purpose, "penetration into computer material" - penetration by means of communication or connection with a computer"

  Section 6 – computer virus- "(a) A person who composes a software program in a manner that enables it to cause damage to or disruption of a non-specific computer or computer material, in order to unlawfully cause damage to or disruption of a computer or computer material, whether specific or non-specific, shall be liable to imprisonment for a period of three years. (b) A person who transfers software program to another, or who infiltrates another's computer with, a software program that is capable of causing damage or disruption as aforesaid in Subsection (a), in order to unlawfully cause the aforesaid damage or disruption, shall be liable to imprisonment for a period of five years"

- **The Privacy Protection Regulations (Data Security), 2017 (based on the 1981 Privacy Protection Law)[21];**

  The regulations apply to both the private and public sectors, and they provide organizational procedures to ensure that data security is integrated into the management processes of all businesses that process personal data.

  The rules are the result of a thorough examination of relevant legislation, standards, and related Israeli and international recommendations. The laws were put in place following thorough consultation with the Israeli people, particularly those who might be affected by them.

  The regulations are projected to significantly improve Israel's data security since they are both flexible, concrete, and particular to the point where they provide enterprises with regulatory certainty and practical

instruments that are easy to execute. With the legislation' implementation in May 2018, we anticipate a new age in which Israel's privacy protection will be greater than ever.

- **The Emergency Regulations, 2020 on the and processing of 'technological information' on Israeli citizens to stop the spread of COVID-19[22];**

  On March 15 and 17, 2020, Israel's transitional government headed by Prime Minister Binyamin Netanyahu approved two separate emergency regulations that allow, among other things, the use of digital surveillance by the General Security Service (GSS) and provide expanded search authority to the Israel Police to combat the spread of the coronavirus. The GSS is responsible for "safeguarding state security … and promoting other vital state interests for the national security of the state, all as prescribed by the government and subject to law.

The Cyber Defence and National Cyber Directorate Bill, which is under negotiation in the Israeli Knesset (Parliament)[23]; and

The Israel National Cyber Directorate is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace. We provide incident handling services and guidance for all civilian entities as well as all critical infrastructures in the Israeli economy, and works towards increasing the resilience of the civilian cyber space.

The Copyright Law, 2007 – Amendment 5 (2019) on the procedure for the disclosure of the identity of internet users under certain circumstances[24].

The law acknowledges copyright as being applicable to original productions – literary, artistic, dramatic, or musical – as well as recordings, as long as they have a connection to Israel or are protected by a decree issued by the Minister of Justice in compliance with an international convention.

The law broadens the range of uses that are either permitted or considered fair use. Use of a creation in legal or administrative proceedings; copying of a creation that is deposited by law for public review; indirect use of a creation by inclusion in another creation such as a photograph, a film, or a record; copying of computer software for backup or maintenance; and use of a creation for broadcast; as part of an educational activity; in libraries, and so on are among them. The law extends copyright protection to the creator's lifetime or, in the case of a joint creation, the last remaining creator's lifetime, to 70 years after his death. Anonymous creations are protected for 70 years, while records and creations owned by the state are protected for 50 years. The law also acknowledges moral rights, which include the creators' rights to name their creation and to be safeguarded from any change or action that could jeopardize the creator's dignity or reputation.

The 2017 Privacy Protection Regulations (Data Protection) outline the levels of security required for several types of information, based on the sensitivity of the data as specified by the regulations. They are divided into the following categories:

- databases that are subject to a basic level of security;
- databases with a medium level of security; and databases with a low level of security.
- databases that require a high level of security

Outsourcing is addressed in paragraph 15 of the Privacy Protection Regulations (Data Security) 2017, which stipulates the responsibility of the outsourced service provider in terms of cybersecurity. The regulations govern the agreement between an Israeli business and its outsourced service provider (which could be a non-Israeli entity) for databases that must be kept secure.

## Enforcement and penalties under the cyber laws in Isreal[25]

The following criminal consequences for cybercrime are set out in the Israeli Computer Law of 1995. (Eg, hacking, theft of trade secrets).

Paragraph 3 stipulates a five-year prison sentence for anyone who:

write software, transfer software to or store software on a computer in such a way that its use will result in false information or false output, or operate a computer using such software; or transmit or store false information or act on information in a way that results in false information or false output; or write software, transfer software to or store software on a computer in such a way that its use will result in false information or false output.

In this context, 'false information' and 'false output' refer to data and output that, depending on their application, may be misleading.

Except if the unlawful entry of a computer or the illegal infiltration of material found on a computer is based on the Wiretap Act of 1979, illegal intrusion of a computer or illegal infiltration of material found on a computer is punishable by three years in prison under paragraph 4.

Anyone who undertakes an act banned by Section 4 in order to commit an offence under any legislation would be punished to five years in prison, according to paragraph 5.

Anyone who alters software in such a way that it is capable of causing harm or disruption to a computer or content stored on a computer, whether stated or unspecified, is subject to paragraph 6 of the law. will be sentenced to three years in prison; and anyone who transfers or instals software capable of causing damage or disruption on another's computer in order to cause unlawful damage or disruption will be sentenced to five years in jail.

The Israeli Privacy Protection Authority is in charge of cyber-related civil matters including personal information and data security breaches (PPA). Any personal data breach must be reported to the PPA under the Privacy Protection Regulations (Data Security) of 2017. The PPA is empowered by law to enforce and supervise any organisation that is required by law to register its databases in Israel. Under the Privacy Protection Law and its regulations, the PPA has the legal authority and reason to apply administrative fines and entry and search orders, which it does in select situations. The PPA ensures that any database must be registered in accordance with the legislation. The applicant must provide all of the following information on the database registration application form:

- the data owner (equivalent to a data controller); and
- the registered database manager's personal information, who bears legal personal liability.

If the management fails to supervise the organization's data control, he or she is legally liable.

Through the Israeli Cyber Emergency Response Team, the Israel National Cyber Directorate monitors national civil cyber threats in order to improve Israel's defence and build a shared basis of civil knowledge on data protection. The National Cyber Directorate is not authorised to enforce any laws.

The Cyber Authority and other government entities are aggressively addressing and enforcing national and international cybersecurity issues. These organisations have unrestricted ability to take whatever actions are necessary to avoid national or international security threats.

The Israeli police force has developed a cybercrime central section to combat crimes such as paedophilia, drug trafficking, credit card fraud, and identity theft that occur on virtual platforms. The cybercrime unit is authorised to investigate and prosecute.

Cyber-related guidelines and processes have been implemented by other government-supervised businesses, such as banks and insurers, to meet worldwide requirements.

With the exception of homeland security problems, none of the aforementioned authorities or government entities have extraterritorial authority over firms that are not based in Israel and do not have a local presence (including subsidiaries and related companies).

## Legislative framework of cybercrime in USA[26]

Computer fraud and abuse are prohibited under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. It's a piece of cyber-security legislation. It safeguards federal computers, bank computers, and Internet-connected systems. It protects them from trespassing, threats, vandalism, spying, and being exploited as fraud instruments by the corrupt. It is not a comprehensive provision; rather, it fills in the fractures and holes left by other federal criminal laws. This is a quick rundown of the CFAA and some of its federal statutory partners, including the Identity Theft Enforcement and Restitution Act, P.L. 110-326, 122 Stat. 3560, and its revisions (2008).

The seven provisions of subsection 1030(a) in their current form prohibit

18 U.S.C. 1030(a)(3); computer trespassing (e.g., hacking) in a federal computer;

18 U.S.C. 1030(a)(2); computer trespassing (e.g., hacking) resulting in exposure to certain governmental, credit, financial, or computer-stored information;

18 U.S.C. 1030(a)(5): destroying a government computer, a bank computer, or a computer used in, or influencing, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, denial of service attack, and other kinds of cyber-attack, cybercrime, or cyber terrorism);

18 U.S.C. 1030(a)(4), perpetrating fraud that includes unauthorised access to a government computer, a bank computer, or a computer utilised in, or affecting, interstate or foreign commerce;

18 U.S.C. 1030(a)(7); threatening to harm a government computer, a bank computer, or a computer utilised in or affecting interstate or foreign commerce;

18 U.S.C. 1030(a)(6), for trafficking in passwords for a government computer or when the trafficking affects interstate or foreign commerce; and 18 U.S.C. 1030(a)(7), for trafficking in passwords for a government computer or when the trafficking affects interstate or overseas business.

18 U.S.C. 1030(a): Using a computer to commit espionage (1).

Attempting or conspiring to commit any of these actions is illegal under Section 1030(b). Subsection 1030(c) lists the penalty for committing crimes, which vary from a year in jail for ordinary cyberspace trespassing to a maximum of life in prison for intentional computer damage that results in death.

The Secret Service's investigation jurisdiction is preserved by Section 1030(d). Common definitions are provided in section 1030(e).

Section 1030(f) does not apply to law enforcement efforts that are otherwise legal. Victims of these offences have a civil cause of action under Section 1030(g). The forfeiture of tainted property is allowed under Sections 1030(i) and (j).

### Critical Infrastructure Information Act

The Critical Infrastructure Information Act of 2002 (CII Act) seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation's vulnerability to terrorism. The Homeland Security Act of 2002 established a framework that allows individuals of the private sector and others to voluntarily submit sensitive information about the Nation's Critical information to Department of Homeland security with the certainty that the information will be shielded from public exposure if it meets specific criteria[27].

### Health Insurance Portability and Accountability Act of 1996 (HIPAA)[28]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that mandated the adoption of national standards to prevent sensitive patient health information from being revealed without the consent or knowledge of the patient. The HIPAA Privacy Rule was developed by the US Department of Health and Human Services (HHS) to implement HIPAA's provisions. A subset of information covered by the Privacy Rule is protected under the HIPAA Security Rule.

Individuals and organizations that fall under the following categories are considered covered entities under the Privacy Rule:

Every healthcare professional, regardless of practice size, who electronically communicates health information in connection with specific transactions is a healthcare provider. Claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has defined criteria under the HIPAA Transactions Rule are examples of these transactions.

Health plans are organizations that offer or pay for medical treatment. Health insurers, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers are all examples of health plans (excluding nursing home fixed-indemnity policies). Employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans are all examples of health plans.

A covered entity is not a group health plan with less than 50 participants that is solely administered by the employer who established and maintains the plan.

Entities that convert nonstandard information received from another entity into a standard (i.e., standard format or data content), or vice versa. Individually identifiable health information is often only received by healthcare clearinghouses when they are acting as a business associate for a health plan or a healthcare provider.

Individually identifiable health information is used or disclosed by business associates (other than members of a covered entity's workforce) to perform or provide operations, activities, or services for a covered entity. Claims processing, data analysis, usage review, and billing are examples of these functions, activities, or services.

### Gramm-Leach-Bliley Act[29]

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing

practices to their customers and to safeguard sensitive data.

## FISMA[30]

In December 2002, the Federal Information Security Management Act (FISMA) [FISMA 2002], which was enacted as part of the E-Government Act (Public Law 107-347) was signed into law. FISMA 2002 mandates that each federal agency creates, document, and implement an agency-wide information security program for all information and systems that support the agency's operations and assets, including those provided or maintained by another agency, contractor, or other sources.

The Federal Information Security Modernization Act of 2014 modifies FISMA 2002 by making a number of changes to improve federal security practices in response to emerging security issues. These improvements result in less overall reporting, a stronger use of continuous monitoring in systems, a greater focus on agencies for compliance, and reporting that is more focused on security incident issues. FISMA 2014 also mandated that the Office of Management and Budget (OMB) amend/revise OMB Circular A-130 to minimize inefficient and unnecessary reporting, as well as to reflect changes in the law and technological advancements.

FISMA, like the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), places a strong emphasis on risk-based security. The Office of Management and Budget (OMB), in support of and to reinforce FISMA, has issued Circular A-130, "Managing Federal Information as a Strategic Resource," which requires executive agencies within the federal government to:

- Make a security plan.
- Assign security duty to the relevant officials.
- Review the security controls in their systems on a regular basis.
- Authorize system processing before beginning operations and on a regular basis thereafter.

FISMA applies to Federal agencies, contractors, or other sources that provide information security for the information and information systems that support the operations and assets of the agency.

## Electronic Communications Privacy Act of 1986 (ECPA)[31]

The Electronic Communications Privacy Act (ECPA) of 1986 combines the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act. The ECPA revised the Federal Wiretap Act of 1968, which covered interception of conversations over "hard" telephone lines but not computer and other digital and electronic communications. Several following pieces of legislation, such as the USA PATRIOT Act, explain and update the ECPA in order to keep up with the growth of new communications technology and methods, including loosening restrictions on law enforcement access to stored communications in some situations.

General Provisions

The ECPA, as modified, safeguards wire, oral, and electronic communications while they are in use, in transit, and when they are stored on computers. Email, phone chats, and data saved electronically are all covered by the Act.

Civil Liberties and Civil Rights

"The SCA's structure incorporates a number of classifications that reflect the drafters' assessments of which types of information pose higher or lesser privacy risks. The drafters, for example, identified a higher level of privacy concern in the content of retained emails than in subscriber account information. Similarly, the

drafters considered that computing services that were 'open to the public' required more stringent [sic] regulation than services that were not... The [Act] provides varied degrees of legal protection based on the perceived relevance of the privacy interest at hand, in order to preserve the wide range of privacy interests outlined by its drafters. A subpoena can be used to collect some information from providers; other information requires a special court order; and still more information requires a search warrant. Furthermore, some legal processes need the subscriber to be notified, while others do not."

The Act follows a general policy of providing more privacy protection for content with higher privacy concerns.

## IV. COMPARATIVE STUDY OF INDIA, USA, AND ISRAEL

| **INDIA** | **ISRAEL** | **USA** |
|---|---|---|
| 1.The Information Technology Act, 2000 ("IT ACT") governs cyber laws in India. The act's principal goal is to give electronic trade legal legitimacy and to make filing electronic records with the government easier | The main law that deals with cybercrimes is the Computer Law (1995). This Law forbids the illegal access to computer material (Article 4), data and system interference (Article 2) and the misuse of devices (Article 6) alongside other offences | Computer fraud and abuse are prohibited under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. It's a piece of cyber-security legislation. It safeguards federal computers, bank computers, and Internet-connected systems. It protects them from trespassing, threats, vandalism, spying, and being exploited as fraud instruments by the corrupt |
| 2. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[32], which mandate that companies holding sensitive personal data or information of users adhere to particular security requirements. | The Privacy Protection Regulations (Data Security), 2017 (based on the 1981 Privacy Protection Law)<br><br>The regulations apply to both the private and public sectors, and they provide organizational procedures to ensure that data security is integrated into the management processes of all businesses that process personal data. | Critical Infrastructure Information Act<br><br>The Critical Infrastructure Information Act of 2002 (CII Act) seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation’s vulnerability to terrorism |

| | | |
|---|---|---|
| 3. Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) 2021 | The Emergency Regulations, 2020 on the and processing of ‘technological information' on Israeli citizens | Health Insurance Portability and Accountability Act of 1996 (HIPAA)<br><br>The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that mandated the adoption of national standards to prevent sensitive patient health information from being revealed without the consent or knowledge of the patient |
| 4. The Information Technology (Guidelines for Cyber Cafe) Rules[33], which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage; and the Information Technology (Guidelines for Cyber Cafe) Rules, which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage. | The Cyber Defence and National Cyber Directorate Bill, which is under negotiation in the Israeli Knesset (Parliament) | Gramm-Leach-Bliley Act<br><br>The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. |
| 5. The government can specify that certain services, such as applications, certificates, and licenses, be delivered electronically under the Information Technology (Electronic Service Delivery) Rules[34], which allow the government to specify that certain services, such as applications, certificates, and | The Copyright Law, 2007 – Amendment 5 (2019) on the procedure for the disclosure of the identity of internet users under certain circumstances | FISMA<br><br>In December 2002, the Federal Information Security Management Act (FISMA) [FISMA 2002], which was enacted as part of the E-Government Act (Public Law 107-347) was signed into law. FISMA 2002 mandates that each federal agency create, document, and implement an agency-wide information |

| | | |
|---|---|---|
| licenses, be delivered electronically. | | security program for all information and systems that support the agency's operations and assets, including those provided or maintained by another agency, contractor, or other sources |
| | 5.The 2017 Privacy Protection Regulations (Data Protection) outline the levels of security required for several types of information, based on the sensitivity of the data as specified by the regulations. They are divided into the following categories:<br><br>databases that are subject to a basic level of security;<br><br>databases with a medium level of security; and<br><br>databases with a low level of security.<br><br>databases that require a high level of security | Electronic Communications Privacy Act of 1986 (ECPA)<br><br>The Electronic Communications Privacy Act (ECPA) of 1986 combines the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act. The ECPA revised the Federal Wiretap Act of 1968, which covered interception of conversations over "hard" telephone lines but not computer and other digital and electronic communications. |

As we compare the legislative framework of the all the three countries it gives a clear picture that India is lacking way behind in relation to cyber legislation specially in relation to the Data protection as Israel and USA have separate legislation on the following topic. A strong legislative action is required from the makers of law in India.

The most important is the critical infrastructure Israel and USA have their own legislations on the critical infrastructure of on the other hand India is lacking a legislation as the critical infrastructure is the most important of all. Any kind on the nuclear power plants or the grid lines of the nation or on the stock exchanges can cripple the economy for many months.

Privacy related laws are missing in India as compared to Israel and Usa as they have their own legislation on the privacy related issues in their respective country.

### Cyber-crime related model that should be adopted by India to become one of the best countries to combat cybercrime

The model prevailing in Israel and USA makes them one of the best countries in relation to cybercrime. Similar model could be adopted by India to strengthen the cybercrime rin the country. They are as follows:

1. Advanced technology parks should be established in relation to crime related to internet and development of public authorities in digital production.

2. Digital production and network safety instruction should be imparted to the students from the school level. Specialization in Graduation should be brought in relation to cyber security/ web security in the curriculum of the students at college level.

3. Research organizations should be set up, if research organization come together, it can make India super power in digital protection.

## V. CONCLUSION & SUGGESTIONS

The worldwide idea of digital violations has begun a battle against them both broadly and universally. Global collaboration is exceptionally required in these seasons of steady logical improvements in PC and organization innovation and the dangers forced by digital crooks. All the previously mentioned worldwide systems are pointed towards accomplishing that collaboration among different nations to battle digital wrongdoings and direct digital law.

India, despite the fact that not a signatory to the Convention on Cyber Crimes, is additionally making an honest effort to battle digital wrongdoings. With the establishment of the IT Act, 2000, and the IT (Amendment) Act, 2008 different advancements identified with digital law have happened in India. In any case, legitimate execution of digital law is as yet required as numerous individuals don't know about the dangers the web can present.

To make India a super power in relation to cybercrime like USA and Israel we have to adopt the approach and methods adopted by them which is mentioned in the chapter for development of cyber security and protection from cybercrimes at national level.

## REFERENCES

[1] Research Scholar, Lovely Professional University, Punjab, India
[2] Associate Professor, Lovely Professional University, Punjab, India
[3] M. Gercke, "Understanding cybercrime: a guide for developing countries," International Telecommunication Union (Draft), vol. 89, p. 93, 2011.
[4] O.-e. I. E. G. o. Cybercrime, "Comprehensive Study on Cyber Crime," UNODC2013.
[5] Apoorva Bhangla and Jahanvi Tuli , A Study on Cyber Crime and its Legal Framework in India, 4 (2) IJLMH Page 493 - 504 (2021), DOI: http://doi.one/10.1732/IJLMH.26089
[6]https://www.drishtiias.com/daily-updates/daily-news-analysis/convention-on-global-cybercrime
[7] https://blog.ipleaders.in/regulatory-framework-for-cyber-crimes/
[8] Apoorva Bhangla and Jahanvi Tuli , A Study on Cyber Crime and its Legal Framework in India, 4 (2) IJLMH Page 493 - 504 (2021), DOI: http://doi.one/10.1732/IJLMH.26089
[9] https://netlawgic.com/cyber-crime-conventions 07 Feb 2022 10am
[10] https://www.lawyered.in/legal-disrupt/articles/diving-information-technology-act-2000-salient-features-and-2008-amendments-rashi-suri

[11] https://learn.lawdocs.in/analysis-of-indian-legal-framework-for-cyber-crimes
[12] https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence
[13] https://www.jigsawacademy.com/blogs/cyber-security/what-is-cyber-law/
[14] https://www.livelaw.in/law-firms/law-firm-articles-/it-rules-2021-digital-media-ott-platforms-186065
[15] meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
[16] meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
[17] meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf
[18] www.cert-in.org.in.
[19]https://www.meity.gov.in/writereaddata/files/The%20Cyber%20Appellate%20Tribunal%28Chairperson_Members%29%20Rules%2C%202009.pdf.
[20] https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/israel/
[21] https://www.gov.il/en/Departments/General/data_security
[22] https://www.loc.gov/item/global-legal-monitor/2020-03-18/israel-emergency-regulations-authorize-digital-surveillance-of-coronavirus-patients-and-persons-subjected-to-home-isolation/
[23] https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page
[24] https://www.loc.gov/item/global-legal-monitor/2007-12-02/israel-new-copyright-law
[25] https://www.mondaq.com/technology/1070854/cybersecurity-comparative-guide
[26] https://www.everycrsreport.com/reports
[27] https://itlaw.fandom.com/wiki/Critical_Infrastructure_Information_Act_of_2002
[28] https://www.cdc.gov/phlp/publications/topic/hipaa.html
[29] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
[30] https://csrc.nist.gov/projects/risk-management/fisma-background
[31] https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285
[32] meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
[33] meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
[34] meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf