Cyber Threats and Cyber Laws

Lesson 3

KEY CONCEPTS

■ Cyber Threats ■ Cyber Warfare ■ Cyber Crime ■ Cyber Terrorism ■ Cyber Threat Hunting ■ Digital Forensics ■ Digital Intellectual Property ■ Data Protection

Learning Objectives

To understand:

- Meaning and Types of Cyber Threats
- What is Cyber Warfare
- Meaning and Kinds of Cyber Crimes
- What constitute Cyber Terrorism
- Significance of Cyber Security and its Mechanism
- Types of Cyber Threats
- Meaning and Process Cyber Threat Hunting
- What is Digital Forensics?
- Concept of Digital Intellectual Property
- Legal purview of the Liability of online platform/intermediaries
- Artificial Intelligence vis-à-vis Data Protection
- Other inter-related concepts

Lesson Outline

- Introduction
- Cyber Threats Cyber Warfare
- Cyber Crime
- Cyber Terrorism
- Types of Cyber Threats/ Attacks
- Cyber Threat Hunting and Digital Forensics
- Digital Intellectual Property
- Liability of online platforms
- Laws applicable to AI and Cyber Laws
- Cyber Security Framework (NCFS)
- Data Protection and AI: Laws and Regulations
- Case Studies
- Lesson Round-Up
- Test Yourself
- List of Further Readings

REGULATORY FRAMEWORK

- Information Technology Act, 2000
- Overview of IT Act, 2000
- The important provisions of IT Act, 2000
- Positive and negative aspects of IT Act, 2000
- Information Technology Rules (IT Rules), 2011
- Companies Act, 2013
- Indian Penal Code, 1860

INTRODUCTION

It was around 900 BC, when for the first time, postal service was introduced in China for governmental use and in 14 BC, the Romans established their 'Postal Services' as means of communication.[1] Since that time, information has continued to be transferred and conveyed through traditional means of communication like postal communication, telephone and fax etc. The development of electronic computers with the support of internet in 1950 has elevated the process of transfer of information from one end to the other. The beginning of point-to-point communication[2]; development of Telnet in 1960s and 1970s; the release of governmental control over internet by America in 1994 and the birth of 'www' i.e. the World Wide Web in 1994 has globally changed the entire process of transferring, sharing and relocating the information.[3] The shift from traditional modes of information to information technology, i.e. a term used to denote the use of technology to communicate, transfer data and process information, has been swift owing to digitalization, which has led to emergence of unprecedented growth of data.

Such developments in the field of information technology have gone a long way towards enhancing the ability of individuals to transfer information liberally and without bottlenecks such as time consumption, congestion of roots, non-connectivity etc., from which postal communication, telecommunication, fax and other modes of communication often suffered. Additionally, information technology has ensured instant access and relocation of information while avoiding the limits and fetters encountered in the traditional means of communication.

Advent of information technology has not only provided us the assorted means of communicating our information at an inclusive platform but it has also ensured quick communication of information. Information technology can be described as any technology that helps us to produce, manipulate, store, communicate, and/or disseminate information. Usually 'Information' refers to data that has been organized and then communicated.[4] In general terms, information technology is a broad term used to refer to any form of technology used to create, transfer, or store information in all of its various forms, be it text, images, sound, multimedia files.[5]

In the system of information and communication technology, it is the use of internet[6] that serves the major function of conveying information at global level. Internet is said to be one of the greatest developments in the province of information and communication advancement. Internet[7] as a backbone of information technology has

1. The History of Communication. (Jan. 2, 2013), http://inventors.about.com/library/inventors/bl_history_of_communication.htm.

2. In telecommunications, a point-to-point connection refers to a communications connection between two nodes or endpoints. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other.

3. Brief History of Internet. (Sept. 9th 2013), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

4. Allen and Morton, Information Technology and the Corporation of the 1990s, New York, Oxford University Press (1994).

5. Longley et al., Dictionary of Information Technology, Macmillan Press, 164 (2nd ed. 2012).

6. In legal parlance, Internet can be defined as an electronic communications network that connects computer networks and organizational computer facilities around the world. (Jan. 7, 2013), http://www.statelawyers.com/Practice/Practice_Detail.cfm/PracticeTypeID:56.

7. Internet is an arrangement of connected computers, which lets the computer users all over the globe exchange data.

touched almost every aspect of life including telecommunication, finance, governance, health care, education etc.[8] at a global platform. India is not an exception to the revolutionary effects of internet and information technology; as per Internet World Statistics, India alone has an internet user base of over 100 million.[9] Internet has not only facilitated the easy exchange and management of information but also proved a far easier medium of transferring data on a global platform just in blink of an eye. In this way, information technology has brought revolutionary changes in the approach of social interactions among people, business world, government agencies, regulatory perspective and control mechanism to an entirely new synchronization.

Information technology has served various advantages to human kind[10] in the form of (i.) speedy social interaction;[11] (ii.) growth of business; (iii.) enhancing the educational capacity of youth[12] etc. Additionally, advantages of information and communication technology can also be seen in terms of email (an essential communication tool for individuals as well as for businesses), availability of information and resources (availability of huge amount of information about every subject like law, government services etc.), services (like banking, insurance etc.), e-commerce (sale and purchase over internet), software downloads etc., which provide ease to the human community in almost all spheres of life.

Pros and Cons of Information Technology	
PROS:	**CONS:**
• Globalization	• Digital Divide
• Communication	• Cyber crime
• Cost effectiveness	• Security threat
• Comfortable life	• Privacy concerns
• Bridging cultural gap	• Unemployment
• Easy accessibility of information	• Intellectual property crime
• Unlimited data storage and backup	• Cyber terrorism
• Online booking of ticket	• Computer related diseases

However, it has been righty said that '*with boon goes the bane'*, and this phrase is also true for information technology. At one side, this easy medium of transferring data and facilitating quicker flow of communication has given birth to numerous modes of communication and transaction; on the other side, various dark sides are being observed under IT enabled and electronic transactions. The major threats among them are Cyber Crimes and Cyber Attacks. Hence, in order to control the mechanism of cyber-crimes and cyber-attacks, cyber law has evolved gradually which ensures cyber security in cyber sphere. Hence this chapter inter-alia aims to provide understanding on the following:

8. Shyam, R. and Bhoria, A., Information Technology (Internet): Effects on Social Participation and Well-Being of Users, Journal of Indian Academy of Applied Psychology, Vol. 37, No.1, 157-162 (2011).

9. Internet Usage Stats and Telecommunications Market Report. (Mar. 27, 2012), http://www.internetworldstats.com/asia/in.htm.

10. Scott et al., Internet Benefits: Consumer Surplus and Net Neutrality, Institute of Policy Integrity, New York University School of Law, (2011). (Jan.7, 2013), http://policyintegrity.org/files/publications/Internet_Benefits.pdf; See also, Gary James on Advantages and Disadvantages of Online Learning. (Jan. 7, 2013), http://www.leerbeleving.nl/wbts/nieuw_basics/addis.pdf.

11. Through internet, communication is faster and easier in comparison to the traditional means of communication, so people on opposite sides of the world can speak to each other over the internet as if they were speaking in person. Apart from this the internet boosts the spread of culture, since all type of communications are made possible through internet.

12. Latchman et al., Information Technology Enhanced Learning in Distance and Conventional Education, IEEE Transactions on Education, Vol. 42, No. 4 (1999).

- Cyber Threats;
- Cyber Warfare;
- Cyber Crimes;
- Cyber Terrorism;
- Cyber Security;
- Cyber Laws;
- AI vis-à-vis Data Protection; and
- Other inter-related concepts.

Source: Remya Ravindran

CYBER THREATS

Cyber security is a serious concern of present times as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the network and security systems. Individuals, small-scale businesses or large organizations, are all being impacted. Therefore, all of these firms, whether IT or non-IT firms, have understood the importance of Cyber Security and focus on adopting all possible measures to deal with cyber threats.

Definition of Cyber Threats

A cyber threat (*also known as cybersecurity threat*) is defined as a malicious act that seeks to steal or damage data or disrupt the digital wellbeing and stability in general. Cyber threats include a wide range of attacks including but not limited to data breaches, computer viruses, denial of service, and numerous other attack vectors. Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data.

Sources of Cyber Threats

Cyber threats may come from a variety of places, people, and contexts. In general, following are the major sources of cyber threats:

- Nation-states
- Terrorists
- Industrial spies
- Organized crime groups
- Unhappy insiders
- Hackers
- Business competitors

CYBER WARFARE

As per Britannica Dictionary, Cyberwar (also called cyberwarfare or cyber warfare) is defined as a war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually a war waged against government and military networks in order to disrupt, destroy, or deny their use of systems to disrupt operations, particularly for tactical, military and cyberespionage reasons.

AIIMS cyber attack raises red flags in national security

India News

Published on Dec 07, 2022 07:21 AM IST

The government has been informed that China was testing the resilience of the Indian system as part of hybrid warfare when Indian Air Force attacked Balakot on February 26, 2019 as a retaliation for the Pulwama terror strike by the Pakistan- based Jaish-e-Mohammed terror group.

Computers and the networks that connect them are collectively known as the domain of cyberspace. Everything that modern society needs to function—from critical infrastructures and financial institutions to modes of commerce and tools for national security—are dependent to a major extent upon cyberspace. Therefore, the threat of cyberwar and its purported effects are a source of great concern for governments and militaries around the world. With the dependability on cyberspace, the day is not far where cyber war is expected to be as fatal as a real war between the nations.

Source: The Hindustan Times, December 07, 2022

CYBER CRIME[13]

With the help of Information and Communication Technology (ICT), people are more interconnected than ever before. Though the dependability on ICT is full of advantages, yet connectivity leaves us vulnerable to the risks of fraud, theft, abuse including cyber-attack. Cyber-crime is any criminal activity that involves a computer, networked device or a network. In general, most cybercrimes are carried out in order to generate profit for the cybercriminals, yet some of cybercrimes are carried out against computers or devices directly to damage or disable them. It can be briefly state that the spectrum of cyber threats is limitless and cyberattacks can come in the form of viruses, malware, email phishing, social media fraud and alike. Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels. A brief description of the impact of cyber-crime is as below:

- Organized cybercrime, state-sponsored hackers, and cyber espionage (a type of cyber-attack in which an unauthorized user attempts to access sensitive data or intellectual property for economic gains, competitive advantage or political reasons) can pose national security risks to our country and our critical infrastructure.
- Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.
- Vulnerability to data breach and loss increases if an organization's network is compromised. Information about a company, its employees, and its customers can be at risk.
- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

CYBER TERRORISM

Cyber terrorism is the convergence of terrorism and cyberspace. The term 'cyber terrorism' was first coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. But its usage was better understood during the 9/11 attacks that took place in the United States of America. In general, it is difficult to define cyber terrorism. Yet, U.S. Federal Bureau of Investigation has defined cyber terrorism as a premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence

13. Students to note that Cyber Crime is descriptively discussed in Chapter 4 of this Study Material. Hence under this sub-section, we are only providing brief views on Cyber Crime.

against clandestine agents and subnational groups. The main aim behind cyberterrorism is to cause harm and destruction. Hence, in brief cyber terrorism signifies use of the internet to carry out violent activities that result in or threaten the loss of life or substantial physical injury to accomplish political or ideological advantages through threat or intimidation.

Cyber Terrorism vis-à-vis Cyber Crime[14]

Cyber terrorism is also named as electronic terrorism, information warfare or Cyber warfare. The basic objective of cyber-attack is hacking, generally to satisfy the ego of hackers of creating terror. The objective of Cyber terrorism is to generate the feeling of terror in the mind of the cyber victims. Cyber terrorism includes commission of acts of destruction, alteration, acquisition and acts of transmission of information systems, programs, computers and networks against the following:

- Defence forces
- Financial Infrastructure
- Civilians
- Destructions of supervisory control and data acquisition system of smart cities
- Exploration of smart army etc.

Basic elements of Cyber Terrorism

- Perpetrator (which may include a group of people) i.e. Cyber Criminal
- Place - Cyber Space
- Action/Method or mode of action – Any Cyber technique
- Tools - Cyber Arsenal or Armory
- Targets - e.g. Government, Company, Place, Individuals, Administration or Digital Infrastructure
- Affiliations-actual or claimed
- Motivations-social, religious, communal or revenge.

Legal Provisions dealing with Cyber terrorism

There is no specific legislation or law which deals with cyber terrorism in India. In 2018, amendments were made to the Information Technology Act, 2000 (hereinafter referred to as 'IT Act'), which led to insertion of Section 66F, which deals with Cyber Terrorism, in the Act. Section 66F is the only provision which deals with and covers any act committed with intent to threaten 'unity, integrity, security or sovereignty of India or promoting terror with Denial of Service Attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty and integrity of India, the security, friendly relations with other states, public order, decency, morality or relating with contempt of court, defamation or incitement to an offence or to advantage of any foreign nation or group of individuals[15]. A brief outline of legal provisions under the IT Act aimed at providing legal protection against cyber terrorism is discussed below:

14. Raman and Sharma (2019) Cyber Terrorism in India: A Physical Reality Orvirtual Myth, Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019

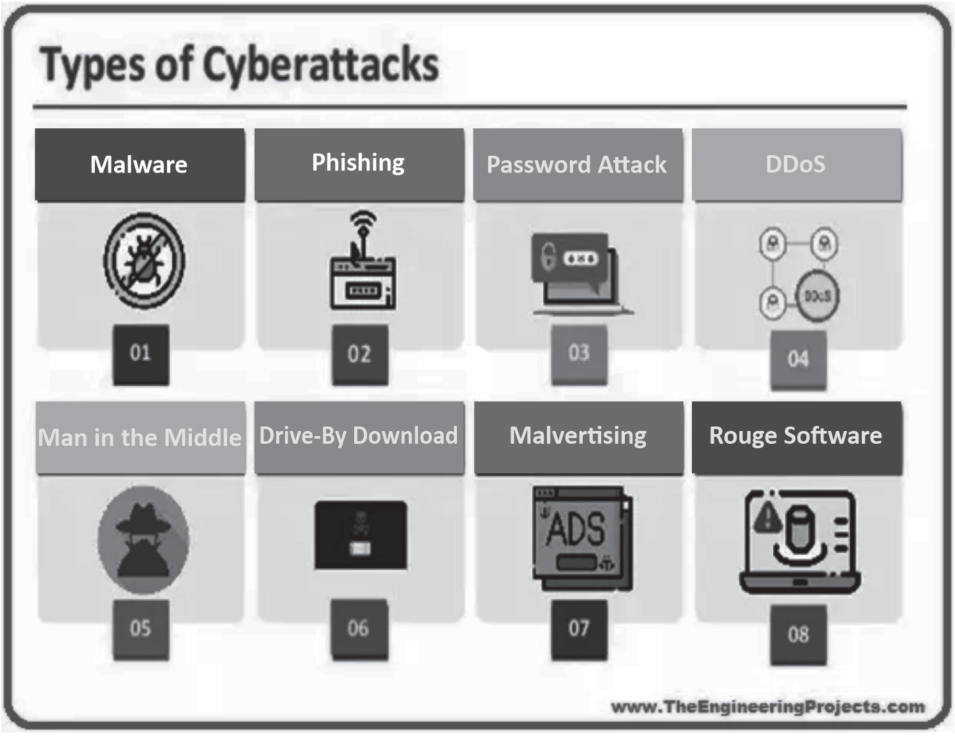
15. Shiv Raman, Nidhi Sharma, "Cyber terrorism in India: A physical reality or virtual myth" 5 Indian Journal of Law and Human Behaviour (2019), available at: https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf .

- Sec. 66: Computer related offences including Hacking.
- Sec. 66A: Punishment for sending "false and offensive messages" through communication service etc. This section also made sending messages deemed 'annoying or inconvenient' an offence. It is pertinent to note that this section has been struck down as being unconstitutional for violating freedom of speech and expression guaranteed under Art. 19(1)(a) of the Constitution of India by the Hon'ble Supreme Court in *Shreya Singhal vs. Union of India (2015) 5 SCC 1*.
- Section 66C: Punishment for Identity theft, i.e. dishonestly and using electronic signature, password or any other unique identification feature of any other person.
- Section 66D: Punishment for cheating by personation by using computer resource.
- Section 66F: Punishment for Cyber Terrorism.
- Section 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Section 69B: Power to authorize to monitor and any computer resource for cyber security.
- Section 70B: Indian Computer Emergency Response Team (CERT) to serve as national agency for incident response.
- Section 84B: Punishment for abetment of offences.
- Section 84C: Punishment for attempt to commit offences.
- Implementation of Information Technology (IT) Security Guidelines, 2000.
- The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009.
- The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.
- The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
- The Information Technology (Electronic Service Delivery) Rules, 2011.
- The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013.

TYPES OF CYBER THREATS/ ATTACKS

As discussed above, a cyber-attack or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.



Source: Medium.com

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. Cyber-attacks can be classified into the following categories:

1) Web-based attacks
2) System-based attacks.

Web-Based Attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. **Injection attacks:** It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information. Example- SQL Injection, code Injection, log Injection, XML Injection etc.
2. **DNS Spoofing:** DNS spoofing is a type of computer security hacking. Whereby data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers' computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.
3. **Session Hijacking:** It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
4. **Phishing:** Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication. For example: an email-borne attack that involves tricking the email

recipient into disclosing confidential information or downloading malware by clicking on a hyperlink in the message.

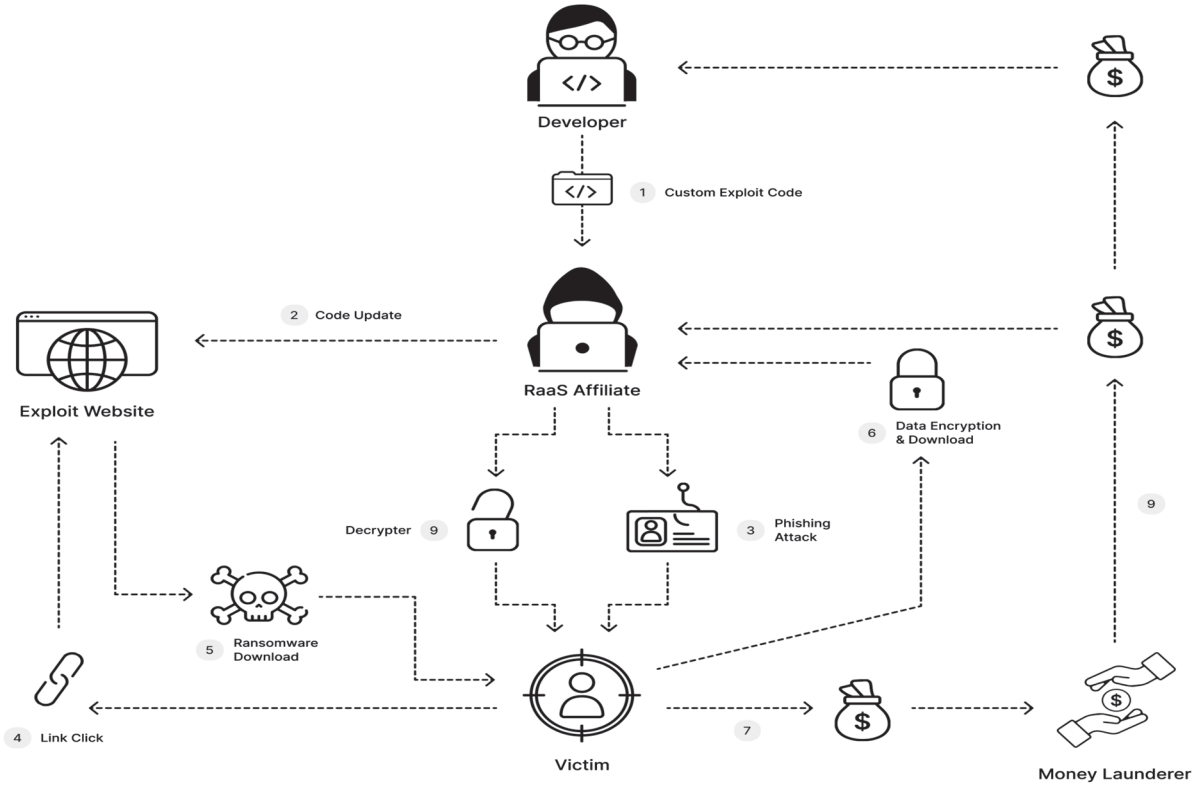
5. **Spear Phishing:** A more sophisticated form of phishing where the attacker learns about the victim and impersonates someone he or she knows and trusts.
6. **Malware:** Malware (malicious software) is software that has been specifically designed to perform malicious tasks on a device or network, such as corrupting data or taking control of a system.
7. **Malware on Mobile Apps:** Mobile devices are vulnerable to malware attacks just like other computing hardware. Attackers may embed malware in app downloads, mobile websites, or phishing emails and text messages. Once compromised, a mobile device can give the malicious actor access to personal information, location data, financial accounts, and more.
8. **Spyware:** Spyware is a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.
9. **Wiper Attacks:** A wiper attack is a form of malware whose intention is to wipe the hard drive of the computer it infects.
10. **Brute force:** It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.
11. **Denial of Service:** It is an attack which is meant to make a server or network resource unavailable to the user. It accomplishes this task by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following:

    Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

    Protocol attacks- It consumes actual server resources, and is measured in a packet.

    Application layer attacks- Its goal is to crash the web server and is measured in request per second.
12. **Dictionary attacks:** These type of attacks store the list of a commonly used passwords and validate them to get the original password.
13. **URL Interpretation:** It is a type of attack where we can change certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
14. **File Inclusion attacks:** It is a type of attack that allows an attacker to access unauthorized or essential files which are available on the web server or to execute malicious files on the web server by making use of the include functionality.
15. **Man in the Middle Attacks:** It is a type of attack that allows an attacker to intercept the connection between client and server and act as a bridge between them. This will enable the attacker to read, insert and modify the data in the intercepted connection. In short, here, an attacker establishes contact between the sender and recipient of electronic messages and intercepts them, perhaps changing them in transit, making the sender and recipient believe that they are communicating directly with one another. A MitM attack may be utilized by the military to confuse an enemy.
16. **Trojans:** Named after the Trojan Horse of ancient Greek history, the Trojan is a type of malware that enters a target system looking like one thing, e.g. a standard piece of software, but then releases the malicious code once inside the host system.

17. **Ransomware:** Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid. Ransomware is one of the most dangerous types of cyber security threats. Some ransomware attack techniques involve stealing sensitive information before the target system is encrypted. Such added processes could classify some ransomware attacks as data breaches.



Source: https://www.upguard.com/blog/cyber-threat

18. **Attacks on IoT Devices:** IoT devices like industrial sensors are vulnerable to multiple types of cyber threats. These include hackers taking over the device to make it part of a DDoS attack and unauthorized access to data being collected by the device. Given their numbers, geographic distribution, and frequently out-of-date operating systems, IoT devices are a prime target for malicious attacks.

> ***Note:***
>
> IoT is an umbrella term that refers to the billions of physical objects or things connected to the Internet, all of which collect and exchange data with other devices and systems over the internet.
>
> IoT Devices are hardware devices such as sensors, gadgets, appliances and other devices/machines that collect and exchange data over the internet.

19. **Data Breaches:** A data breach is a theft of data by a malicious attacker. Motives for data breaches include crime (i.e., identity theft), a desire to embarrass an institution (e.g., Edward Snowden or the DNC hack), and espionage.

20. **Data Manipulation:** Data manipulation is a form of cyber-attack that doesn't steal data but aims to change the data to make it harder for an organization to operate.

21. **Data Destruction:** Data destruction is when a cyber attacker attempts to delete data.
22. **Malvertising:** Malvertising is the use of online advertising to spread malware.
23. **Rogue Software:** Rogue software is malware that is disguised as real software.
24. **Unpatched Software:** Unpatched software is software that has a known security weakness that has been fixed in a later release but not yet updated.

System-Based Attacks

These are the attacks which are intended to compromise a computer or a computer network.

Some of the important system-based attacks are as follows:

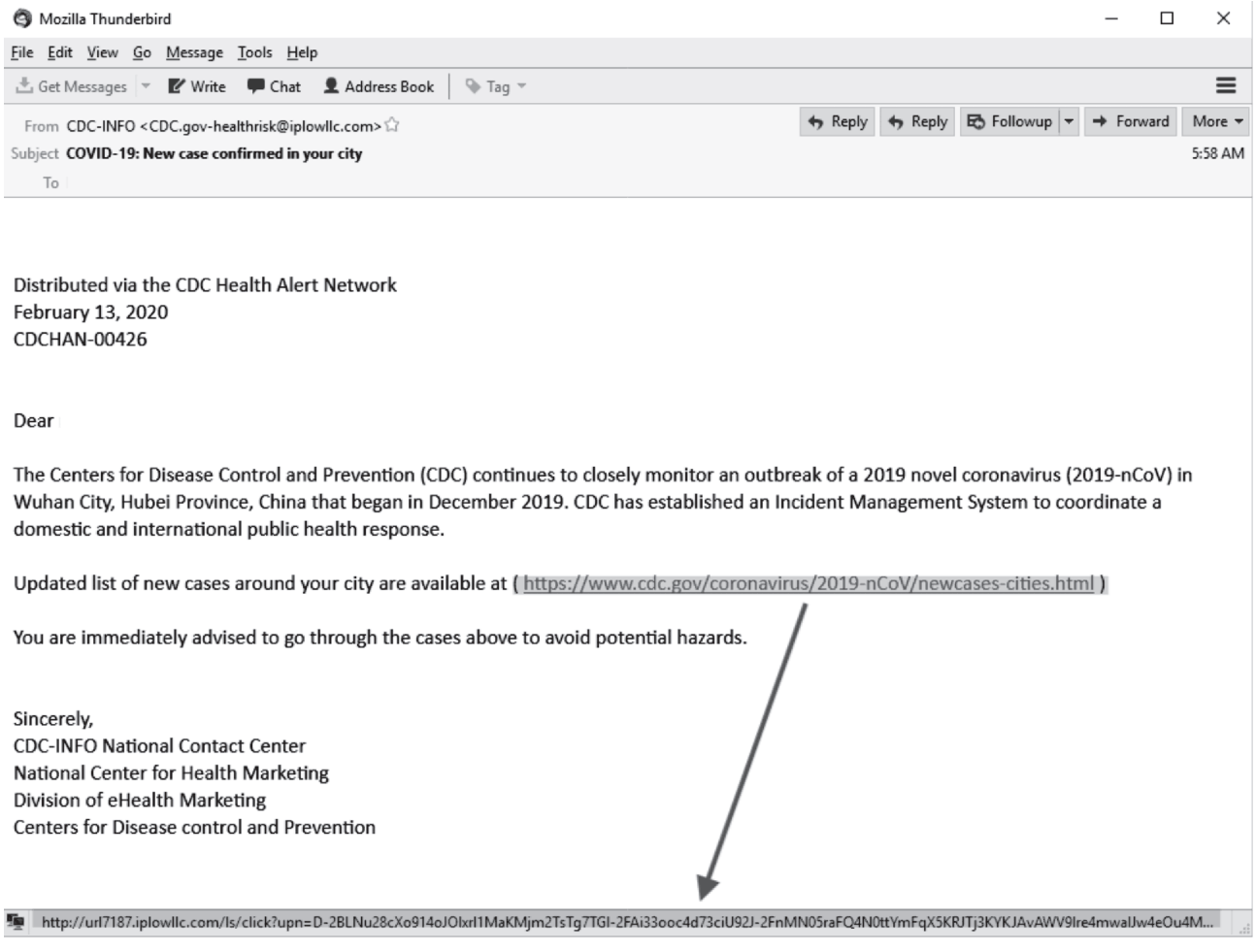
1. **Virus:** It is a type of malicious software program that spreads throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
2. **Worm:** It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works in the same manner as a computer virus. Worms often originate from email attachments that appear to be from trusted senders.
3. **Trojan horse:** It is a malicious program that makes unexpected changes to computer settings and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.
4. **Backdoors:** It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
5. **Bots:** A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.
6. **Zero-Day Exploits:** A zero-day exploit is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw.
7. **Advanced Persistent Threats:** advanced persistent threat is when an unauthorized user gains access to a system or network and remains there without being detected for an extended period of time.
8. **Data Centre Disrupted by Natural Disaster:** The data center your software is housed in could be disrupted by a natural disaster like flooding.
9. **Drive-by Downloads:** A drive-by download attack is a download that happens without a person's knowledge often installing a computer virus, spyware, or malware into the system.
10. **Intellectual Property Theft:** Intellectual property theft is stealing or using someone else's intellectual property without permission.
11. **Supply Chain Attacks:** A supply chain attack is when a cybercriminal hacks an organization by compromising a third-party vendor in its supply chain.

Recent Cybers Threats[16] - 2022

Example of some of the common cyber threats are as follows:

Covid-Themed Phishing Attacks

Since the coronavirus pandemic, Covid-themed phishing attacks have spiked, preying upon the virus-related anxieties of the public.

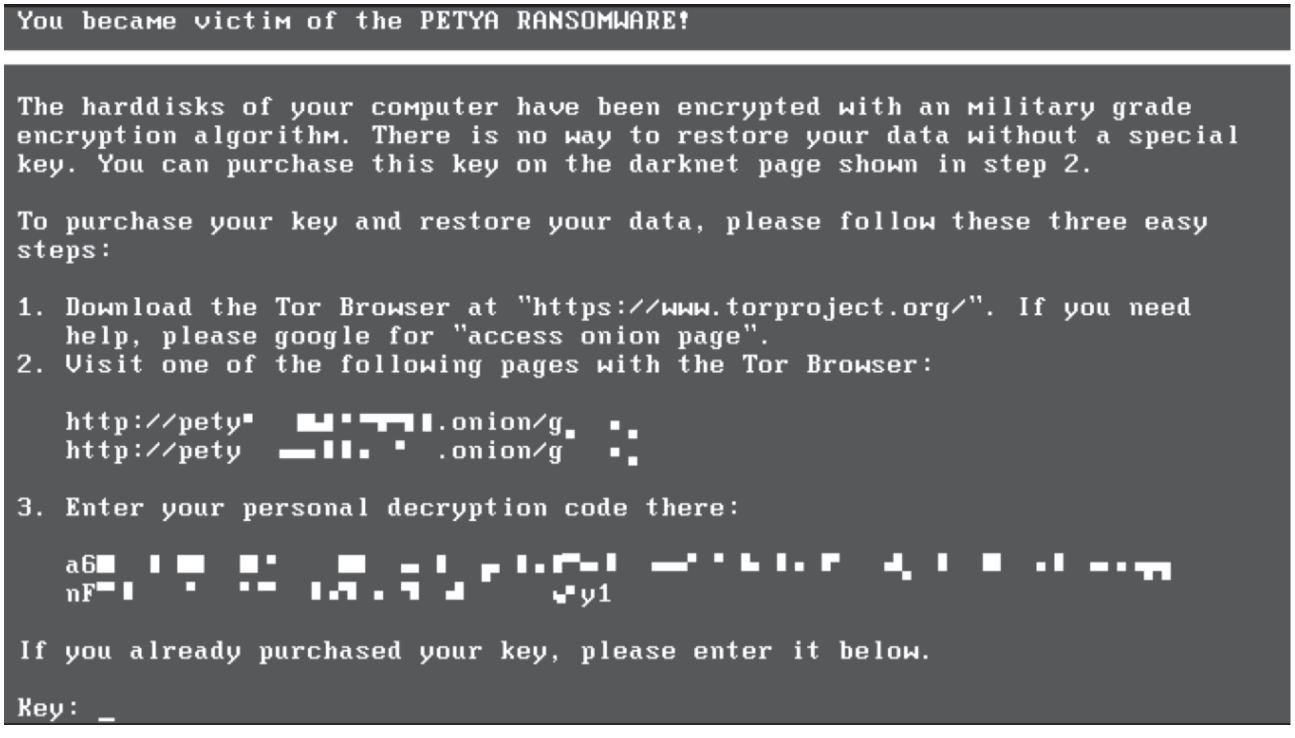


Source: ncsc.org

Ransomware Attacks

Ransomware attacks are one of the most frightening cyber threats. During these attacks, a victim's sensitive data is encrypted and only decrypted if a ransom price is paid. Victims only become aware that they've been compromised when they are presented with a formidable message announcing the successful attack. Sometimes these messages are falsely attributed to law enforcement agencies.

16. For more details, kindly read Tunggal Abi Tyas (2022) Cybersecurity: What is a Cyber Threat, UpGuard.



Source: nytimes.com.

Insider Threats

Insider threats includes the security threats and attacks made by the insiders like employers, outsourcing vendors and alike. Unlike phishing attacks, this type of security-bypassing cyber threat cannot be mitigated with a control strategy.

Supply Chain Attacks

According to the Cost of a Data Breach Report, 2022 by IBM[17] and the Ponemon Institute, it was revealed that third-party software vulnerabilities are gaining popularity as a primary attack method.

Polyglot Files

Polyglot are files that can have multiple file type identities. Polyglot files as such are not hostile by nature. Cybercriminals package malicious code into polyglot files to bypass file-type security controls.

Distributed Denial of Service (DdoS) Attacks

As the adoption rate of IoT devices in both the home and office continues to rise, the risk of DDoS attack rises accordingly. During a DDoS attack, cybercriminals direct a high concentration of network requests from multiple compromised IoT devices at a targeted website. This causes the victim's servers to overload, forcing them offline. All forms of DDoS are illegal, even if it is used to gain an advantage during a friendly online gaming session.

17. Complete Report is available at https://www.ibm.com/downloads/cas/3R8N1DZJ

Social Engineering

Social engineering, in the context of cyber threats, is an effort to obtain login credentials through manipulation and trickery. Phishing campaigns are the usual attack vectors of social engineering, but these cyber threats can also be presented in person. For example, threat actors posing as IT professionals asking for your password.

Phishing

Phishing attacks are a subcategory of social engineering, the differentiator is that they most commonly deployed via email, whereas a social engineering attack could occur through a telephone conversation.

According to the 2022 cost of a data breach report by IBM[18] and the Ponemon Institute, in 2022, Phishing was the second most expensive data breach attack vector, averaging US$ 4.91 million per breach, increasing from US$ 4.65 million in 2021.

Malvertising

The year 2022 has seen an increase in the instances of Malvertising. An example of a malvertising attack is the Latin American banking trojan known as MIspadu. The trojan was embedded in a Facebook ad campaign for McDonald's coupons. When users interacted with the ad, a zip file containing the bank credential-stealing trojan was downloaded and installed on their system.

Mispadu malvertising campaign - Source: welivesecurity.com

Zero-Day Exploits

A zero-day exploit is a software vulnerability or flaw that is discovered and exploited by hackers before it is known to software creators or sellers. The term "zero-day" refers to the fact that programmers have no time to address or patch the issue given that they too only recently noticed it.

Zero-day exploits are security vulnerabilities that are exploited by cybercriminals before a patch is released for them. These exposures are usually associated with ubiquitous software providers. A recent example is a zero-day exploit impacting Microsoft Exchange servers.

18. Complete Report is available on https://www.ibm.com/downloads/cas/3R8N1DZJ

CYBER THREAT HUNTING[19] AND DIGITAL FORENSICS

Cyber Threat Hunting

Cyber Threat Hunting is a proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools.

It has to be clearly noted that there is a distinction between cyber threat detection versus cyber threat hunting. Threat detection is a somewhat passive approach to monitoring data and systems for potential security issues. In the present-day information technology era, it is still a necessity to take the aid of threat hunter. Proactive cyber threat hunting tactics have evolved to use new threat intelligence on previously collected data to identify and categorize potential threats in advance of attack.

In the current times, when security of information technology and its systems are imperative, we cannot sit back and wait for threats to strike our technologies, systems and networks; hence cyber threat hunting is required for developing hypotheses based on knowing the behaviors of threat actors and validating those hypotheses through active searches in the environment.. In threat hunting, experts don't wait for alarms or obvious signs of trouble. Instead, they use their skills to investigate deeply using forensic methods. Basically, they take a proactive and thorough approach to find and handle cybersecurity threats. Cyber threat hunting aggressively assumes that a breach in the enterprise has or will occur. Security personnel hunt down threats in their environment rather than deploy the latest tool.

Threat Hunting Investigations

Traditional cyber threat hunting is based on a manual process in which a security analyst scrutinizes data based on their knowledge of the network and systems to build assumptions about potential threats. Cyber threat hunting has advanced in effectiveness and efficiency through the addition of automation, machine learning, and User and Entity Behavior Analytics (UEBA) to alert enterprise security teams of potential risks.

Once the risk or potential risk, as well as frequency of a hunt has been determined, an investigation is initiated. Examples of Cyber Threat Hunting investigations include:

- *Hypothesis Driven Investigations*: When significant information of a new, imminent threat vector is discovered, cyber threat hunting will delve deeper into network or system logs in search of hidden anomalies or trends that could signal the new threat. Analytics Driven Investigation: Searches based on information gathered from Machine Learning (ML) and Artificial Intelligence (AI) tools.

  > ***Note:*** Machine Learning is a growing technology which enables computers to learn automatically from past data.

- *Tactics, Techniques, and Procedures (TTP) Investigation*: Hunting for attack mannerisms typically use the same operational techniques. This is helpful to source or attribute the threat and to leverage existing remediation methods that worked with these behaviors. Tactics, Techniques, and Procedure (TTP) investigation is an organised method of evaluating and comprehending the techniques and procedures employed attackers or adversaries in executing cyber attacks or harmful actions. It entails examining their approaches (overall strategy or plan), techniques (particular methods or instruments employed), and procedures (step-by-step processes or activities conducted) in order to acquire knowledge about their motivations, abilities, and potential effect.

19. Source: Trellix – What is Cyber Threat Hunting? Available at https://www.trellix.com/en-us/security-awareness/operations/what-is-cyber-threat-hunting.html

Threat Hunting Techniques

Though threat hunting is specific to each environment, yet some techniques can be applied to almost any environment. Some of the core threat hunting techniques include:

1. ***Baselining:*** Baselining helps the hunter understand what "normal" looks like within an organization. It is similar to developing an established or usual behaviour guide. This allows the hunter to immediately notice anything unusual or beyond the norm.
2. ***Attack-Specific Hunts:*** Baselining aids the hunter in understanding the overall hunt environment, but attack-specific hunts can help track malicious activity faster. Attack-specific hunts typically focus on a specific threat actor or threat. However, the limits of their specific hunt model can throw off false positives. Attack-specific hunts combine with baselining often produce good results.
3. ***Time Sensitivity:*** All hunts are time sensitive, and therefore require hunters to validate their baseline terms periodically. Keeping up with attackers' shifting to new techniques – or reverting back to old techniques – require hunters to validate intelligence-based hunts and even hunt again if legacy techniques are detected.
4. ***Third-Party Sources:*** Hunting for needles in a data haystack can overwhelm teams of hunters. Third-party providers can help guide hunters to more successful hunts. Following benefits can be gathered from third-party sources:
    - Ruling out false positive leads
    - Focus on interesting leads
    - IP lookups
    - Geolocation
    - Encrypted traffic metadata
    - Log detection
    - Attacker technique overlays
    - Link analysis of *internal* vs. *external or host* vs. *network data points*

Hunting Steps

A cyber threat hunt is composed of steps or processes designed for an efficient, successful hunt. These steps include:

Step 1: Hypothesis

Threat hunts begin with a hypothesis or a statement about the hunter's ideas of what threats might be in the environment and how to go about finding them. A hypothesis can include a suspected attacker's tactics, techniques, and procedures (TTPs). Threat hunters use threat intelligence, environmental knowledge, and their own experience and creativity to build a logical path to detection.

Step 2: Collect and Process Intelligence and Data

Hunting for threats requires quality intelligence and data. A plan for collecting, centralizing, and processing data is required.

Step 3: Trigger

A hypothesis can act as a trigger when advanced detection tools point threat hunters to initiate an investigation of a particular system or specific area of a network.

Step 4: Investigation

Investigative technology aids in the detection of anomalies in a system or network. It digs deep to find any unexpected activity that might be hazardous. It determines if these discoveries are harmless or actually malicious. So, it's like a tool that examines and distinguishes the harmless stuff from the harmful one.

Step 5: Response/Resolution

Data gathered from confirmed malicious activity can be entered into automated security technology to respond, resolve, and mitigate threats. Actions taken can include getting rid of harmful files, bringing back changed or deleted files to their original condition, updating rules for firewalls or intrusion prevention systems, installing security updates, and adjusting system settings. Throughout this process, there is also a focus on learning from the incident to enhance security and be better prepared against similar attacks in the future.

DIGITAL FORENSICS[20]

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. The term digital forensics was first used as a synonym for computer forensics. From legal perspective, digital forensics is the process of identifying, preserving, analysing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.[21] As per Techopedia - "*Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events. The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances*."

Steps of Digital Forensics

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

Steps of Digital Forensics

Identification - First, find the evidence, noting where it is stored.
Preservation - Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.
Analysis - Next, reconstruct fragments of data and draw conclusions based on the evidence found.
Documentation - Following that, create a record of all the data to recreate the crime scene.
Presentation - Lastly, summarize and draw a conclusion.

DIGITAL INTELLECTUAL PROPERTY

As per the definition given by the Law Insider, Digital Intellectual Property means any and all of the following that is owned by Digital on, or any time after, the date hereof : (i) trade secrets, unpatented formulations, manufacturing methods and other know-how, (ii) copyrights, (iii) all patents on and pending applications to

20. Source: https://www.eccouncil.org/what-is-digital-forensics/#:~:text=SQL%20Injection%20Attack%3F-,What%20Is%20Digital%20Forensics%3F,a%20synonym%20for%20computer%20forensics.

21. Also access write up on digital forensics available at https://www.sentinelone.com/cybersecurity-101/what-is-digital-forensics-and-incident-response-dfir/?utm_content=demo-request&utm_medium=paid-search&utm_source=google-paid&utm_campaign=apj-t1-en-g-s-dsa-rlsa&utm_term=&utm_campaignid=19582401347&gclid=EAIaIQobChMI4MfN3p-D_QIVjZNmAh1yVAq0EAAYAiAAEgKf0fD_BwE

patent any technology or design; (iv) all registrations of and applications to register copyrights; and (v) computer software, including systems, applications, program listings, manuals and documentation (whether owned by Digital Electronics or licensed by Digital Electronics from third parties).

In simple words, Digital Intellectual Property (Digital IP) is intellectual property in digital format. Throughout the globe, the businesses and the individual stores, create, or otherwise handle some sort of digitalized information. Though protecting digital intellectual property encourages increased levels of innovation and creativity, resulting in the acceleration of progress, yet reality of digital information poses problems surrounding the use and re-use of information, and the rights and responsibilities of rights holders and consumers under existing laws.

While Digital IP encourages innovation, creativity, and economic growth, protecting it poses a challenging task, and is difficult for a number of reasons. Digital products are not tangible, and can be reproduced at a very low cost with the potential for immediate delivery via the Internet across virtually unlimited geographic markets. There are many stakeholders that can represent a broad range of legitimate concerns. Hence, it is important to understand what are different concerns for protecting Digital IP and the strategies to protect digital IP.

Ways for Protection of Digital / Intellectual Property:[22]

Digital Rights Management (DRM) technologies (also known as Electronic Rights Management Systems) ensure copyright through identifying and protecting the content, controlling access of the work, protecting the integrity of the work and ensuring payment for the access. DRM technologies prevent illegal users from accessing the content. User ID and password are used to protect access, along with licensing agreements. Another way to protect digital content is through Technical Protection Measures (TPM). These technologies allow publishing companies in securing and protecting content such as music, text and video from unauthorized use. If an author wishes to collect fee for use of his or her work, then DRM technology can be used.

The TPM and DRM technologies are increasingly employed to sell and distribute content over the Internet.

1. **Cryptography:** Cryptography is the oldest mechanism employed to ensure security and privacy of information over networks.. This process involves encrypting or scrambling the information to make it unreadable or in a language that is difficult to understand. Only the authorized user has the ability to decrypt or unscramble it. However, cryptography protects the work during transmission or distribution only. After the work is decrypted, it loses its protective measures.
2. **Digital Watermark Technology:** A digital watermark is a digital signal or pattern inserted into a digital document. It is similar to the electronic on-screen logo used by TV channels. A unique identifier is used to identify the work. The message might contain information regarding ownership, sender, recipient etc. or information about copyright permission. The system consists of a watermark generator, embedder and a watermark detector decoder. The legal user can remove these watermarks with a predetermined algorithm. The watermarking technology is extensively used in protecting multimedia works.
3. **Digital Signature Technology:** Digital signature includes identity of the sender and/or receiver date, time, any unique code etc. This information can be added to digital products. This digitally marks and binds a software product for transferring to a specified customer. Digitally signed fingerprints guarantee document authenticity and prevent illegal copying.
4. **Electronic Marking:** In this technique, the system automatically generates a unique mark that is tagged to each of the document copies. This technique is used to protect copyright as well as in electronic publishing where documents are printed, copied or faxed.

22. Source: http://eprints.rclis.org/28939/1/Intellectual%20Property%20Rights%20in%20Digital%20Environment_ISI.pdf

5. **Security Features of Operating System:** For protection of files, data etc. the operating system of computer such as Windows 2000 Professional, Windows 2000 Server, MS-SQL Server has some unique special security and integrity features.

LIABILITY OF ONLINE PLATFORMS

With the rise of e-commerce and online trading, online platforms are increasingly exposed to claims of intellectual property ("IP") infringement. Their visibility and deep pockets often make them a more worthy target as compared to individual users of platforms, whose obscure identities and business scale seldom justify protracted legal proceedings.

Indeed internet has revolutionized the way we interact; however, it has also bought with it a host of problems such as hate speech, fake news, illegal lobbying and personal data theft. The number of these issues not only make the criminal/offender liable, yet many a times, online platforms are also made liable for the cyber security threat.

As per Section 2 (1)(w) of Information Technology Act, 2000 - *Unless the context otherwise requires - "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.*

As the per the above definition, online platforms fall under the definition of intermediary. Hence, lets us understand the liability of intermediaries and the legal provisions governing the same.

Intermediaries are widely recognized as essential cogs in the wheel of exercising the right to freedom of expression on the Internet. Most major jurisdictions around the world have introduced legislations for limiting intermediary liability in order to ensure that this wheel does not stop spinning. With the 2008 amendment of the Information Technology Act 2000, India joined the bandwagon and established a 'notice and takedown' regime for limiting intermediary liability.

> "Intermediary liability, which is based on the legal principle of vicarious liability, means that the service providers shall be held accountable for any illegal act of the user on their platform. As Rebecca MacKinnon has said, "Intermediary liability means that the intermediary, a service that acts as 'intermediate' conduit for the transmission or publication of information, is held liable or legally responsible for everything its users do."

But in the recent times, considering the abuse of online platforms, it is demanded time and again to create an efficient regulatory regime for all the intermediaries including online platforms.[23]

Legal/Regulatory regime of "Intermediary/Online Platform Liability" in India

Kapoor Saumya (Chadha and Chadha Intellectual Property Law Firm) in her article titled *Tracking the development of "Intermediary Liability" in India in India*[24], has meticulously discussed the regulation regime of intermediaries vide various laws and sub-legislations incorporated in India. Further, some landmark cases in India are also discussed wherein Indian courts have been proactive in adjudicating on these issues. A brief of that article is mentioned as below:

23. Sur Aihik (August 12, 2022): India needs legislation to hold platform liable for online harms: IT for change. Available at https://www.moneycontrol.com/news/business/india-needs-legislation-to-hold-platforms-liable-for-online-harms-it-for-change-9018861.html

24. Available at https://s3.amazonaws.com/documents.lexology.com/8db09138-482a-4951-b255-6513ca1eaad3.pdf?AWSAccessKeyId=AKIAVYILUYJ754JTDY6T&Expires=1675854906&Signature=tF9cQSg9FZoCzslcQj%2Ft%2BvoDPtA%3D

Information Technology Act, 2000 (IT Act)

Under the IT Act, initially only network service providers were protected "for any third-party information or data made available by them if they proves that the offence or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such offence or contravention." Thus, the original IT Act provided little or no safe harbour protection to intermediaries.

Safe Harbour Protection

The safe harbour protection for e-commerce marketplaces is an important aspect that deserves careful consideration. The concept of safe harbour under Section 79 of the IT Act, 2000, acts as a defence for the intermediaries, but there are some instances where Intellectual Property Rights (IPR) are openly violated by the intermediaries. Safe harbour protection acts as an inherent security granted to intermediaries against the imposition of liability for acts done by third parties.

Safe harbour provisions were introduced to protect intermediaries from becoming liable for the acts of third parties, provided the intermediary observed 'due diligence'. Intermediaries are shielded from liability under Section 79 of the IT Act for data, material, and information shared by users through them but over which they have no direct knowledge. Under the safe harbour, intermediaries are protected from third-party information and data made available or hosted by them thereby acting as a defence. Intermediaries are protected by safe harbour from all legal consequences unless they knew that illicit content was being broadcast on their platform.

Avnish Bajaj vs. State[25] and the Amendment to the IT Act 2008

In this case, the Managing Director (and not the company Baazee.com) was charged with criminal provisions under the Indian Penal Code, 1860 (Hereinafter referred to as 'IPC') as well as the Information Technology Act, 2000 (Hereinafter referred to as 'IT Act'), for content circulated by a third party on its ecommerce platform. However, the Managing Director escaped liability since the company was not added as an accused either before the High Court or before the Supreme Court. Further, the Delhi High Court also observed that companies bear the risk of acquiring knowledge if the content uploaded escapes the filters which are meant for blocking pornographic content.

In this case, it was also observed that there was a requirement for widening the scope of protection given to intermediaries, and thus, the IT Act was amended in 2008 to include a safe harbour regime under Section 79 of the IT Act and to amend the definition of intermediaries (as it reads presently). Section 79 of the Information Technology Act 2000[26] introduced the 'safe harbour' immunity clause that protected an intermediary from being held liable for third-party content on its platform and affords broad-ranging legal immunity – provided the intermediary observed 'due diligence' and followed certain 'guidelines' as prescribed by the Central Government. Only if due diligence laid down by the government is not followed by the intermediary, it

25. Avnish Bajaj vs. State, 150 (2008) DLT 769

26. Section 79 of Information Technology Act reads as : Exemption from liability of intermediary in certain cases. - (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. (2) The provisions of sub-section (1) shall apply if- (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does not- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf. (3) The provisions of sub-section (1) shall not apply if- (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or othorise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner. Explanation. -For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

would be made liable for a third party's actions, even if the same were done without the knowledge of the intermediary.

The Information Technology (Intermediaries Guidelines) Rules, 2011 ("Intermediary Guidelines") (2011)[27]

After the amendment to the IT Act in 2008, the Government of India introduced the Intermediary Guidelines, which were mandatory for all intermediaries to follow for claiming safe harbour protection. These are to be read in consonance with the IT Act and the due diligence requirements that must be observed by intermediaries, provided under Rule 3, are:

- Intermediaries to publish rules and regulations, privacy policy and user agreement;
- Rules and regulations, terms and conditions or user agreement shall specify all prohibited acts, i.e. belonging to other persons, grossly harmful, harassing or unlawful, harms minors, infringes any intellectual property rights, violates any law, is deceiving or misleading, impersonates any person, contains virus, threatens India etc. and the intermediary should inform users that violation of same shall lead to termination of access,
- Intermediaries to not knowingly host or publish information as specified in sub-rule (2),
- Intermediaries to disable such information within 36 hours and storage of same for 90 days for investigation purposes,
- Intermediaries to provide assistance to authorised government agencies,
- Intermediaries to take all reasonable measures to secure its computer resource,
- Intermediaries to report cyber security incidents to the Indian Computer Emergency Response Team and
- Intermediaries to appointment and publish the details of a Grievance Officer on its website.

However, the IT Act and the Intermediary Guidelines were inundated by various issues such as ambiguity in prohibited content and forced decision by intermediaries. Further, any person could request the intermediaries to take down the unlawful content. However, these issues were mostly resolved in the Shreya Singhal judgement.

Shreya Singhal vs. Union of India (2015)[28]

In 2015, in the landmark Shreya Singhal judgement, the Supreme Court for the first time recognized the Indian citizen's free speech rights over the Internet by striking down and declaring unconstitutional the draconian Section 66A of the IT Act, which provided for punishment for sending offensive messages through communication services.

Further, regarding intermediary liability, the Court held that "*Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material.... Similarly, the Information Technology Intermediary Guidelines Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment*."

The Court also observed that "*it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.*" Subsequently, in the case of Kamlesh Vaswani v Union of India (Writ Petition (Civil) No. 177 of 2013), the Supreme Court issued directions to intermediaries to disable specific content where website operating child pornography was sought to be restricted.

27. The Intermediaries Guidelines Rules, https://meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf

28. Shreya Singhal vs. Union of India, [(2015) 5 SCC 1]

My Space Inc. vs. Super Cassettes Industries Ltd. (2017)[29]

In this case, the division bench of the Delhi High Court distinguished Copyright matters and held that if intermediaries were given the responsibility of identifying illegal content, it could have a chilling effect on free speech and will lead to private censorship. This judgment dealt with uploading of music on myspace.com and a copyright infringement suit was brought by Super Cassettes India Ltd.

The Court also gave the concept of 'actual or specific knowledge' and held that intermediaries can be held liable if they have actual or specific knowledge of the existence of infringing content on their website from content owners and despite such notice, they do not takedown the content. There is no necessity of a court order in such cases. The two-judge bench of the Delhi High Court further pronounced that "*in case of internet intermediaries, interim relief has to be specific and must point to actual content, which is being infringed*".

Kent Ro Systems Ltd & Anr vs. Amit Kotak & Ors (2017)[30]

In this case, the Petitioner, in a suit for permanent injunction against the Respondent for infringing its intellectual property rights by copying its designs, also added eBay India as a party for permitting the Respondent to advertise, offer to sell and sell its product on its website.

The Court held that "*to hold that an intermediary, before posting any information on its computer resources is required to satisfy itself that the same does not infringe the intellectual property rights of any person, would amount to converting the intermediary into a body to determine whether there is any infringement of intellectual property rights or not... The IT Rules, according to me do not oblige the intermediary to, of its own, screen all information being hosted on its portal for infringement of the rights of all those persons who have at any point of time complained to the intermediary... Merely because intermediary has been obliged under the IT Rules to remove the infringing content on receipt of complaint cannot be read as vesting in the intermediary suo motu powers to detect and refuse hosting of infringing contents... I am of the view that to require an intermediary to do such screening would be an unreasonable interference with the rights of the intermediary to carry on its business*." Thus, the Court reiterated the specific knowledge principle of the Myspace case.

Subsequently, *in Lifestyle Equities C.V. and Ors v Amazon Sellers Service Private Limited & Another[31]*, the Court directed Amazon to share the details about the person who had uploaded the links as well as to remove the links advertising the infringing and counterfeit goods.

Christian Louboutin SAS vs. Nakul Bajaj and Ors (2018)[32]

In this case, the Delhi High Court clarified the responsibilities and liabilities of ecommerce intermediaries that were previously undetermined. The Court held that the Defendant was not an intermediary and was an "active participant" and thus, would be liable for infringement. The Court also held that the conduct of intermediaries, in failing to observe 'due diligence', could amount to 'conspiring, aiding, abetting or inducing' unlawful conduct and would disqualify them from the 'safe harbour' exemption, as per Section 79(3)(a) of the IT Act.

Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018, ("Draft Rules") (2018)[33]

On December 24, 2018, Ministry of Electronics & Information Technology released the Draft Rules for amending the existing Intermediaries Guidelines to curb the "Misuse of Social Media and spreading Fake News". These Draft Rules place several obligations on the intermediaries, some of which are enabling traceability to determine

29. My Space Inc. vs Super Cassettes Industries Ltd., [236 (2017) DLT 478]

30. Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors, [2017 (69) PTC 551 (Del)].

31. Lifestyle Equities C.V. and Ors v Amazon Sellers Service Private Limited & Anr., [CS (COMM) 1015/2018].

32. Christian Louboutin SAS vs. Nakul Bajaj & Ors, [2018(76) PTC 508(Del)]

33. https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_%20Amendment_24122018.pdf

the originator of the information for assistance to law enforcement, proactive monitoring of content uploaded on its platform by deploying automated tools, takedown of illegal content within 24 hours, and mandatory incorporation of companies having more than 5 million users in India.

M/S Luxottica Group S.P.A & Another vs. M/S Mify Solutions Pvt Ltd & Ors (2019)[34]

The Plaintiff filed a trademark infringement suit alleging that the Defendant sells counterfeit products of the Plaintiff's brand 'OAKLEY'. The Court held that the due diligence and care required under the IT Act had not been met and the Defendant was guilty of trademark and copyright infringement. The Court herein applied the tests laid down in the Christian Louboutin case to determine whether the ecommerce platforms claiming to be exempted under Section 79 of the IT Act actually qualify as intermediaries or not. The Court observed that presence of any element which shows active participation could deprive intermediaries of the immunities and factors such as allowing storing of counterfeit goods, using the mark in an invoice, advertising the mark etc., would determine whether the entity in question is an intermediary or not.

Amway India Enterprises Pvt Ltd vs. 1Mg Technologies Pvt Ltd & Another (2019)[35]

One of the main issues in this case was the conflict between Direct Selling Business and ecommerce platforms and whether the intermediary had stepped into the shoes of the seller by setting its own retail prices, discounts, return/refunds policies etc. Thus, the issue was whether the intermediary had violated the Direct Selling Guidelines issued by the Government, which were binding on the Plaintiff. In this regard, the Single Judge held that the Direct Selling Guidelines were binding on ecommerce platforms and the sellers on such platforms. However, the Division Bench held that such guidelines are advisory in nature and are not law and thus, not enforceable.

Further, the Court also gave a detailed reasoning as to why major ecommerce giants are actively involved and thus, do not qualify as intermediaries entitled to protection under the 'safe harbour' provided in Section 79 of the IT Act. It was held that any non-compliance of the due diligence requirements as per the Intermediary Guidelines and failure to adhere to their own policies would make the ecommerce platforms liable. The Division Bench also observed that the value-added services provided by the Defendant as online market places, do not dilute the safe harbour granted to them under Section 79 of the IT Act.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[36]

The Intermediary Guidelines Rules, 2011 were replaced by the Information Technology (IT) Rules, 2021, which were formulated by the Union Government in accordance with Section 87(2) of the IT Act, 2000. As per the said rules, large digital platforms with more than 5 million users would be required to publish periodic compliance reports each month. The Rules prescribe a framework for the regulation of online content in terms of current affairs, news, and audio-visual content. In India, all intermediaries, including OTT platforms and digital portals, must offer a grievance redressal process to address user complaints. These rules aim to empower netizens for the timely resolution of their grievances with a mechanism for redressal and assistance of a Grievance Redressal Officer (GRO) residing in India.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 4(1)(d), mandate that social media outlets post monthly compliance reports that include the following information:

- Information about complaints filed and measures undertaken in response, and
- The number of particular communication links or informational components that the social media platform has blocked or erased as part of proactive monitoring.

34. Luxottica Group SPA and Ors v Mify Solutions Pvt Ltd and Ors, [2019(77) PTC 139(Del)]

35. Amway India Enterprises Pvt Ltd v 1Mg Technologies Pvt Ltd & Anr., [CS (OS) 410/2018, CS (OS) 453/2018, CS (OS) 480/2018, CS (OS) 531/2018, CS(OS) 550/2018, CS (OS) 75/2019 and CS (OS) 91/2019]

36. Source: Liability of online marketplaces in India (2021) iPleders.

LAWS APPLICABLE TO AI AND CYBER LAWS

Information Technology Act, 2000 (IT Act, 2000)

Overview of IT Act, 2000

It is the first law to regulate cyberspace which has been approved by the Indian Parliament. The Act defines the following as its object:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

However, as cyber-attacks become dangerous, along with the tendency of humans to misunderstand technology, several amendments are being made to the legislation. It highlights the grievous penalties and sanctions that have been enacted by the Parliament of India as a means to protect the e-governance, e-banking, and e-commerce sectors. It is important to note that the IT Act's scope has now been broadened to include within its ambit all the latest communication devices.

The IT Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and enforceability. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce.

The important provisions of IT Act, 2000

The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process governing cyber-crimes. Following are some of the relevant sections:

- Section 43: This section of the IT Act applies to individuals who indulge in cyber crimes such as damaging the computers of the victim, without taking due permission of the victim. In such a situation, if a computer is damaged without the owner's consent, the owner is fully entitled to a refund for the complete damage.

  In *Poona Auto Ancillaries Pvt. Ltd., Pune vs. Punjab National Bank, HO New Delhi & Others (2018)*, Rajesh Aggarwal of Maharashtra's IT department (representative in the present case) ordered Punjab National Bank to pay Rs. 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs. 80.10 lakh from Matharu's account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

- Section 66: Applies to any conduct described in Section 43 that is dishonest or fraudulent. The offence under this section is punishable with three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh.

In *Kumar vs. Whiteley (1991),* during the course of the investigation, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added, and modified files. As a result of investigations, Kumar had been logging on to a BSNL broadband Internet connection as if he was an authorized legitimate user and modifying computer databases pertaining to broadband Internet user accounts of subscribers. On the basis of an anonymous complaint, the CBI registered a cyber-crime case against Kumar and conducted investigations after finding unauthorized use of broadband Internet on Kumar's computer. Kumar's wrongful act also caused the subscribers to incur a loss of Rs. 38,248. N G Arun Kumar was found guilty and sentenced by the Additional

Chief Metropolitan Magistrate. The magistrate ordered him to undergo a rigorous year of imprisonment with a fine of Rs. 5,000 under Sections 420 of IPC and 66 of the IT Act.

- Section 66B: This section describes the penalties for fraudulently receiving stolen communication devices or computers, and prescribes a possible three-year prison sentence. Depending on the severity, a fine of up to Rs. 1 lakh may also be imposed upon the accused.
- Section 66C: The focus of this section is to prohibit identity theft, by penalising the act of fraudulently and dishonestly using the electronic signature, password or any other unique identification feature of any person. This section imposes imprisonment up to 3 years along with fine upto one lakh rupees.
- Section 66D: This section penalises cheating by personation using computer resources. Punishment if found guilty can be imprisonment of up to three years and/or up-to Rs. 1 lakh fine.
- Section 66E: Taking pictures of private area of any person, publishing or transmitting them without a person's consent is punishable under this section. Penalties, if found guilty, can be imprisonment of up to three years and/or up-to Rs. 2 lakh fine.
- Section 66F: This section prescribes punishment for the offence of cyber terrorism. An individual convicted of a crime can face imprisonment of up to life. An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.
- Section 67: This section punishes the act of publishing or transmitting obscene material in electronic form. If convicted, the prison term is up to five years and the fine is up to Rs. 10 lakh.

Positive and negative aspects of IT Act, 2000

This legislation confers the following benefits:

- Until recently, the development of electronic commerce in our country was hindered primarily due to a lack of legal infrastructure to govern commercial transactions online. Due to the enactment of this legislation, several companies are now able to conduct e-commerce activities without any fear.
- Digital signatures are officially recognized and sanctioned by the Act. Therefore, corporations and organizations are now able to use digital signatures to conduct online transactions.
- Additionally, the Act also paves the way for corporate entities to also act as Certification Authorities for the issuance of Digital Signature Certificates under the Act. There are no distinctions in the Act as to what legal entity may be designated as a Certifying Authority, provided the government's standards are followed.
- Furthermore, the Act permits the companies to electronically file any of their documents with any office, authority, body or agency owned or controlled by the appropriate government by using the electronic form prescribed by the concerned government.
- The use of electronic records and digital signatures in government and its agencies has been approved as a policy matter within the meaning of the IT Act. A digital signature is a mechanical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature enables the recipient to believe that the message was created by a known sender and has not been altered in transit, i.e., the message is tamper-proof. The Government has thus started using digital signatures across all platforms such as granting of licenses, permits, filing of applications, payment of charges and other financial transactions through electronic means.

- Hacking is a common threat faced by most companies nowadays. However, the IT Act changed the landscape completely. A statutory remedy is now provided to corporate entities in case anyone attempts to breaches their computer systems or network and damages or copies data. Damages can be claimed from anyone who uses a computer, computer system or computer network without the permission of the owner or other person in charge of the computer/system or network.

However, the said Act has a few drawbacks:

- Section 66A is considered to be in accordance with Article 19(2) of the Constitution of India since it does not define the terms 'offensive' and 'menacing'. It did not specify whether or not these terms involved defamation, public order, incitement or morality. As such, these terms are open to interpretation.

> ***Note:*** Article 19(2) of the Constitution curtails the freedom of speech and expression to some extent by enabling the State to impose restrictions in the interests of security and sovereignty of India, friendly relations with foreign states, public order, decency or morality, among other things.

- Considering how vulnerable the internet is, the Act has not addressed adequately issues such as privacy and content regulation, which are essential.
- A domain name is not included in the scope of the Act. The law does not include any definition of domain names, nor does it state what the rights and liabilities of domain name owners are.
- The Act doesn't make any provision for the intellectual property rights of domain name proprietors. In the said law, important issues pertaining to copyright, trademark, and patent have not been addressed, therefore creating many loopholes.

INFORMATION TECHNOLOGY RULES (IT RULES)

There are several aspects of the collection, transmission, and processing of data that are covered by the IT Rules, including the following:

- *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:* According to these rules, entities holding individuals' sensitive personal information must maintain certain security standards that are specified.
- *The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021:* To maintain safety over the web of users' data, these rules govern the role of intermediaries, including social media intermediaries, to prevent the transmission of harmful content on the internet.
- *The Information Technology (Guidelines for Cyber Cafe) Rules, 2011:* According to these guidelines, cybercafés must register with an appropriate agency and maintain a record of users' identities and their internet usage.
- *The Information Technology (Electronic Service Delivery) Rules, 2011:* Basically, these regulations give the government the authority to regulate the delivery of certain services, such as applications, certificates, and licenses, by electronic means.
- *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules):* CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. In accordance with rule 12 of the CERT-In rules, a 24-hour incident response helpdesk must be operational at all times. Individuals, organisations and companies can report cybersecurity incidents to Cert-In if they experience a Cybersecurity Incident or threat. The Rules provide an Annexure listing certain Incidents that must be reported to Cert-In immediately.

- Another requirement under Rule 12 is that service providers, intermediaries, data centres, and corporate bodies inform CERT-In within a reasonable timeframe of cybersecurity incidents. As a result of the Cert-In website, Cybersecurity Incidents can be reported in various formats and methods, as well as information on vulnerability reporting, and incident response procedures. In addition to reporting cybersecurity incidents to CERT-In in accordance with its rules, Rule 3(1)(l) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 also requires that all intermediaries shall disclose information about cybersecurity incidents to CERT-In.

Proposed Digital India Act: An Act in Progress to replace Information Technology Act, 2000

With digital transformation at its high in India, March 2023 has witnessed a magnificent move with the official announcement of enacting Digital India Act (DIA) while replacing a 24-year-old Information Technology Act of 2000 (IT Act). This proactive move by the Ministry of Electronics and Information Technology (MeitY) aligns with India's ambitious "Digital India" initiative.

On 9th March 2023, the Minister of State for the Ministry of Electronics and Information Technology (MEITY), held a consultation to officially announce that the Information Technology Act of 2000 (IT Act) will be replaced with a new Digital India Act (DIA), a future-ready legislation. The contents of the new act were laid down in the presentation. The MEITY is conducting rounds of consultations in the coming months and soliciting feedback from various stakeholders. This draft has generated debates and discussions on the regulation of the Internet today.[37]

Nine Pillars of Digital India

1. Broadband Highways
2. Universal Access to Mobile Connectivity
3. Public Internet Access Programme
4. e-Governance: Reforming Government through Technology
5. e-Kranti - Electronic Delivery of Services
6. Information for All
7. Electronics Manufacturing
8. IT for Jobs
9. Early Harvest Programmes

Necessity for Digital India Act (DIA)

The proposed Digital India Act (DIA) *inter-alia* with an aim to provide a *future ready legislation* opts "*principles and rule-based approach*" for regulating digital transactions including the evolving era of Artificial Intelligence and Machine Learning. With this background, we aim to discuss the salient features of DIA and its possible impact on industries for aligning their compliance calendar with principle and rule-based approach.

Need for Digital India Act

- Outdated Regulations: The existing IT Act of 2000 was crafted in an era when the internet had only 5.5 million users, and is ill-equipped to handle the internet's current state.
- Today, with 850 million users, various intermediaries, and new forms of user harms like cyberstalking and doxing, the IT Act falls short of addressing these complexities.

37. Reproduced from Sanhita Chaurita (8th August 2023) Explained: The Digital India Act 2023, Vidhi Centre For Legal Policy.

- Inadequacy of Current Regulations: Despite the existence of regulatory elements like Intermediary Guidelines, Digital Media Ethics Code, and data protection rules, they are insufficient when it comes to governing new-age technologies.
- Need for Legal Adaptation: With technological advancements like AI, Blockchain, and IoT, the legal framework must evolve to address their unique challenges. This includes enhancing cybersecurity measures, data protection, and regulating emerging tech sectors.
- Addressing E-commerce and Online Content: The growth of e-commerce, digital transactions, and online content sharing requires updated regulations. The Digital India Act will tackle issues related to consumer protection, electronic contracts, and content moderation on social media platforms.
- Global Alignment and Best Practices: To engage effectively in the global digital landscape, India's regulations must align with international standards and practices.

On the path of digital economy, we are already witnessing reformative landscape of legal and regulatory regime with major focus on fintech sectors, enterprise and deep technology sectors, e-commerce, consumer protection and data management.

Among other factors, following the major reasons which necessitates the introduction of proposed Digital India Act:

Limitation of IT Act, 2000	Challenges in Cyberspace	Tech-Aligned Regulation
• IT Act is around 24 years old and was enacted in early days of internet. • It does not adequately cover modern internet-based services such e-commerce, social media platforms and alike. • Inadequate principles for data / privacy protection. • Legal recognition of electronic records, transactions and electronic signatures over the electronic medium	• Multiple categories of Intermediaries • Digital Media • Social Media • AI and ML • OTT • Complex forms of user harms – sim-swaps, catfishing, cyber stalking, online gaslighting • Disinformation • Increased flow of data and need to regulate the data at global parameters • Alignment with contemporary regulations including DPDP Act, 2023 and Limitation Act, 1963.	• Need for Global Standards of Cyber Laws • Comprehensive need on user rights, trust & safety. • Emerging Technology • High risk automated-decision making systems. • New forms of cybercrimes. • Requirement of a converged, coordinated & harmonized institutional regulatory body. • To strengthen user rights and security specially women and child safety.

Salient Features of Proposed Digital India Act

The proposed DIA includes following salient features:

- Principle and Rule based Approach
- Digital Governance and Adjudicatory Architecture
- Open Internet
- Safe and Secure Cyberspace
  - *For example - strengthening the penalty framework for non-compliance and issuing advisories on the information & data security practices, etc.*
- Responsible and Ethical Use of Online Technologies
- Safeguard Innovation and Promoting Start-ups
- Digital User Rights
- Regulation of Intermediaries (basis the type of Intermediary) –
  - *for example, enterprise software providers such as cloud service providers should not be subjected to the same set of regulations as that of significant social media intermediaries.*
- *Principle of Safe Harbour*
  - Accountability
  - Inclusive Regulatory Framework – *Balanced with sectoral regulations.*
  - Emerging Technology, Risk (Management) and Guard Rails
  - Ensuring Safety and Privacy of Children (*Industry Specific Requirements*)
  - Algorithmic Transparency and regulation of Artificial Intelligence (*"AI"*)

Requirement of Industry Alignment towards Goals and Proposed Structure of DIA:

One shall always remember one of powerful legal maxim "*Ignorantia Juris Non Excusat*", which means ignorance of law is not an excuse. Hence, one should stay prepared before the proposed DIA is notified. It is to be noted that separate rules will govern different kinds of industry. Hence ***Industry Specific Compliance Calendars*** will be required. Although pursuant to notification of DIA, a detailed proposal on the requirements under DIA along with strategy and pedology on compliance calendars shall follow.

Challenges Ahead in the Implementation of DIA, 2023[38]

- **Burdensome Compliance Requirements**: The act's regulations may place a significant burden on businesses, particularly small and medium-sized enterprises (SMEs).
- **Freedom of Expression**: The review of the "safe harbor" principle for online platforms could potentially impact freedom of expression. Ensuring that the act doesn't curb this fundamental right is a delicate task.
- **Resource and Infrastructure Requirements**: Effective enforcement of the DIA will require substantial resources, expertise, and infrastructure. Investing in these areas will be crucial.
- **Stakeholder Interests**: Balancing the interests of various stakeholders, including tech giants and citizens' rights, poses a significant challenge. Ensuring that all voices are heard and considered in the implementation process is essential.

38. Reproduced from India's Digital Future: The Digital India Act 2023, Drishti IAS, 2023

- **Surveillance and Privacy Concerns**: Critics argue that certain provisions of the act may grant excessive surveillance powers to the government, potentially compromising privacy rights. Robust safeguards should be incorporated to protect against abuse of power and violations of privacy.
- **Data Localization and Cross-Border Data Flows**: The act's approach to data localization is a point of contention. While localization can enhance data protection and security, it may also disrupt cross-border data flows, impacting global businesses that rely on efficient data transfers.

Way Forward for Effective Implementation of DIA, 2023[39]

- Stakeholder Engagement: All relevant stakeholders, including government bodies, technology companies, legal experts, and civil society, should be involved in the drafting and implementation process. This will help create a balanced and comprehensive legal framework.
- Balancing Regulation and Innovation: Stricter regulations, particularly in emerging technologies, could inadvertently stifle entrepreneurial initiatives and deter foreign investments. Striking the right balance between regulation and innovation is critical.
- Collaboration and Capacity Building: Invest in building the capacity of law enforcement agencies, judiciary, and regulatory bodies to effectively enforce the DIA.
- Collaborate with other countries and international organizations to align the DIA with global best practices and standards in the digital space.
- Public Awareness: Conduct public awareness campaigns to educate citizens about their rights and responsibilities in the digital realm, fostering a culture of digital literacy.

Way Forward[40]

The intention behind the DIA is laudable and this legislation will be revamping India's technology sector regulations. It is for the first time that consultations are taking place during the pre-draft stage of the bill. Policymakers are aware of the challenges that might arise therefore the opinions of important stakeholders are being valued. The need for comprehensive and relevant legislation was much needed for the evolving technology sector in India.

While the DIA will promote the growth of India's digital economy, and address the challenges which new-age technologies bring with them like data privacy and cyber security. However, doing away with the safe harbour principle will be criticized by Bigtechs. Additionally, it will require specialists and developed infrastructure for law enforcement, tackling the uncertainties of new-age technologies, AI, deep fakes, and dispute resolution in the proposed legislation. Defining territorial jurisdiction is necessary due to the borderless nature of information and interactions over the Internet. While transparency and accountability are the founding pillars of the act it will also have to balance the interests of important stakeholders like users, big techs, government, businesses, and civil society.

Undoubtedly, it will be one of the most landmark legislations in the jurisprudence of the country as it will protect the freedom of expression and the fundamental rights of citizens on social media platforms. Along with enhancing privacy, online safety, and security, it will also safeguard citizen's data. It will foster innovation and growth of new-age technologies which will be beneficial in education, health, and administration. It will be interesting to see how building this proposed legislation plays out in the coming future.

39. Reproduced from India's Digital Future: The Digital India Act 2023, Drishti IAS, 2023

40. Reproduced from Sanhita Chaurita (8th August 2023) Explained: The Digital India Act 2023, Vidhi Centre For Legal Policy

COMPANIES ACT, 2013

The Companies Act, 2013 is a legislation which regulates the framework of companies right from incorporation of companies, registration, responsibilities, directors, dissolution of company, etc. This Act enshrines in law all the techno-legal requirements that need to be met by a company operating in India. As part of the Companies Act 2013, the Serious Fraud Investigation Office (for brevity, 'SFIO') is entrusted with powers to investigate and prosecute serious frauds committed by Indian companies and their directors.

As a result of the 2014 notification of the Companies Inspection, Investment, and Inquiry Rules, the SFIOs have become even more proactive and serious in regard to this. By ensuring proper coverage of all the regulatory compliances, the legislature ensured that every aspect of cyber forensics, e-discovery, and cybersecurity diligence is adequately covered. Moreover, the Companies (Management and Administration) Rules, 2014 prescribe a strict set of guidelines that confirm the cybersecurity obligations and responsibilities of corporate directors and senior management.

INDIAN PENAL CODE, 1860

If the IT Act is not sufficient to cover specific cyber-crimes, law enforcement agencies can apply the following sections of the Indian Penal Code, 1860 (hereinafter referred to as 'IPC'):

- Section 292 and Section 293: Section 292 and 293 of IPC prohibit publication and sale of obscene books, pamphlets, paper, writing, drawing, painting, etc. which shall be deemed to be 'lascivious or appeals to the prurient interests', which can include obscene advertisements. The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cybercrimes as well. Both these provisions also regulate the manner in which obscene material or sexually explicit acts or exploits of children are published or transmitted electronically. The penalty for such acts is imprisonment up to 2 years and fine up to Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second-time) offenders.
- Section 354C: In this provision, cybercrime is defined as taking or publishing pictures of a woman engaging in a private act without her consent. In this section, voyeurism is discussed exclusively since it includes watching a woman's sexual actions as a crime. In the absence of the essential elements of this section, Section 292 of the IPC and Section 66E of the IT Act are broad enough to include offences of an equivalent nature. Depending on the offence, first-time offenders can face up to 3 years in prison, and second-time offenders can serve up to 7 years in prison.
- Section 354D: Stalking, including physical and cyber stalking, is described and punished in this section. As per this section, the act of any man following and contacting a woman to foster personal interaction despite indication of disinterest or monitoring the use by a woman of the internet, email or any other form of electronic communication amounts to the offence of stalking. This offence is punished by imprisonment of up to 3 years for the first offence and up to 5 years for the second offence, along with a fine in both cases.

In the case of *Kalandi Charan Lenka vs. the State of Odisha (2017)* before the Orissa High Court, the victim received a series of obscene messages from an unknown number. The accused also sent emails to the victim and created a fake account on Facebook containing morphed and offensive images of her. The Orissa High Court, therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC.

- Section 379: Under this section, the offence of theft entails punishment, i.e. imprisonment for up to

three years in addition to the fine. This section may come into play in part because many cyber-crimes involve stolen electronic devices like computers, laptops and mobile phones.

- Section 420: This section talks about cheating and dishonestly inducing delivery of property. Seven-year imprisonment in addition to a fine is imposed under this section which may come into play when cybercriminals commit illegal acts like creating fake websites and cyber frauds.
- Section 463: This section involves falsifying documents or records electronically. Spoofing emails is punishable by up to 7 years in prison and/or a fine under this section.
- Section 465: This provision typically deals with the punishment for forgery. Under this section, offences such as the spoofing of email and the preparation of false documents in cyberspace maybe indirectly covered and punished with imprisonment ranging up to two years, or fine or both. In *Anil Kumar Srivastava vs. Addl Director, MHFW (2005),* the accused had forged the signature of the AD and then filed a case that made false allegations against the AD. Since the accused attempted to pass the forged document off as a genuine document, the Court held that the accused was liable under Sections 465 and 471 of the IPC.
- Section 468: Fraud committed with the intention of cheating may result in a seven-year imprisonment and a fine. Email spoofing may be covered within this section.

Furthermore, there are many more sections of the IT Act and the Indian Penal Code, which pertain to cyber-crimes, in addition to the provisions listed above.

Even though there are laws against cyber-crime in place, the rate of cyber-crime is still rising drastically. It has been reported that cyber-crime in India increased by 11.8% in the year 2020, which accounted for reporting around only 50,000 cases. Cyber-crime is one of the toughest crimes for the Police to solve due to many challenges they face including underreporting, the jurisdiction of crime, public unawareness and the increasing costs of investigation due to technology.

Certain offences may end up being bailable under the IPC but not under the IT Act and vice versa or maybe compoundable under the IPC but not under the IT Act and vice versa due to the overlap between the provisions of the IPC and the IT Act. For example, if the conduct involves hacking or data theft, offences under sections 43 and 66 of the IT Act are bailable and compoundable, whereas offences under Section 378 of the IPC are not bailable and offences under Section 425 of the IPC are not compoundable. Additionally, if the offence is the receipt of stolen property, the offence under section 66B of the IT Act is bailable while the offence under Section 411 of the IPC is not. In the same manner, in respect of the offence of identity theft and cheating by personation, the offences are compoundable and bailable under sections 66C and 66D of the IT Act, whereas the offences under Sections 463, 465, and 468 of the IPC are not compoundable and the offences under sections 468 and 420 of the IPC are not bailable.

In *Gagan Harsh Sharma vs. State of Maharashtra (2018),* the Bombay High Court addressed the issue of non-bailable and non-compoundable offences under sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act that are bailable and compoundable.

Criminal Law is proposed to be replaced from New Legislations

The three new criminal laws that were passed by Parliament in 2023 will come into effect from July 1, 2024, according to a notification by the Ministry of Home Affairs (MHA).[41]

41. Reproduced from The Hindu, Three Criminal Laws to be effective from July 01, 2024. Available at https://www.thehindu.com/news/national/three-newly-enacted-criminal-laws-to-come-into-effect-from-july-1/article67881602.ece

Hon'ble Union Minister of Home Affairs in a conference said that India has abolished the 150-year-old original laws of criminal justice and introduced new laws. He said that two of the major issues in these three laws are related to this conference. First, to deliver timely justice and second, to curb crimes by increasing conviction rate. He said that in all three laws, efforts are being made to take both these issues forward with the help of technology. Home Minister added that we have taken a bold decision and it has been made mandatory for a Forensic Science Officer to visit the crime scene of offences which have punishment of 7 years or more. He said that this will simplify the investigation, it will be easier for the judges and it will also make the prosecution simple. This will also help us in increasing the conviction rate. Along with this, efforts are also being made to modernize the entire process. Hon'ble Minister further said that after 5 years, India's criminal justice system will be the most modern system in the world.[42]

It is to be noted that Section 106(2) of the Bharatiya Nyaya Sanhita (BNS), which provides for punishment of "0-10 years" in "hit and run" cases, has been put on hold. Earlier this year, transporters and drivers across the country struck work to protest the particular provision.

The Bharatiya Nyaya Sanhita, Bharatiya Nagrik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam that will replace the Indian Penal Code, 1860; Code of Criminal Procedure, 1898; and the Indian Evidence Act, 1872, respectively, received President Droupadi Murmu's assent on December 25, 2023.

CYBER SECURITY FRAMEWORK (NCFS)

As the most credible global certification body, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach. To manage cyber-related risks responsibly, the NIST Cybersecurity Framework includes guidelines, standards, and best practices. According to this framework, flexibility and affordability are of prime importance. Moreover, it aims at fostering resilience and protecting critical infrastructure by implementing the following measures:

- A better understanding, management, and reduction of the risks associated with cybersecurity.
- Prevent data loss, misuse, and restoration costs.
- Determine the most critical activities and operations that must be secured.
- Provides evidence of the trustworthiness of organizations that protect critical assets.
- Optimize the cybersecurity 'Return on Investment' (ROI) by prioritizing investments.
- Responds to regulatory and contractual requirements.
- Assists in the wider information security program.
- Using the NIST CSF framework in conjunction with ISO/IEC 27001 simplifies the process of managing cybersecurity risk. Moreover, NIST's cybersecurity directive also allows for easier collaboration in the organization as well as across the supply chain, allowing for more effective communication.

DATA PROTECTION AND AI: LAWS AND REGULATIONS

In 2019, in a two-day G-20 summit in Osaka in Japan, the Prime Minister of India underscored the significance of Digital Economy & Artificial Intelligence. He emphasized the government's reliance on the 5 'I's that stand

42. Brief from Union Home Minister and Minister of Cooperation Shri Amit Shah address on the 5th International and 44th All India Criminology Conference of National Forensic Science University (NFSU) in Gandhinagar, Gujarat, Press Information Bureau of India. https://pib.gov.in/PressReleasePage.aspx?PRID=1998860

for ***Inclusiveness, Indigenization, Innovation, Investment in infrastructure & International*** cooperation in developing these two areas. The concept of Artificial Intelligence is based on the idea of building machines capable of thinking, acting, and learning like humans.

Artificial Intelligence: Brief Description

- It describes the action of machines accomplishing tasks that have historically required human intelligence.
- It includes technologies like machine learning, pattern recognition, big data, neural networks, self-algorithms etc.
- The origin of the concept can be traced back to the Greek mythology, although it is only during modern history when stored program electronic computers were developed.
- Example: Millions of algorithms and codes are there around the humans to understand their commands and perform human-like tasks. Facebook's list of suggested friends for its users, a pop-up page, telling about an upcoming sale of the favourite brand of shoes and clothes that comes on screen while browsing the internet are the work of artificial intelligence.
- A Complex Technology: AI involves complex things such as feeding a particular data into the machine and making it react as per the different situations. It is basically about creating self-learning patterns where the machine can give answers to the never answered questions like a human would ever do.

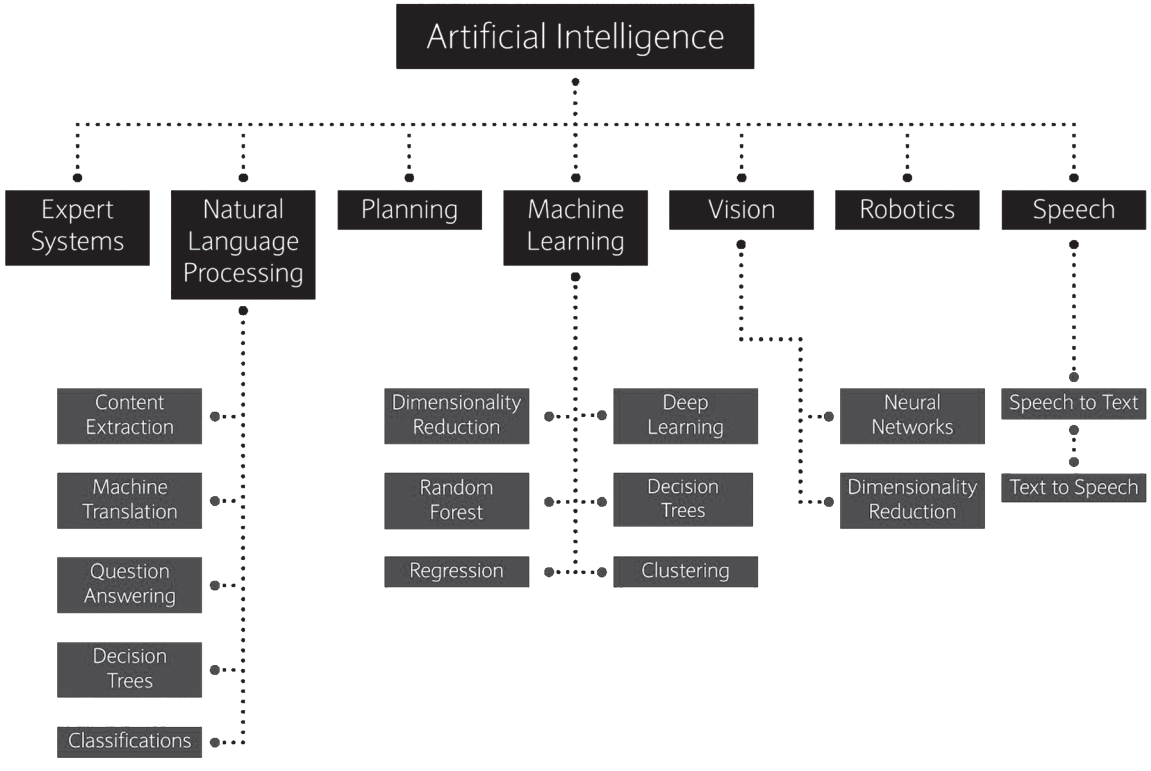
AI is a Different Technology

- AI is different from hardware driven robotic automation. Instead of automating manual tasks, AI performs frequent high volume computerized tasks reliably.
- AI is often misunderstood for machine learning. AI is a broader concept with a bunch of technologies that include machine learning and other technologies like natural language processing, inference algorithms, neutron networks etc.

Evolution

- In the year 1956, American computer scientist John McCarthy organised the Dartmouth Conference, at which the term 'Artificial Intelligence' was first adopted. From then on, the world discovered the ideas of the ability of machines to look at social problems using knowledge data and competition.
- There used to be several dedicated projects on the same and the government was funding the research.
- Every aspect of science and especially when one starts looking at empowering machines to behave and act like human beings, the questions of ethics arise. About 70's and late 80's, there was a time when the governments stopped funding research into AI.
- AI experienced a resurgence following concurrent advances in computer power and large amounts of data and theoretical understanding in the 21st century.
- AI techniques now have become an essential part of the technology industry helping to solve many challenging problems in computer-science. From Apple SIRI to self-driving cars, AI is progressing rapidly.

AI Methods



Source: https://www.drishtiias.com/

India and AI

- According to the Global AI Report 2019 (i.e. a Canada based company's report), India stood at the ninth position in terms of the number of the AI specialists working in the field, while the US, China and the UK topped the list.
- The top ranked countries in this Report have many academic institutes with programs on AI. They have therefore a much greater number of people skilled to do research in the field.
- India, on the contrary, lacks the opportunities in formal education in data science but is slowly trying to encourage the adoption of AI in educational institutes.
- Starting this year, the CBSE has AI as an elective subject for its ninth grade classes.
- The International Institute of Information Technology, Hyderabad (for brevity, 'IIT Hyderabad') has launched a full-fledged Bachelor of Technology (B Tech) program in AI becoming the first Indian educational institution to do so. It is also most likely the third educational institute in the world after Carnegie Mellon University and the Massachusetts Institute of Technology to have a full-fledged B Tech program on AI.
- IIIT Hyderabad is another educational institute that introduced popular executive programs on AI and machine learning and blockchain and distributed ledger technologies.
- Defence forces of India are now venturing into the products and technologies which will aid defence measures using the AI and technologies.

- In India, corporates have started collaborating with academia on AI. IBM's Blue project is an example.
- There are many startups in the country which are doing great work in image analytics, data analytics, predictive intelligence etc.
- It is estimated that AI will add 957 billion dollars to India's GDP by the year 2035 boosting India's annual growth by 1.3% points.

Benefits

- In Policing: India still has a conventional policing. AI based products open a new window of opportunity to do predictive policing in India. With the help of AI, one can predict the pattern of crime, analyze lot of CCTV footage which are available across the country to identify suspects.

> ***Note:*** Policing refers to maintenance of law and order by the police force in a country.

- Government is digitizing all the records, especially the crime records putting it into one single place called CCTNS, i.e. Crime and Criminal Tracking Network & Systems, where all the data including the image, biometrics, or the criminal history of a convict or suspect is available.
- In Agriculture: It has many uses, for example, it can help sense one how much water the crop needs.
- For solving complex issues like efficient utilization of available resources.
- Analyzing the Data: The AI technology helps in analyzing data and thus can improve the efficiency of the systems like power management in cars, mobile devices, weather predictions, video and image analysis.

Steps taken by the Government

- In 2018-19 budget, the government mandated NITI Aayog to establish the National Program on AI with a view to guiding research and development in new and emerging technologies.
- NITI Aayog then adopted a three pronged approach undertaking exploratory proof of concept AI projects in various areas, crafting a national strategy for building a vibrant AI ecosystem in India and collaborating with various experts and stakeholders.
- On 20th March, 2019, NITI Aayog circulated the cabinet note to establish a cloud computing platform called AIRAWAT (Artificial Intelligence Research, Analytics and Knowledge Assimilation Platform).
- The note circulated by NITI Aayog proposes that the government should pump in Rs. 7,500 crore rupees over 3 years as well as set up a high-level task force that will oversee the roll out and implementation of AI.
- The move to create cloud computing platform is part of the government's goal of making India a pioneer amongst emerging economies with regards to AI and transform sectors like education, health, agriculture, urbanization and mobility.
- In Budget 2018, the government announced funds to support the country's AI, machine learning, robotics and IoT sector.
- As part of the initiative, NITI Aayog in the year 2018, published a draft National Strategy for AI, planning its scope for research, adoption and commercialization.
- It envisioned AI use case clearly in the sectors like healthcare, agriculture, education, smart cities and infrastructure, smart mobility and transportation.

- The Ministry of Commerce and Industry has also set up task forces to explore the use of AI and Big Data technologies in the country.
- In the Budget 2019-20, the government has announced setting up of a National Sports Education Board under Khelo India to prepare youth for new age skills, Artificial Intelligence, IoT, Big Data, 3D Printing, Virtual Reality etc.

Data Protection: Indian Legal Perspective

Need of Legal Mechanism

To encounter the challenges of information privacy and to promote legal control over privacy protection in electronic transactions, some legal policies and regulations have already been established at international and national level. At international level, some fair information principles like Notice, Choice, Access, Consent, Enforcement etc. are directed to be followed by the e-commerce companies to ensure the information privacy in the conduct of online transactions. Though at the industry level, even the e-commerce companies are also taking some steps to protect the information privacy of the individuals by adopting and declaring privacy policy, yet much is left to be governed by the nationally and internationally commended regulations.

At national level, countries around the world have enacted different laws to protect privacy of individuals. A Business Week/Harris Poll survey[43] found that over 57% of the online buyers want some legal regulations or law to control the use and disclosure of their information by e-commerce websites and to ensure protection of information privacy. Numerous survey[44] conducted by various researchers (Harris Poll Survey, Georgia Institute of Technology survey, Pew Internet and American life etc.) have discovered the fact that consumers as well as businesses want legal protection to regulate protection of personal data and privacy in the regime of e-commerce transactions.

Enumerations below support the need of legal protection for data privacy in e-commerce transactions:

A. Business Week/Harris Poll survey shows that 86% of their respondents want that online businesses should provide consumers with 'opt-in' and 'opt-out' clauses before collecting their personal and sensitive personal information. This supports the demand for consumers' legal control on personal data collection and further sharing of data.

B. A survey conducted by American Society of Newspaper Editors on privacy concerns (2000)[45] showed that 51% of respondents strongly felt that online companies might violate their personal privacy and same study showed that 52% of the respondents were having 'no confidence at all' in the online company that they use the personal information of their consumers exactly in the same way which they had said they would.

C. Number of surveys conducted by Georgia Institute of Technology's Graphic, Visualization, and Usability (GVU) Center[46] has discovered that a majority of individuals strongly insist upon and support anonymity in electronic transactions.

D. Business Week/Harris Poll (2000)[47] survey found that 89% of their respondents were not comfortable with the online tracking system of online websites and prefer a restriction to be imposed on the web tracking especially in the tracking of their personal information.

43. Harris Poll, Privacy and American Business Press Release (online). (June 24, 2012), http://www.epic.org/privacy/survey/.

44. Harris Poll, Online Privacy: A Growing Threat, Business Week, 96 (2000). (June 22, 2012), http://epic.org/privacy/survey/.

45. See, Public Opinion on Privacy, Supra note 181.

46. Survey Report. (June 22, 2012), http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/graphs/#privacy.

47. Public Opinion on Privacy, Supra note 181.

E. Pew Internet and American Life Project[48] (2000) found in their studies that 54% of internet users were objecting to online tracking and they were afraid of the creation of their profile in online transactions. USA Weekend Poll (2000) also showed that 65% of respondents thought that tracking computer usage and creation of users' profile in internet was an invasion of privacy.

F. Pew Internet and American Life Project study showed that 56% of internet users are unaware and unknown about installation and use of cookies and more sophisticated tracking tools, such as 'web bugs' or 'spyware' by online business to access and collect consumers' personal information and thereafter tracking their online behaviour.

G. Pew and American Life Report[49] (2000 and 2008) showed that 94% of internet users believe that privacy violations should be regulated by the State and they want ability to avail remedies against privacy invasions by online companies.

It can be assumed that adequate legal protection over privacy concern and information privacy will ensure individuals' about the protection of their privacy rights in e-commerce transactions.

Indian Laws for Data Protection

Individual's data like name, telephone numbers, profession, family, choices, pan card number, credit card details, social security number etc. are disclosed in the electronic transactions and then are available on various websites.[50] Though the authorized collection and the storage of data may only create probability of the loss of information privacy[51] but the unauthorized access, collection, use, misuse, relocation and transmission of the information to the third party essentially result in the intrusion of information privacy of the individuals. Hence, improper control on transmission of information can be the root cause for privacy challenges in electronic transactions. Law will not only determine, what privacy entails, how it is to be valued, and to what extent it should be endowed with legal protection, but also ensures authorized protection to the circumstances under which individuals can value their privacy and protect it from the violation of unauthorized intrusion by others.[52] Knight Bruce in *Prince Albert v Strange*[53] upheld that a third party intrusion into one's privacy results in grave violation of right to privacy and hence, implies need of legal protection to right to privacy.

To counter the challenges of information and communication technology, the Indian Legislature has enacted Information Technology Act, 2000, Information Technology (Amendment) Act, 2008 and other legislations too, but challenges of information privacy and data privacy are not addressed in an exclusive and specific manner. India is not having a comprehensive legislative framework to deal specifically with privacy issues in electronic transactions.[54] The Information Technology Act, 2000 was enacted chiefly to facilitate e-commerce; hence privacy is not the primary concern of the Act.[55]

---

48. Public Opinion on Privacy, Supra note 181.

49. Report on Trust and Privacy Online: Why American Want to rewrite the rules, Pew Internet and American Life Project. (June 22, 2012), http://www.pewinternet.org/reports/toc.asp?Report=19.

50. Miriam J. Metzger, Privacy, Trust and Disclosure: Exposing Barriers to Electronic Commerce, Journal of Computer Mediated Communication, Vol. 9 No. 4, (2004). (May 27, 2012), http://jcmc.indiana.edu/vol9/issue4/metzger.html.

51. Information privacy is synonym to data privacy. Information Privacy or data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. (May 27, 2012), http://en.wikipedia.org/wiki/Information_privacy.

52. Ruth Gavison, Privacy and the Limits of Law, The Yale Law Journal, Vol. 89, No. 3, 421-471 (Jan. 1980). (May 28, 2012), http://www.jstor.org/stable/795891?origin=JSTOR-pdfand.

53. Prince Albert v Strange (1848) 2 De G and SM 652, 698; 64 ER 293, 314.

54. Shrikant Ardhapurkar et al., Privacy and Data Protection in Cyberspace in Indian Environment, International Journal of Engineering Science and Technology, Vol. 2, No. 5, 942-951 (2010).

55. Mathur, S. K., Indian Information Technology Industry: Past, Present and Future A Tool for National Development, Journal of Theoretical and Applied Information Technology. (2006) (Online). (May 28, 2012), http://perso.univ-rennes1.fr/eric.darmon/floss/papers/MATHUR.pdf.

Information Technology Act, 2000 and Data Protection

Indian legislature has enacted Information Technology Act, 2000 for the purpose of complying with the requirements of UNCLTRAL (United Nations Commission on International Trade Law) model law[56] on electronic commerce[57] on one hand, and for providing legal recognition to the transactions carried out by the means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.

The Act was brought into existence for the following reasons:[58]

i. To facilitate the development of e-commerce transactions;

ii. To ensure the regulatory environment for the security of e-commerce transactions;

iii. To provide legal structure for governing electronic contracts, security and integrity of electronic transactions;

iv. To facilitate and validate the use of digital signatures for authenticating the electronic records;

v. To facilitate the growth of Indian IT sector across the globe;

vi. To ensure the safety and security of electronic transactions; and

vii. To attract Foreign Direct Investment (FDI) in Information Technology sector.

Note: E-commerce or electronic commerce is the trading of goods and services over the internet.

Under the regime of privacy rights, every individual wants to keep his or her personal affairs to himself, but in the electronic transactions, variety of individual's information are collected and stored, which can easily enable others to identify that individual. Databases collected in the online transactions, when cross-matched can easily create profile of the individuals and can predict their behaviour. This involves the sheer violation of data privacy in electronic transactions. The provisions of the Act for the purpose of data privacy in electronic transactions can be examined as follows:

A. Provisions pertaining to data[59] protection and personal data[60] protection.

In Information Technology, Act, 2000, no such concept as 'personal data' has been discussed. It defines 'data'[61] but does not provide any definition of personal data. Furthermore, the definition of data

56. UNCITRAL Model Law on Electronic Commerce, Guide to Enactment with 1996 (May 27, 2013), http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

57. The UNCITRAL Model Law on E-commerce is a resolution of the U.N. General Assembly which recommends that all States give favorable consideration to the Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

58. Nasir, M. Ali, Legal Issues involved in E-commerce, Ubiquity (Mazgine), New York, NY, USA (2004). (May 28, 2012), http://ubiquity.acm.org/article.cfm?id=985607.

59. Data means information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by Section 68, or(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d). Source: Information Commission Office, Government of United Kingdom. (May 29, 2012), http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx.

60. Personal data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and (c) includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Source: Information Commission Office, Government of United Kingdom. (May 29, 2012), http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx.

61. Section 2 (o) of IT Act, 2000 'data' means a representation of information, knowledge, facts, concepts or instructions which are being

is provided with more relevancy to cybercrime.[62] Hence, there is confusion among the researchers whether the Indian IT Act, 2000 deals with 'data protection' or with 'personal data protection' as well.

B. Civil Liability in case of data, computer database theft, privacy violation etc.[63]

The Act has devoted Section 43 (a) to 43 (h) to enlist wide range of cyber contraventions related to unauthorized access to computer, computer system, computer network and resources. Section 43 of the Act[64] covers various issues, which create civil liability against the wrongdoer and provides for damages (not exceeding one crore rupees) to the person so affected from the defined instances.

These instances include:

i. Computer trespass, violation of privacy etc.

ii. Digital copying, downloading and extraction of data, computer database or information; theft of data held or stored in any media,

iii. Data contamination, computer disruption etc.,

iv. Data loss, data corruption etc.,

v. Computer data/database disruption, spamming etc.,

vi. Denial of service attacks, data theft, fraud, forgery etc.

C. Criminal Liability in case of data, computer database theft, privacy violation etc.[65]

The Act also provides (vide Chapter XI) for defining and creating liability for cyber offences. Sections 65 to 74 of the Act cover a wide range of cyber offences related to unauthorized alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, and computer database. Some provisions deal with the data related offences, like Section-65 related to 'Tampering with the computer source' which was not limited to the protection of computer source code but was extending safeguards for computer data base from unauthorized access. Section 66 (Hacking with computer system), was also indirectly protecting data from unauthorized access and misuse. According to Dr. Unni, unauthorized access to any information diminishes its value/utility and hence injures the confidentiality of a document.[66] For example, if any sensitive personal information is transmitted over e-mail or saved in an e-mail, or in computer and if any person accesses the said document without any authority, then the value of the information is completely lost and it will result in loss of personal data and will make the accessing party liable under Section 66.

D. It is noteworthy that to make a person liable under Section 66, his guilty intention to cause such access has to be proved. Further, out of various provisions dealing with cyber offences, it is only Section 72[67]

---

prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

62. The Final Report: The First Analysis of the Personal Data Protection Law in India, Prepared by CRID-University of Namur, Report delivered in the framework of contract, JLS/C4/2005/15 between CRID and the Directorate General, Justice, Freedom and Security. (May 29, 2012), http://ec.europa.eu/justice/data-protection/index_en.htm.

63. Sharma, Vakul, Information Technology-Law and Practice, Delhi: Universal Law Publishing Co. Pvt. Ltd (2004).

64. Section 43 of Information Technology Act, 2000: Penalty for damage to computer, computer system, etc. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

65. Sharma, Vakul, Supra note 334.

66. V.K. Unni, Internet Service Provider's Liability for Copyright Infringement-How to clear the Misty Indian Perspective, Richmond Journal of Law and Technology. Vol. 13 (2001). (May 29, 2012), http://jolt.richmond.edu/v8i2/article1.html.

67. Section 72 of Information Technology Act, 2000: Penalty for breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations

of the Act, which is specifically directed at the protection of confidentiality and privacy. Section 72 aimed at the protection of privacy and confidentiality from public (and private) authorities,[68] which have been granted power under the provisions of Information Technology Act, 2000 to secure access to any electronic record, book, register, correspondence, information, document or other material information. The purpose of incorporating this section was to ensure that the person who is legally entitled to secure an access to any information[69] shall not take unfair and unmerited advantage of such information by disclosing it to any unauthorized third party without seeking due consent. This section creates an obligation of confidence between the 'data collectors' and 'data subject'. Section 72 has a limited application, as it is applicable only to the persons who have gained access to the information under some authorized channel and not to the unauthorized access of personal information by available means.[70]

From the above discussion, it can be submitted that Information Technology Act, 2000 is not a data protection legislation per se. The Act does not lay down any specific provisions for data protection and privacy protection. The IT Act, 2000 is a general legislation, which articulates on various subject matters that involves digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. Therefore, the sphere of data protection and privacy in electronic transactions was largely unregulated, which led to amendments in information technology laws in the year 2008.

The Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008 has been enacted to facilitate and legalize e-commerce transactions, e-fund transfers, e-storage of data, e-filling of documents with the Government departments on one side and to increase the protection of personal data and information for national security, countries' economy, public health and safety on the other.[71] Section 43A of this Act directs that all body corporates,[72] which are in possession of data and information of their consumers in their computer source, will implement 'reasonable security practices[73]' to prevent the unauthorized access to the personal data of their consumers. This section further entails that failure to protect the sensitive personal data of the individuals during the processing period by the company will make company liable to compensate the aggrieved person, whose personal data is so compromised. While explaining Section 43A of IT (Amendment Act), 2008, Kamlesh Bajaj[74] has detailed that

made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

68. These public and private authorities may be referred as 'data collectors' or 'data users'.

69. Persons conferred under the Act : The Act has conferred powers to : a)The Controller of Certifying Authorities (Ss. 17-18) b) The Deputy and Assistant Controllers of Certifying Authorities (Ss. 17 and 27) c)Licensed Certifying Authorities (S. 31) and Auditors (Rule 312) d) The Adjudicating Officer (S 46) e) The Presiding Officer of the Cyber Appellate Tribunal (Ss. 48-49) f) The Registrar of the cyber Appellate tribunal (S. 56 and rule 263) g)Network Service provider (S. 79) h) Police Officer (Deputy Superintendent of Police) (S. 80). (May 29, 2012), http://www.legalserviceindia.com/article/l288-Breach-of-privacy-and-Confidentiality-.html.

70. Salim Nimitha, Breach of Privacy and Confidentiality under the Information Technology Act, 2000, Legal Service India, (2009). (May 29, 2012), http://www.legalserviceindia.com/article/l288-Breach-of-privacy-and-Confidentiality-.html.

71. Workshop Report, National Seminar on Enforcement of Cyber law, New Delhi, (May 8, 2010). (May 27, 2012) http://catindia.gov.in/pdfFiles/IT_Act_2000_vs_2008.pdf.

72. Section 43 A, Explanation (i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

73. Section 43 A, Explanation (ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

74. CEO of Data Security Council of India, 2009.

the company will be liable for the loss of data during its processing at company's end and the company cannot seek exemption from their responsibility on the ground that there was no negligence on the part of the company in implementing or maintaining reasonable security practices. He further explained that reasonable security practices and procedure will constitute practices and procedures to protect information from unauthorized access, damage, use, modification, disclosure or impairment as may be specified in an agreement between the parties or as may be specified in any law in force.

The penalty under Section 72 of IT Act, 2000 for the disclosure of information was restricted only to those who are legally authorized to secure access to an electronic record and document under the Act, and hence Section 72-A[75] has been incorporated in IT (Amendment) Act, 2008, which provides liabilities of intermediaries and other persons for breach of privacy and confidentiality under lawful contract. Section 72-A[76] reads as, 'save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract; has secured access to any material containing personal information about another person; with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain; discloses; without the consent of the person concerned, or in breach of a lawful contract; such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. Apart from Sections 43A and 72A, there are some other provisions as well which though not specifically but in one way or other tackle the challenges of data protection and data privacy.

The provisions are:

A. Section 66 – Computer Related Offences.

B. Section 66A – Punishment for sending offensive messages through communication service, etc.

C. Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device.

D. Section 66C – Punishment for identity theft.

E. Section 66D – Punishment for cheating by personation by using computer resource.

F. Section 66E – Punishment for violation of privacy.

G. Section 66F – Punishment for cyber terrorism.

H. Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

I. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

J. Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

K. Section 67C – Preservation and Retention of information by intermediaries.

L. Section 69 – Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

M. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource.

N. Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

O. Section 79 – Exemption from liability of intermediary in certain cases.

75. Penalty for breach of confidentiality and privacy.

76. Section 72A: Punishment for disclosure of information in breach of lawful contract.

P. Section 84A –Modes or methods for encryption.

Q. Section 84B –Punishment for abetment of offences.

R. Section 84C –Punishment for attempt to commit offences.

Personal Data Protection Bill, 2019 - Key Highlights

The Government of India had introduced the Personal Data Protection Bill 2019 (hereinafter referred to as 'PDP Bill') in the Lok Sabha on 11 December 2019. The "Bill" was referred for examination and recommendations to a Joint Committee of both Houses of Parliament (called JPC) on 12 December 2019. JPC received more than 200 representations including that of Dua Associates / Dua Consulting. Around eight members had submitted their written dissent on the said Bill.

The Joint Parliamentary Committee chaired by Member of Parliament, Shri P.P. Chaudhary tabled the report on the Bill along with the amended Bill before both Houses of Parliament on 16th of December 2021. The Committee deliberated for over two years, during which time that Bill underwent substantial changes in scope and nature. A total of 188 amendments have been recommended out of which 91 amendments are of significant nature, while the rest are editing of legal nature in different sections.

Salient features of the "Bill" introduced on 11th December, 2019:

The "PDP Bill 2019" which defines both personal and non-personal data, is a substantive framework which introduces a specialized regulatory approach for the Protection and Privacy of Data in any form (digital or non-digital) in India. The proposed legal framework would be applicable to processing, storage and transfer of any form of personal data across sectors of the economy, academia, industry and the society. The Bill has limited provisions relating to Non Personal Data (NPD).

The framework is on the lines and pattern of General Data Protection Regulations (GDPR) of European Union. Some of the provisions of the "Bill" also reflect the directions followed in the California Privacy Act.

The framework classifies data into 3 broad categories namely:

- Personal Data
- Sensitive Personal Data (SPD)
- Critical Sensitive Personal Data

The nature of sensitive personal data has been defined in the legal terms. The entities across different sectors and individuals will be required to follow its provisions while processing, storing and transmitting data in the domestic territory and in cross-border exchange too. The provisions provide for special conditions to process biometric data.

The consent of the user with respect to collecting, and usage of his/her "data" is the underlying feature of the framework. A framework for consent mechanism is proposed. The Bill also has provisions relating to ground for processing of data without consent.

The Bill provides for the rights of the Data Principal including right of data portability. There are special requirements in the Bill for processing of personal and sensitive data related to children.

The framework would regulate 'data localisation' particularly 'sensitive personal data' and 'critical sensitive data'. Consent of the user and approval of the Regulator would be essential for cross border transfer of Personal Data.

Any breach of sensitive personal data and critical sensitive data will attract heavy fine and compensation to the Data Principal (the owner of such data).

The Data Protection framework proposes to set up an elaborate regulatory mechanism consisting of a

Regulatory Authority namely Data Protection Authority (DPA) Adjudication and Appellate Tribunal to regulate process storage and flow of data in the country. All entities would be obligated to appoint a Data Protection Officer who will have responsibility of enforcement and supervision of privacy policy and reporting of data breach to the concerned authorities.

India's Digital Personal Data Protection Act, 2023: Key Provisions[77]

Initially introduced in 2019, the Digital Personal Data Protection Act holds considerable importance as a legislative measure aimed at safeguarding individuals' privacy rights. Its primary focus lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. The DPDP Bill underwent 81 amendments after its initial introduction, resulting in a comprehensive overhaul to its present form.

By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the challenges posed by data handling in the digital age. Key provisions of the DPDP Act, 2023 are as follows:

Definitions: Although many concepts in the DPDP Act closely resemble those found in the EU's General Data Protection Regulation (GDPR), framework, there are differences in how terminology is used.

(a) **Data fiduciary**: This refers to the entity that, either independently or in collaboration with others, establishes both the purpose and the methods for processing personal data (similar to a data controller). The government can classify any data fiduciary or a specific group of data fiduciaries as 'significant data fiduciaries' (SDFs). The criteria for this classification as an SDF include he nature of processing activities (such as the volume and sensitivity of personal data involved and the potential impact on data principals' rights) to broader societal and national concerns (such as the potential effects on India's sovereignty and integrity, electoral democracy, state security, and public order). The designation of SDF comes with heightened compliance obligations as explained below.

(b) **Data processor**: This is an entity responsible for processing digital personal data on behalf of a data fiduciary.

(c) **Data principal**: These are individuals whose personal data is gathered and processed (equivalent to a data subject).

(d) **Consent manager**: A person registered with the Data Protection Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent, and interoperable platform.

Applicability: The DPDP Act applies to all data, whether originally online or offline and later digitized, in India. Additionally, the Act applies to the processing of digital personal data beyond India's borders, particularly when it encompasses the provision of goods or services to individuals within the Indian territory.

Age verification mechanisms will be necessary for all companies in India (telcos, banks, e-commerce, etc.) under the new DPDP law, per reporting from The Economic Times. The compliance requirement is not just limited to social media platforms. This is essential to record the verifiable consent of users per legal experts

Personal data breach: This means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data.

Individual consent to use data and data principal rights: Under the new legislation, personal data will be included and processed only with explicit consent from the individual, unless specific circumstances pertaining

77. Reproduced from Khyati Anand and Melissa Cyrill (September 18, 2023), India's Digital Personal Data Protection Act, 2023: Data Privacy Compliance India Briefing. Available at https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/

to national security, law, and order require otherwise. Under data principal rights, individuals also have the right to information, right to correction and erasure, right to grievance redressal, and right to nominate any other person to exercise these rights in the event of the individual's death or incapacity. Currently, there is no specified timeline for the implementation of grievance redressal and data principal rights.

Additional obligations of SDFs: Depending on the quantity and sensitivity of the data they manage—data fiduciaries deemed as SDF are subject to additional obligations under the DPDP Act. Every significant data fiduciary is required to appoint a Data Protection Officer (DPO) responsible for addressing the inquiries and concerns of data principals—those individuals whose data is collected and processed. Regarding international data transfers, the DPDP Act permits data fiduciaries to transfer personal data for processing to any country or territory outside India. However, the central government can impose restrictions through notifications. These restrictions will be determined after assessing relevant factors and establishing necessary terms and conditions to ensure the maintenance of data protection standards during international processing.

Establishment of a Data Protection Board: The Data Protection Board will function as an impartial adjudicatory body responsible for resolving privacy-related grievances and disputes between relevant parties. As an independent regulator, it will possess the authority to ascertain instances of non-compliance with the Act's provisions and impose penalties accordingly. The appointment of the chief executive and board members of the Data Protection Board will be carried out by the central government, ensuring a fair and transparent selection process. To provide an avenue for customers to challenge decisions made by the Data Protection Board, the government will establish an appellate body. This appellate body may be assigned to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which will be responsible for adjudicating disputes related to data protection and hearing appeals against the decisions made by the Data Protection Board.

Voluntary undertaking: Under this provision, the Data Protection Board has the authority to accept a voluntary commitment related to compliance with the DPDP Act's provisions from any data fiduciary at any stage of complaint proceedings. This voluntary undertaking may entail specific actions to be taken or refrained from by the concerned party. Furthermore, the terms of the voluntary undertaking can be modified by the Board if necessary. The voluntary undertaking serves as a legal barrier to proceedings concerning the subject matter of the commitment, unless the data fiduciary fails to adhere to its terms. In the event of non-compliance, such a breach is considered a violation of the DPDP Act, and the Board is authorized to impose penalties for this infringement. Additionally, the Board has the discretion to require the undertaking to be made public.

Alternate disclosure mechanism: This mechanism will allow two parties to settle their complaints with the help of a mediator.

Offence and penalties: Data fiduciaries can face penalties of up to INR 2.5 billion for failing to comply with the provisions. These include: penalties of up to INR 10,000 for breach of the duty towards data principals; penalty up to INR 2.5 billion for failing to take reasonable security safeguards to prevent breach of personal data; fines up to INR 2 billion for failure to notify the Data Protection Board and affected data principals in case of a personal data breach; penalties of up to INR 2 billion for violation of additional obligations related to children's data; penalty of INR 1.5 billion for failure to comply with additional obligations of significant data fiduciary; penalty of INR 500 million for breach of any other provision of the DPDP Act, 2023 and rules made thereunder.

Conflict with existing laws: The provisions of the DPDP Act will be in addition to and not supersede any other law currently in effect. However, in case of any conflict between a provision of this Act and a provision of any other law currently in effect, the provision of this Act shall take precedence to the extent of such conflict.

Exemptions under the DPDP Act

The exemptions provided in the DPDP Act are as follows:

- For notified agencies, in the interest of security, sovereignty, public order, etc.

- For research, archiving, or statistical purposes.
- For start-ups or other notified categories of data fiduciaries.
- To enforce legal rights and claims.
- To perform judicial or regulatory functions.
- To prevent, detect, investigate, or prosecute offences.
- To process in India personal data of non-residents under foreign contract.
- For approved merger, demerger, etc.
- To locate defaulters and their financial assets etc.

Steps for companies prepare for compliance under the Digital Personal Data Protection Act

By following the below steps, companies can prepare for compliance with India's DPDP Act and protect personal data in line with regulatory guidelines.

Assess and build data privacy:

- Evaluate current compliance status.
- Create a phased action plan covering governance, technology, people, and processes.
- Establish a privacy organization with defined roles, including the DPO, especially if your entity's status is an SDF.

Inventory personal data systems:

- Identify critical data storage and processing systems.

Identify data processors:

- List third parties handling personal data.
- Update agreements and communicate responsibilities.

Draft DPDP Act-compliant documents:

- Create approved data privacy policies and processes.
- Update necessary documents.
- Develop privacy notices, consent forms, and standard contract clauses.

Design consent mechanisms:

- Define consent types.
- Develop user-friendly consent processes.
- Implement efficient consent management tools.

Establish data principal rights handling:

- Set up processes for addressing data principal rights.
- Develop procedures for request handling.
- Use tools for efficient rights management.

Implement data breach response:

- Create breach management processes.
- Integrate with incident management.

Define data retention periods:

- Categorize data and align retention periods with requirements.

Evaluate and implement privacy technologies:

- Choose suitable tech solutions.
- Assess compatibility and scalability.
- Implement chosen solutions.

Conduct communication and awareness programs:

- Develop plans and materials.
- Launch awareness initiatives.
- Provide training to stakeholders.

Monitor government notifications:

- Stay updated on Central Government notifications and any forthcoming rules under the Act.
- Take necessary actions based on government directives.

Global Data Protection Models

European Union (EU) model: The EU's GDPR imposes stringent requirements on organizations to ensure the careful safeguarding of personal data and demands evidence of such protection. The regulation establishes rigorous standards for obtaining consent, empowering customers to exercise control over how their data is handled and protected. Widely acknowledged as a ground-breaking and crucial legislative framework, the GDPR offers valuable guidance to countries in defining the fundamental rights and responsibilities that should be integrated into their own data protection laws. Its primary objective is to effectively respond to the challenges posed by our increasingly digital and interconnected world.

United States (US) model: The US model emphasizes safeguarding an individual's personal privacy from government intrusion. It permits the collection of personal information, provided that the individual is made aware of such data collection and its intended use. Unlike some other countries, the US does not have a singular data protection regulation; instead, it has a combination of laws at both the federal and state levels that are designed to protect the data of its residents.

China model: The Personal Information Protection Law (PIPL) introduces enhanced rights for data principals in China, aiming to curb the improper usage of personal data. The law encompasses key notions, such as personal information, sensitive personal information, and processing. Notably, it explicitly defines its jurisdiction beyond national borders. The PIPL incorporates fundamental elements of data protection, including principles governing the processing of personal information, provisions for consent and non-consent-based grounds for processing, mechanisms for cross-border data transfers, and the rights of data subjects.

EUROPEAN UNION (PROPOSED) AI ACT, 2024[78]

The Artificial Intelligence Act (AI Act) is a proposed European Union regulation on Artificial Intelligence (AI) in the European Union. It aims to establish a common regulatory and legal framework for AI. Proposed by the European Commission on 21 April 2021 and passed in the European Parliament on 13 March 2024, it awaits reading in the EU Council.

78. Reproduced from High-level summary of the AI Act, EU Artificial Intelligence. Available at https://artificialintelligenceact.eu/high-level-summary/

Its scope would encompass all types of AI in a broad range of sectors (exceptions include AI systems used solely for military, national security, research, and non-professional purpose). As a piece of product regulation, it would not confer rights on individuals, but would regulate the providers of AI systems, and entities using AI in a professional context.

The AI Act was revised following the rise in popularity of generative AI systems such as ChatGPT, whose general-purpose capabilities present different stakes and did not fit the defined framework. More restrictive regulations are planned for powerful generative AI systems with systemic impact.

Summary of European Union proposed AI Act

The highly anticipated EU Artificial Intelligence Act is finally here! With extra-territorial reach and wide-reaching ramifications for providers, deployers, and users of Artificial Intelligence ("AI"), the Artificial Intelligence Act ("AI Act") was finally approved by the European Parliament ("EP") on March 13, 2024. The text of the approved version is based on the political agreement that the EP reached with the Council of the European Union in December 2023. Members of the EP passed the law with 523 votes in favor, 46 against, and 49 abstentions. The Act aims to safeguard the use of AI systems within the EU as well as prohibiting certain AI outright.

The AI Act applies to:

- providers placing AI systems or models on the market in the EU or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of whether those providers are located within or outside the EU;
- deployers of AI systems that have their place of establishment in or who are located within the EU;
- providers and deployers of AI systems that have their place of establishment or who are located in a third country in situations where the output produced by the AI system is used in the EU;
- importers and distributors of AI systems into or within the EU;
- product manufacturers who place an AI system on the market or put it into service an AI system within the EU together with their product and under their own name or trademark;
- authorized representatives of AI systems where such providers are not established in the EU; and
- affected persons or citizens located in the EU.

The AI Act is subject to a final linguist check by lawyers, which is expected to take place in April 2024. This is essentially a validation of the language in the final text of the AI Act to ensure that language translations do not lose the legal meaning set out in the original text. It will also need to be formally endorsed by the European Council. As such, it is expected to be finally adopted before the end of the EP's legislature in June 2024.

The AI Act will enter into force 20 days after its publication in the Official Journal. It will be fully applicable 24 months after its entry into force. However, certain provisions will come into force and need to be complied with sooner.

Four (4) Point Summary of European Union Proposed AI

The AI Act classifies AI according to its risk:

- Unacceptable risk is prohibited (e.g. social scoring systems and manipulative AI).
- Most of the text addresses high-risk AI systems, which are regulated.
- A smaller section handles limited risk AI systems, subject to lighter transparency obligations: developers and deployers must ensure that end-users are aware that they are interacting with AI (chatbots and deepfakes).

- Minimal risk is unregulated (including the majority of AI applications currently available on the EU single market, such as AI enabled video games and spam filters – at least in 2021; this is changing with generative AI).

The majority of obligations fall on providers (developers) of high-risk AI systems.

- Those that intend to place on the market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or a third country.
- And also third country providers where the high risk AI system's output is used in the EU.

Users are natural or legal persons that deploy an AI system in a professional capacity, not affected end-users.

- Users (deployers) of high-risk AI systems have some obligations, though less than providers (developers).
- This applies to users located in the EU, and third country users where the AI system's output is used in the EU.

General purpose AI (GPAI):

- All GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training.
- Free and open licence GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk.
- All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections.

AI systems:

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm.
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.
- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.
- social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.
- inferring emotions in workplaces or educational institutions, except for medical or safety reasons.
- 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when:
- searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited;

- preventing substantial and imminent threat to life, or foreseeable terrorist attack; or
- identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).

Governance

How will the AI Act be implemented?

- The AI Office will be established, sitting within the Commission, to monitor the effective implementation and compliance of GPAI model providers.
- Downstream providers can lodge a complaint regarding the upstream providers infringement to the AI Office.

The AI Office may conduct evaluations of the GPAI model to:

- Assess compliance where the information gathered under its powers to request information is insufficient.
- Investigate systemic risks, particularly following a qualified report from the scientific panel of independent experts.

Timelines

See this post for an overview of the full implementation timeline.

After entry into force, the AI Act will apply:

- 6 months for prohibited AI systems.
- 12 months for GPAI.
- 24 months for high risk AI systems under Annex III.
- 36 months for high risk AI systems under Annex II.

Codes of practice must be ready 9 months after entry into force.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021[79]

In year 2021, Government notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Amidst growing concerns around lack of transparency, accountability and rights of users related to digital media and after elaborate consultation with the public and stakeholders, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 has been framed in exercise of powers under section 87 (2) of the Information Technology Act, 2000 and in supersession of the earlier Information Technology (Intermediary Guidelines) Rules 2011.

While finalizing these Rules, both the Ministries of Electronics and Information Technology and Ministry of Information and Broadcasting undertook elaborate consultations among themselves in order to have a harmonious, soft-touch oversight mechanism in relation to social media platform as well as digital media and OTT platforms etc.

Part- II of these Rules shall be administered by Ministry of Electronics and IT, while Part-III relating to Code of Ethics and procedure and safeguards in relation to digital media shall be administered by the Ministry of Information and Broadcasting.

79. Reproduced from Press Information Bureau of India. Available at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1700749

Background:

The Digital India programme has now become a movement which is empowering common Indians with the power of technology. The extensive spread of mobile phones, Internet etc. has also enabled many social media platforms to expand their footprints in India. Common people are also using these platforms in a very significant way. Some portals, which publish analysis about social media platforms and which have not been disputed, have reported the following numbers as user base of major social media platforms in India:

- WhatsApp users: 53 Crore
- YouTube users: 44.8 Crore
- Facebook users: 41 Crore
- Instagram users: 21 Crore
- Twitter users: 1.75 Crore

These social platforms have enabled common Indians to show their creativity, ask questions, be informed and freely share their views, including criticism of the Government and its functionaries. The Government acknowledges and respects the right of every Indian to criticize and disagree as an essential element of democracy. India is the world's largest open Internet society and the Government welcomes social media companies to operate in India, do business and also earn profits. However, they will have to be accountable to the Constitution and laws of India.

Proliferation of social media, on one hand empowers the citizens then on the other hand gives rise to some serious concerns and consequences which have grown manifold in recent years. These concerns have been raised from time to time in various forums including in the Parliament and its committees, judicial orders and in civil society deliberations in different parts of country. Such concerns are also raised all over the world and it is becoming an international issue.

Of late, some very disturbing developments are observed on the social media platforms. Persistent spread of fake news has compelled many media platforms to create fact-check mechanisms. Rampant abuse of social media to share morphed images of women and contents related to revenge porn have often threatened the dignity of women. Misuse of social media for settling corporate rivalries in blatantly unethical manner has become a major concern for businesses. Instances of use of abusive language, defamatory and obscene contents and blatant disrespect to religious sentiments through platforms are growing.

Over the years, the increasing instances of misuse of social media by criminals, anti-national elements have brought new challenges for law enforcement agencies. These include inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, financial frauds, incitement of violence, public order etc.

It was found that currently there is no robust complaint mechanism wherein the ordinary users of social media and OTT platforms can register their complaint and get it redressed within defined timeline. Lack of transparency and absence of robust grievance redressal mechanism have left the users totally dependent on the whims and fancies of social media platforms. Often it has been seen that a user who has spent his time, energy and money in developing a social media profile is left with no remedies in case that profile is restricted or removed by the platform without giving any opportunity to be heard.

Evolution of Social Media and Other Intermediaries:

If we notice the evolution of social media intermediaries, they are no longer limited to playing the role of pure intermediary and often they become publishers. These Rules are a fine blend of liberal touch with gentle self-regulatory framework. It works on the existing laws and statues of the country which are applicable to content whether online or offline. In respect of news and current affairs publishers are expected to follow the journalistic conduct of Press Council of India and the Programme Code under the Cable Television Network Act, which are already applicable to print and TV. Hence, only a level playing field has been proposed.

Rationale and Justification for New Guidelines:

These Rules substantially empower the ordinary users of digital platforms to seek redressal for their grievances and command accountability in case of infringement of their rights. In this direction, the following developments are noteworthy:

- The Supreme Court in suo-moto writ petition (Prajjawala case) vide order dated 11/12/2018 had observed that the Government of India may frame necessary guidelines to eliminate child pornography, rape and gangrape imageries, videos and sites in content hosting platforms and other applications.
- The Supreme Court vide order dated 24/09/2019 had directed the Ministry of Electronics and Information Technology to apprise the timeline in respect of completing the process of notifying the new rules.
- There was a Calling Attention Motion on the misuse of social media and spread of fake news in the Rajya Sabha and the Minister had conveyed to the house on 26/07/2018, the resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law. He had conveyed this after repeated demands from the Members of the Parliament to take corrective measures.
- The Ad-hoc committee of the Rajya Sabha laid its report on 03/02/2020 after studying the alarming issue of pornography on social media and its effect on children and society as a whole and recommended for enabling identification of the first originator of such contents.

Consultations:

The Ministry of Electronics and Information Technology (MEITY) prepared draft Rules and invited public comments on 24/12/2018. MEITY received 171 comments from individuals, civil society, industry association and organizations. 80 counter comments to these comments were also received. These comments were analyzed in detail and an inter-ministerial meeting was also held and accordingly, these Rules have been finalized.

Salient Features

Guidelines Related to Social Media to Be Administered by Ministry of Electronics and IT:

- ***Due Diligence To Be Followed By Intermediaries:*** The Rules prescribe due diligence that must be followed by intermediaries, including social media intermediaries. In case, due diligence is not followed by the intermediary, safe harbour provisions will not apply to them.
- ***Grievance Redressal Mechanism:*** The Rules seek to empower the users by mandating the intermediaries, including social media intermediaries, to establish a grievance redressal mechanism for receiving resolving complaints from the users or victims. Intermediaries shall appoint a Grievance Officer to deal with such complaints andshare the name and contact details of such officer. Grievance Officer shall acknowledge the complaint within twenty four hours and resolve it within fifteen days from its receipt.
- ***Ensuring Online Safety and Dignity of Users, Specially Women Users:*** Intermediaries shall remove or disable access withing 24 hours of receipt of complaints of contents that exposes the private areas of individuals, show such individuals in full or partial nudity or in sexual act or is in the nature of impersonation including morphed images etc. Such a complaint can be filed either by the individual or by any other person on his/her behalf.
- ***Two Categories of Social Media Intermediaries:*** To encourage innovations and enable growth of new social media intermediaries without subjecting smaller platforms to significant compliance requirement, the Rules make a distinction between social media intermediaries and significant social media intermediaries. This distinction is based on the number of users on the social media platform. Government is empowered to notify the threshold of user base that will distinguish between social media intermediaries and significant social media intermediaries. The Rules require the significant social media intermediaries to follow certain additional due diligence.

Additional Due Diligence to Be Followed by Significant Social Media Intermediary:

- Appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and Rules. Such a person should be a resident in India.
- Appoint a Nodal Contact Person for 24x7 coordination with law enforcement agencies. Such a person shall be a resident in India.
- Appoint a Resident Grievance Officer who shall perform the functions mentioned under Grievance Redressal Mechanism. Such a person shall be a resident in India.
- Publish a monthly compliance report mentioning the details of complaints received and action taken on the complaints as well as details of contents removed proactively by the significant social media intermediary.
- Significant social media intermediaries providing services primarily in the nature of messaging shall enable identification of the first originator of the information that is required only for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material punishable with imprisonment for a term of not less than five years. Intermediary shall not be required to disclose the contents of any message or any other information to the first originator.
- Significant social media intermediary shall have a physical contact address in India published on its website or mobile app or both.
- Voluntary User Verification Mechanism: Users who wish to verify their accounts voluntarily shall be provided an appropriate mechanism to verify their accounts and provided with demonstrable and visible mark of verification.
- Giving Users An Opportunity to Be Heard: In cases where significant social media intermediaries removes or disables access to any information on their own accord, then a prior intimation for the same shall be communicated to the user who has shared that information with a notice explaining the grounds and reasons for such action. Users must be provided an adequate and reasonable opportunity to dispute the action taken by the intermediary.
- Removal of Unlawful Information: An intermediary upon receiving actual knowledge in the form of an order by a court or being notified by the Appropriate Govt. or its agencies through authorized officer should not host or publish any information which is prohibited under any law in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries etc.
- The Rules will come in effect from the date of their publication in the gazette, except for the additional due diligence for significant social media intermediaries, which shall come in effect 3 months after publication of these Rules.

Digital Media Ethics Code Relating to Digital Media and OTT Platforms to Be Administered by Ministry of Information and Broadcasting:

There have been widespread concerns about issues relating to digital contents both on digital media and OTT platforms. Civil Society, film makers, political leaders including Chief Minister, trade organizations and associations have all voiced their concerns and highlighted the imperative need for an appropriate institutional mechanism. The Government also received many complaints from civil society and parents requesting interventions. There were many court proceedings in the Supreme Court and High Courts, where courts also urged the Government to take suitable measures.

Since the matter relates to digital platforms, therefore, a conscious decision was taken that issues relating to digital media and OTT and other creative programmes on Internet shall be administered by the Ministry of Information and Broadcasting but the overall architecture shall be under the Information Technology Act, which governs digital platforms.

Consultations:

Ministry of Information and Broadcasting held consultations in Delhi, Mumbai and Chennai over the last one and half years wherein OTT players have been urged to develop "self-regulatory mechanism". The Government also studied the models in other countries including Singapore, Australia, EU and UK and has gathered that most of them either have an institutional mechanism to regulate digital content or are in the process of setting-up one.

The Rules establish a soft-touch self-regulatory architecture and a Code of Ethics and three tier grievance redressal mechanism for news publishers and OTT Platforms and digital media.

Notified under section 87 of Information Technology Act, these Rules empower the Ministry of Information and Broadcasting to implement Part-III of the Rules which prescribe the following:

- Code of Ethics for online news, OTT platforms and digital media: This Code of Ethics prescribe the guidelines to be followed by OTT platforms and online news and digital media entities.
- Self-Classification of Content: The OTT platforms, called as the publishers of online curated content in the rules, would self-classify the content into five age based categories- U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult). Platforms would be required to implement parental locks for content classified as U/A 13+ or higher, and reliable age verification mechanisms for content classified as "A". The publisher of online curated content shall prominently display the classification rating specific to each content or programme together with a content descriptor informing the user about the nature of the content, and advising on viewer description (if applicable) at the beginning of every programme enabling the user to make an informed decision, prior to watching the programme.
- Publishers of news on digital media would be required to observe Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act thereby providing a level playing field between the offline (Print, TV) and digital media.
- A three-level grievance redressal mechanism has been established under the rules with different levels of self-regulation.

  Level-I: Self-regulation by the publishers;

  Level-II: Self-regulation by the self-regulating bodies of the publishers;

  Level-III: Oversight mechanism.
- Self-regulation by the Publisher: Publisher shall appoint a Grievance Redressal Officer based in India who shall be responsible for the redressal of grievances received by it. The officer shall take decision on every grievance received by it within 15 days.
- Self-Regulatory Body: There may be one or more self-regulatory bodies of publishers. Such a body shall be headed by a retired judge of the Supreme Court, a High Court or independent eminent person and have not more than six members. Such a body will have to register with the Ministry of Information and Broadcasting. This body will oversee the adherence by the publisher to the Code of Ethics and address grievances that have not be been resolved by the publisher within 15 days.
- Oversight Mechanism: Ministry of Information and Broadcasting shall formulate an oversight mechanism. It shall publish a charter for self-regulating bodies, including Codes of Practices. It shall establish an Inter-Departmental Committee for hearing grievances.

Other Statutes on Data Protection

Apart from Information Technology Act, 2000 and Information Technology (Amendment) Act, 2008, there are following statutes as well which affords some indirect protection to data and privacy:

1. Indian Penal Code, 1860[80]
2. Indian Telegraph Act, 1885[81]
3. Indian Contract Act, 1872[82]
4. Indian Copyright Act, 1957[83]
5. The Specific Relief Act, 1963[84]
6. The Public Financial Institution Act, 1983[85]
7. The Consumer Protection Act, 1986[86]
8. The Credit Information Companies (Regulation) Act, 2005[87]

CASE STUDY

1. On Cyber Threat

User accounts accessed by attackers due to flaw in "view as" feature: In September 2018, the social media company admitted to a serious vulnerability (which was described as a flaw in Facebook's "view as" feature) that allowed hackers to gain access to accounts and even third-party apps that used Facebook for login to gain unauthorized access to millions of accounts, initially it was stated that 50 million accounts were affected. Access tokens for 30 million accounts were stolen by hackers, who accessed contact information (name and email id/ phone number) for 14 million accounts and additional information was accessed for another 15 million accounts including gender, religion, location and device information. Within a month, the company had disclosed that another 40 million user accounts were deemed at risk from the security flaw before steps were taken to protect them. The company said it reset the access tokens of the 50 million accounts affected by the attack and took a "precautionary step" of resetting tokens for the other 40 million accounts. This raises an alarm of cyber threat on the PIIs of the users.

2. On Cyber Crime

- Zee News in their publication on April 29, 2022 reported that the first two months of 2022 reported more cyber-crimes than the entire 2018, according to data by CERT-In (Indian Computer Emergency Response Team). CERT-In is the nodal agency to deal with cyber security threats and operates under the Ministry of Electronic & Information Technology.

80. The IPC, 1860 does not directly address the breach of data privacy but has been used to bring prosecutions for data theft under Section 405 (criminal breach of trust), 406 (Punishment for criminal breach of trust), 420 (cheating and dishonesty including delivery of property).

81. This Act protects the personal information and privacy of individuals in the telecommunication area.

82. The Indian Contract Act renders data protection and privacy protection in the form of breach of contract and specific performance of contract. The law of contract says that the parties involved in a contract must adhere with the rules and regulations as specified in the agreement. If terms and conditions calling for the protection of information are violated by the disclosure of the information shared between the parties, causing intentional damages to other amounts to breach of contract.

83. This Act provides security to literary, artistic, dramatic and musical work. The copyright act provide right to the original author of above mentioned fields so that no one can misuse their work and maintain the privacy if it is related with some sensitive information and maintain the originality of work. Specifically mention Section 16 and 63B of Indian Copyright Act, 1957.

84. This Act provides for the specific relief to the people, who can claim temporary and permanent injunctions against unauthorized disclosure of confidential information.

85. Kottabomman Transport Corporation Limited vs. State Bank of Travancore and Others, AIR 1992 Ker. 351: Banks are under a duty to secrecy and not to disclose information to third party.

86. This Act provides the provisions through which the consumer can claim protection from exploitation and can save them from deficiency of services by disclosing proprietary information, personal information etc. without adequate authorization.

87. See, Section 19: Information should be accurate and protected against unauthorized use and disclosure.

- Cyber-crime cases have witnessed a steady spike since 2018. India reported 2,08,456 incidents in 2018; 3,94,499 incidents in 2019; 11,58,208 cases in 2020; 14,02,809 cases in 2021; and 2,12,485 incidents in the first two months of 2022. The above figures show that cyber-crimes increased almost seven times in three years between 2018 and 2021, and more sharply during the pandemic.
- A total of 17,560; 24,768 and 26,121 Indian websites were hacked in 2018, 2019 and 2020 respectively, CERT-In data further says.
- The National Crime Records Bureau (NCRB), however, presents a different set of data. According to NCRB, India reported 50,035 cyber-crimes in 2020; 44,546 cases in 2019 and 27,248 cases in 2018.
- The year 2020 saw 4,047 cases of online banking fraud; 2,160 cases of ATM fraud; 1,194 credit/debit card fraud and 1,093 OTP frauds. As per NCRB data, there were 972 cases of cyber stalking/bullying of women and children and 578 cases of fake news on social media.
- Committing fraud was found to be the biggest motive and accounted for 30,142 out of the total 50,035 cases (60.02 per cent). This was followed by sexual exploitation (6.6 per cent) and extortion 4.9 per cent.
- Cyber-crime rate was highest in Karnataka (16.2 per cent), followed by Telangana (13.4 per cent) and Assam (10.1 per cent).

LESSON ROUND-UP

- Advent of information technology has not only provided us the assorted means of communicating our information at an inclusive platform but it has also ensured quick communication of information.
- However, it has been righty said that 'with boon goes the bane', so is the sphere of information technology. At one side, this easy medium of transferring data and quicker communication has given birth to numerous recompenses of communication and transaction; on the other side, various dark sides are being observed under IT enables and electronic transactions. The major among them are Cyber Crimes and Cyber Attacks.
- Hence in order to control the mechanism of cyber-crimes and cyber-attacks, cyber law has been evolved gradually which ensures cyber security in cyber sphere.
- Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems.
- A cyber threat (also known as cybersecurity threat) is defined as a malicious act that seeks to steal or damage data or disrupt the digital wellbeing and stability in general.
- Cyber threats may come from a variety of places, people, and contexts.
- Cyberwar (also called cyberwarfare or cyber warfare) is defined as a war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states.
- Cyber-crime is any criminal activity that involves a computer, networked device or a network. In general, most cybercrimes are carried out in order to generate profit for the cybercriminals, yet some of cybercrimes are carried out against computers or devices directly to damage or disable them.

- Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels.
- The term cyberterrorism was first coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. But its usage was better understood during the 9/11 attack.
- A cyber or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.
- Cyber threat hunting is a proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools.
- A cyber threat hunt is composed of steps or processes designed for an efficient, successful hunt.
- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
- The term digital forensics was first used as a synonym for computer forensics.
- Indeed internet has revolutionized the way we interact; however, it has also bought with it a host of problems such as hate speech, fake news, illegal lobbying and personal data theft. The number of these issues not only make the criminal/offender liable, yet many a times, online platforms are also made liable for the cyber security threat.
- To encounter the challenges of information privacy and to promote legal control over privacy protection in electronic transactions, some legal policies and regulations have already been established at international and national level.
- At international level, some fair information principles like Notice, Choice, Access, Consent, Enforcement etc. are directed to be followed by the e-commerce companies to ensure the information privacy in the conduct of online transactions.
- Though at the industry level, even the e-commerce companies are also taking some steps to protect the information privacy of the individuals by adopting and declaring privacy policy, yet much is left to be governed by the nationally and internationally commended regulations.
- At national level, countries around the world have enacted different laws to protect privacy of individuals.
- With digital transformation at its high in India, March 2023 has witnessed a magnificent move with the official announcement of enacting Digital India Act (DIA) while replacing a 24-year-old Information Technology Act of 2000 (IT Act).
- This proactive move by the Ministry of Electronics and Information Technology (MeitY) aligns with India's ambitious "Digital India" initiative.
- The proposed Digital India Act (DIA) *inter-alia* with an aim to provide a *future ready legislation* opts "*principles and rule-based approach*" for regulating digital transactions including the evolving era of Artificial Intelligence and Machine Learning.
- One shall always remember one of powerful legal maxim "*Ignorantia Juris Non Excusat*", which means ignorance of law is not an excuse.
- Hence, one should stay prepared before the proposed DIA is notified. It is to be noted that separate rules will govern different kinds of industry. Hence ***Industry Specific Compliance Calendars*** will be required.

- The intention behind the DIA is laudable and this legislation will be revamping India's technology sector regulations.
- It is for the first time that consultations are taking place during the pre-draft stage of the bill. Policymakers are aware of the challenges that might arise therefore the opinions of important stakeholders are being valued.
- The need for comprehensive and relevant legislation was much needed for the evolving technology sector in India.
- The three new criminal laws that were passed by Parliament in 2023 will come into effect from July 1, 2024, according to a notification by the Ministry of Home Affairs
- For all three new criminal laws, efforts are being made to take these issues forward with the help of technology.
- This will also help us in increasing the conviction rate. Along with this, efforts are also being made to modernize the entire process.
- Initially introduced in 2019, the Digital Personal Data Protection Act holds considerable importance as a legislative measure aimed at safeguarding individuals' privacy rights.
- Its primary focus lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. The DPDP Bill underwent 81 amendments after its initial introduction, resulting in a comprehensive overhaul to its present form.
- By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the challenges posed by data handling in the digital age.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What do you mean by Cyber Threats? Discuss four recent types of Cyber Threats encountered in covid times.
2. What is Cyber Threat Hunting? Describe few techniques of Cyber Hunting.
3. Write a brief note on Digital Intellectual Property along with ways to protect the same.
4. Discuss Artificial Intelligence (AI). Briefly describe the development of AI in India.
5. Write Short Note on any Four of the following:
    a. Cyber Warfare
    b. Cyber Terrorism
    c. Digital Forensics
    d. Safe Harbour Protection
    e. Cyber Security Framework (NCFS)
6. Briefly discuss the need and proposed structure of proposed Digital India Act
7. Write a short note on Digital Personal Data Protection Act, 2023 and also analyze its significance in the perspective of protecting data privacy of personal information.

LIST OF FURTHER READINGS

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

- Chattopaddhyay Sougata (2020) Intellectual Property Rights in Digital Environment, ePrints in Library and Information Science
- Erdal Ozkaya (2022) Practical Cyber Threat Intelligence: Gather, Process, and Analyze Threat Actor Motives, Targets, and Attacks with Cyber Intelligence Practices Paperback – Import, 27 June 2022, BPB Publications
- European Union on Liability of online platform (2021), Study Published by Scientific Foresight Unit (STOA) European Parliamentary Research Service, EU. Available on https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf
- Malik Surendra and Malik Sudeep (2019) Supreme Court on Information Technology Act, Internet and Cyber Laws and Aadhar, Eastern Book Company
- Pokhariyal Purvi, Kashyap Amit and Arun Prasad (2022) Artificial Intelligence: Law and Policy Implications, Eastern Book Company, ISBN: 9789389656954, 9789394364806
- Raman and Sharma (2019) Cyber Terrorism in India: A Physical Reality Or Virtual Myth, Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019
- Singh and Mara (2021) Intermediary Liability in India – Moving Goalposts, Mondaq
- What is Digital Forensics and Incident Response (DFIR), SentinelOne
- Proposed Digital India Act. Proposal By MEITY. Report available at https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf