INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 2 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 2 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-2-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ARTIFICIAL INTELLIGENCE (AI) AND CYBERCRIMES

AUTHOR - RAKESH MISHRA, PHD (LAW) – SCHOLAR AT INVERTIS UNIVERSITY, BAREILLY (U.P)

BEST CITATION - RAKESH MISHRA, ARTIFICIAL INTELLIGENCE (AI) AND CYBERCRIMES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 4 (2) OF 2024, PG. 145-163, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

AI is "Artificial Intelligence" that is Intelligence which is artificial in nature; where Intelligence is the ability to understand, learn, think and in some way or the other take decisions. On the other hand, Cybercrimes are crimes that include computer and/or computer networks. With the exponential rise in the technological development the criminals are no more traditional in the manner they commit crimes. Gone are the days when people used paper files / folders to save their valuable documents and locked them in the almirah or bank lockers. Neither, people now prefer to maintain some cash in hand to meet some unexpected exigencies. With the advent of computers, digital files/folders are better preferred to be saved in digital lockers and people feel quite save with it. Even almost all banking transactions are preferred to be done online because of the lucrative ease of use which even saves time, physical hassle and also symbolises a high status.

However, in reality now we are more vulnerable to threat of digital theft and robbery because of the Artificial Intelligence and its bye-products like virus, spyware, spam, Impersonation attacks, deepfake, rapid malware generation, automated spear phishing, enhanced Botnets etc, which are increasing exponentially each day are posing great threat to the social, financial, administrative and many more aspects of governments throughout the world.

This paper intends to highlight the future of cybercrime, which is based upon the emerging technologies and Artificial Intelligence. This paper also intends to study the various means the Governments around the world are opting to tackle with the problems of Cybercrime with special reference to the Government of India while critically examining the existing laws and their effectiveness and trying to find out the legal solutions to tackle with the problem of "Bad AI" using means of "Good AI" in compliance with the existing laws in India without infringement of the Fundamental Rights bestowed upon the citizens by the Constitution of India.

INTRODUCTION

HISTORY

In ancient times, inventors made things called "automatons" which were mechanical and moved independently of human intervention. The word "automaton" comes from ancient Greek, and means "acting of one's own will." One of the earliest records of an automaton comes from 400 BCE and refers to a mechanical pigeon created by a friend of the philosopher Plato.

Dates of note:

1921: Czech playwright Karel Čapek released a science fiction play "Rossum's Universal Robots" which introduced the idea of "artificial people" which he named robots. **This was the first known use of the word.**

1949: Computer scientist Edmund Callis Berkley published the book "Giant Brains, or Machines that Think" which compared the newer models of computers to human brains.

1950: Alan Turing published "Computer Machinery and Intelligence" which proposed a test of machine intelligence called The Imitation Game.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1955: John McCarthy held a workshop at Dartmouth on "artificial intelligence" which is the first use of the word, and how it came into popular usage.

1956: The field of AI research was founded at a workshop held on the campus of Dartmouth College, USA during the summer of 1956. Those who attended would become the leaders of AI research for decades.

1958: John McCarthy created LISP (acronym for List Processing), the first programming language for AI research, which is still in popular use to this day.

1961: The **first industrial robot Unimate** started working on an assembly line at General Motors in New Jersey, tasked with transporting die casings and welding parts on cars (which was deemed too dangerous for humans).

1968: Soviet mathematician Alexey Ivakhnenko published "Group Method of Data Handling" in the journal "Avtomatika," which proposed a new approach to AI that would later become what we now know as "Deep Learning."

1979: The American Association of Artificial Intelligence which is now known as the Association for the Advancement of Artificial Intelligence (AAAI) was founded.

1980: First conference of the AAAI was held at Stanford.

1984: The AAAI warns of an incoming "AI Winter" where funding and interest would decrease, and make research significantly more difficult.

1997: Windows released a speech recognition software (developed by Dragon Systems).

2002: The first Roomba was released.

2006: Companies such as Twitter, Facebook, and Netflix started utilizing AI as a part of their advertising and user experience (UX) algorithms.

2011: Apple released Siri, the first popular virtual assistant.

2016: Hanson Robotics created a humanoid robot named Sophia, who became known as the first "robot citizen" and was the first robot created with a realistic human appearance and the ability to see and replicate emotions, as well as to communicate.

2017: Facebook programmed two AI chatbots to converse and learn how to negotiate, but as they went back and forth, they ended up forgoing English and developing their own language, completely autonomously.

2018: A Chinese tech group called Alibaba's language-processing AI beat human intellect on a Stanford reading and comprehension test.

2021: OpenAI developed DALL-E, which can process and understand images enough to produce accurate captions, moving AI one step closer to understanding the visual world.

AI AND CYBERCRIMES

AI that is Artificial Intelligence, broadly refers to a machine's ability to combine computers, datasets and sets of instructions to perform tasks that usually require human intelligence, such as reasoning, learning, decision-making and problem-solving.

Cybercrimes may, in general, be defined as those criminal activities using computers, computer networks and other set of digital devices.

TYPES OF AI[271]

There are two types of AI. The first one is Narrow AI (weak AI), which is designed and trained for a specific task. It excels in performing a particular function, but lacks the broad cognitive abilities of human intelligence. Examples include virtual personal assistants, image recognition systems, and speech recognition software. The second type is General AI or Strong AI.

This hypothetical form of AI would possess the ability to understand, learn, and apply knowledge across a broad range of tasks, similar to human intelligence. Achieving General

[271] Bhushan, Tripti (2024) "Artificial Intelligence, Cyberspace and International Law," Indonesian Journal of International Law: Vol. 21: No. 2, Article 3. Available at: https://scholarhub.ui.ac.id/ijil/vol21/iss2/3

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

AI is a long-term goal and remains an area of active research.

TYPES OF CYBERCRIMES

Cybercrimes are accomplished through cyber-attacks which is an offensive, unauthorized system or network access by a third party known as a Hacker who aims at destroying or stealing confidential information from a computer network, information system, or personal device: by disabling, destroying or by remotely controlling the computer systems.

Broadly speaking, there are two types of cybercrimes. One without the use of Artificial Intelligence and the other with the use of Artificial intelligence.

Cybercrimes without use of Artificial Intelligence –

Malware attack: - "Malware" is a malicious software virus including worms, spyware (a software that steals personal and/or confidential information without one's knowledge), ransomware (a software that blocks access to the network's key components), adware (a software that displays advertising contents on the user's screen), and trojans (a software that disguises itself as a legitimate software).

Phishing Attack: - Here an attacker impersonates to be a trusted contact and sends fake mails to the victim. Upon opening such mails and clicking to the malicious links or opening the mail's attachment by the user (victim), the attacker gains access to the confidential information of the user along with the account credentials. Sometimes, malware is also installed through such phishing attacks.

Password attack: - This is cracking of the password of victims computer through various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat etc. Different types of password attacks are brute force attacks, dictionary attacks, and keylogger attacks.

Man-in-the-Middle (MITM) attack: - Also known as an eavesdropping attack is an attack where an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host and steal and manipulate data.

SQL Injection attack: - This occurs on a database-driven website when the attacker/ hacker manipulates a standard SQL query by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information. The attacker is thus able to get Administrator rights to view, edit, and delete tables in the databases.

Denial-of-Service attack: - Attackers target systems, servers, or networks by flooding them with traffic to exhaust their resources and bandwidth resulting that the website that the server hosts either slows down or shuts down. It is also known as a DdoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

Insider Threat: - As the name suggests, this threat does not involve a third party but an insider who may be an individual from within the organization who knows everything about the organization, thus causing tremendous damages.

Cryptojacking: - Closely related to cryptocurrency occurs when attackers access someone else's computer for mining cryptocurrency by gaining access by infecting a website or manipulating the victim to click on a malicious link.

They also use adware with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

Watering Hole attack: - Here, the victim is not an individual but a particular group of an organization, region, etc. The attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Then such websites are infected with malwares to gain personal information by remote access to the infected computer.

Spoofing: - Impersonation of someone or something trustworthy to access sensitive information and do malicious activities is called spoofing. It is basically, getting into one's computer or computer network, by pretending to have identity of another computer who has trusted access to the secured information of the victim's computer of network.

Identity – Based attacks: - Logging in by someone's PINs to steal unauthorized access to their systems.

Code Injection attacks: - This is done by inserting malicious code into a software application to manipulate data.

DNS Tunnelling attacks: - Here the attacker uses the Domain Name System (DNS) to bypass security measures and communicate with a remote server. When the attacker manipulates the DNS records from a website to control its traffic, its called DNS spoofing.

Corporate Account Takeover (CATO): - Use of stolen login credentials to access others' bank accounts by the attackers

Whale-Phishing attacks: - Target to high-profile individuals like executives or celebrities using sophisticated social engineering techniques to get sensitive information.

Spear-Phishing attacks: - Target to specific individuals or groups under an organization using social engineering techniques to get sensitive information.

Session Hijacking: - Here the hacker gains access to a user's session ID to authenticate the user's session with a web application and takes the control of user's session.

Brute Force attack: - This works effective against weak passwords. The attacker uses trial-n-hit method to crack the password and then gains access to the targeted system.

Web attacks: - Here the attacker targets websites by inserting SQL injection, cross-site scripting (XSS) and file inclusion.

Drive-by attacks: - Here the attacker floods the user's system with malware by luring him to visit its compromised website and later exploits the weaknesses in other software in the user's system to insert the malware without the user's knowledge.

Cross-Site Scripting (XSS) attacks: - Unauthorized code is inserted into legitimate website to access the victim's information.

Eavesdropping attacks: - The attacker intercepts between two communicating parties to gain unauthorised private information.

Birthday attack: - This is a cryptographic attack that exploits the birthday paradox to access a collision in a hash function. The attacker successfully generates two inputs to get the same output hash value.

Rootkits: - Rootkits can be used to hide other types of malware, such as spyware or keyloggers, and can be challenging to detect and remove.

Cybercrimes with use of Artificial Intelligence –

Deepfake – Deepfake is in fact "deep learning" plus "fake media" which refers to the use of AI to create fake images, fake videos and/or fake audio that are difficult to distinguish from the real one. Deepfake is used by attackers to impersonate someone in a phishing attack and/or to gather information or trick people causing financial, emotional, and social harm. For example, use of deepfake to generate non-consensual pornography of celebrities or spread political misinformation and many more.

AI-Powered Password Cracking – This is use of AI with machine learning (ML) to improve algorithms for guessing user passwords. Large password datasets are analysed and thereby different password combinations are automatically generated.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

AI-Phishing attacks – AI enabled phishing attacks are very difficult to detect. Using AI cloning and customisation of any website can be done in seconds in such a manner that it looks identical to the original website. This gives an impression to the server of authentic access and thus allowing access to the internal resources.

Spear Phishing Attacks with the use of ChatGPT is becoming increasingly popular where a cybercriminal writes an email with perfect grammar and language usage as per the region/country of the target victim, styled in the language of a legitimate source and sends out automated communications mimicking someone/some authority trustworthy. When a user clicks a link to start furnishing information, the hacker takes control of the account.

AI-Impersonation – AI impersonation has become increasingly common when cybercriminals are carrying out vishing scams. Vishing is a type of phishing scam that occurs through a phone call. In a vishing attack, the cybercriminals call their target (victim) and pretends be someone whom the victim knows more likely a family member or a friend or a colleague. Since, large amounts of data can be analysed by AI, a fake persona (voice, in this case) can be generated from it using a process called synthesis. The victim's voice is first analysed from a sufficient amount of audio and video recordings and then through speech synthesis, the voice of the victim is generated that sounds exactly like the victim's. recently, several extortion cases have popped up, where the cyber-criminal uses this technique for deception to extort parents whose child is out of home.

Denial-of-Service attacks – Using AI, the attacker launches more sophisticated and powerful distributed denial of service in which multiple systems are used to flood the target system with traffic, thus slowing down or shutting down of the target system.

AI-Powered Ransomware – Ransomware aims at blackmailing organisations to pay money by making their data and related systems unavailable through encryption or by threatening to leak sensitive data to the public. AI is used to combine simultaneous ransomware attacks. Individuals or even organisations may be targeted for such attacks. Email addresses may be tracked and simultaneously highly personalised dynamic emails may be designed to bypass the counter-measures and gain access to the system by instant diagnosis of the weaknesses of the system to escalate the attack.

Advanced Persistent Threats (APTs) – Here the attacker is present in a system network for a long time and gradually snips confidential information.

Data Processing Giant – The cybercriminals use machine learning algorithms (MLA) and analyse large data to detect patterns that cannot be done by humans. AI algorithms enable computerized defencelessness by scanning and weakness detection of intelligent systems and adaptive malware development, etc. Through this, cybercrimes like Payment gateway fraud, Intellectual property theft etc is done.

Cyber Terrorism – Terrorism through cyberattacks is called cyber terrorism. Individuals or groups use cyber-attacks to cause fear, disrupt systems, or harm individuals or organizations. Such Cyberterrorists are often motivated by political or social causes.

Enhanced Botnets – A network of hijacked computer devices is called botnet. This is the infiltration stage of a multi-layered system and serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution. Botnets automate, and speed up a hacker's ability to carry out larger attacks. The term "botnet" is formed by the words "robot" and "network." Botnets use the devices of other person to scam or cause disruption to some other person without the knowledge or consent of the former person. A bot herder leads a collective of hijacked devices with remote commands. Zombie computers, or bots, refer to

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

each malware-infected user device that's been taken over for use in the botnet. These devices operate mindlessly under commands designed by the bot herder.

RECENT CYBERCRIMES

- **International**[272]

The Guardian Cyber Attack:

On 20 December 2022, The Guardian newspaper in UK was the subject of a ransomware attack. This caused the company to ask its staff to work remotely while internal systems were disconnected and triaged.

In this case, the organisation employed to investigate, KnowBe4, has identified that email phishing was the initial attack vector.

Toronto SickKids:

On 20 December 2022, the Hospital for Sick Children (SickKids) in Toronto announced a 'code grey', which meant that it had experienced one or more system failures.

This attack is unique because the provider of the ransomware-as-a-service infrastructure, the LockBit Group, has publicly apologised for the attack. LockBit has also provided unlock codes for the scrambled data.

FAA incident:

The US grounded all flights following issues with a critical system operated by the Federal Aviation Administration (FAA) on 11 January 2023. Such was the level of disruption to air travel across the US that Transportation Secretary Pete Buttigieg was forced to consider the possibility that it was a result of a cyber-attack.

Royal Mail ransomware attack:

It began in November 2022 when the Emotet malware was detected on Royal Mail servers. Then in early January 2023, Royal Mail was subject to a ransomware attack by an affiliate using LockBit Ransomware-as-a-Service (RaaS). This attack affected a distribution centre near Belfast, Northern Ireland, where the printers began printing the ransomware gang's demands.

Hive ransomware gang infiltrated and shutdown (for now):

The FBI proudly announced that it had won against the gang using the Hive ransomware. This was a successful international effort (as all these investigations must be) involving authorities from Germany, the Netherlands, UK's NCA, Europol and likely others, alongside the FBI. The Hive ransomware has been around since 2021 and is offered as ransomware-as-a-service (RaaS). Those leasing the RaaS, called affiliates, used the standard double-extortion method of encrypting the data locally. They also exfiltrated it so they could threaten to publish and demand money for decryption.

MOVEit:

The MOVEit software, marketed by Progress Software Corporation, was exploited in this way. The Cl0p Russia-linked ransomware group (also known as TA505) claimed responsibility.

The American Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on June 7th, in which it they describe how the Cl0p group exploited 'CVE-2023-34362', a previously known SQL injection vulnerability. This meant that internet-facing MOVEit Transfer web applications were infected with a web shell named LEMURLOOT, which was then used to steal data from underlying MOVEit Transfer databases.

Microsoft Storm-0558:

Microsoft has described how Storm-0558, a Chinese hacking group, obtained a Microsoft account (MSA) consumer key which enabled it to forge tokens that allowed them to access OWA and Outlook.com accounts from around 25 organisations.

The UK Electoral Commission:

On the 8th August 2023 the UK Electoral Commission issued a public notification that its database had been breached and the personal

[272] https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2023/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

data of approximately 40 million people exposed. The incident was identified in October 2022.

The Commission first described the attack as 'a complex cyber-attack'. Security researchers uncovered an unpatched Microsoft Exchange Server, vulnerable to the ProxyNotShell attack at the time of the intrusion.

DarkBeam:

In mid-September-2023, a security hole was noticed at DarkBeam, a cyber risk protection company. The issue was first spotted by Bob Diahechenko, CEO of SecurityDiscovery, who believes that more than 3.8 billion records were exposed.

- **INDIA**[273]

Cyber Attack on Cosmos Bank:

A daring cyber-attack was carried in August 2018 on Cosmos Bank's Pune branch which saw nearly 94 Crores rupees being siphoned off. The switching system which acts as an interacting module between the payment gateways and the bank's centralized banking solution was attacked.

The Malware attack on the switching system raised numerous wrong messages confirming various demands of payment of visa and rupee debit card internationally.

This was the first malware attack in India.

ATM System Hacked in Kolkata:

In July 2018 fraudsters hacked into Canara bank ATM servers and wiped off almost 20 lakh rupees from different bank accounts. The hackers used skimming devices on ATMs to steal the information of debit cardholders.

Websites Hacked:

Over 22,000 websites were hacked between the months of April 2017 and January 2018. As per the information presented by the Indian Computer Emergency Response Team. The attacks were intended to gather information about the services and details of the users in their network.

Phishing Attack on Wipro:

There were reports about an attack on the Wipro system by major online news portals. Attack as per reported was a phishing attack and was done by a group through gift card fraud.

Bib B Amitabh Bachchan 's Twitter Account Hacked:

Amitabh Bachchan's Twitter handle got hacked and the perpetrators posted hateful messages putting everybody in shock.

Personal Data Exposed from JustDial Database:

An unprotected API end was the issue in this incident. Justdial one of India's leading local search platforms let a loose end that exposed all of their user data who accessed their services through the web, mobile, and their phone number.

Cyberattack on Union Bank of India: Another shocking cyberattack that made everyone alert was done in July 2017. The attack was on one of India's biggest banks; the Union Bank of India. The attack was initiated when an employee opened an email attachment. This email attachment had a malware code. It allowed the hackers to get inside the bank's system and steal the bank's data.

The email attachment forged a central bank email. The employee overlooked the details and trusted the email, which initiated a malware attack and allowed the hackers to get inside the bank's data and steal Union Bank's access codes for the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is used for international transactions. The hacker used these codes and transferred $170 million to a Union Bank account at Citigroup Inc in New York.

Malware attack on Kudankulam Nuclear Power Plant (KKNPP): Authorities on October 20, 2019, confirmed that the nuclear power station in Kudankulam faced

[273] https://www.testbytes.net/blog/cyber-attacks-on-india/

a cyber attack. The attack was initiated by the North Korean hacker group- Lazarus. This attack was done to get information on thorium-based reactors, an alternative to uranium.

They used a malware named 'Dtrack' to get inside the company's system through a couple of loopholes that persisted in their security systems.

Indian journalists, activists spied on by Israeli spyware Pegasus:
2019 saw another big cyber-attack when Israeli spyware Pegasus was used to spy on academicians, lawyers, activists, and journalists in India.
WhatsApp confirmed that NSO Group used Israeli spyware, called Pegasus to get access to the passwords, text messages on messaging apps like WhatsApp. Pegasus took advantage of loopholes in the servers. Pegasus allowed to hack and get access to everything on the phones of the user (victims) remotely.

Facebook database leak data of 419 million users:
Another very prominent attack was on Facebook and Twitter user data. The personal information of around 419 million users was broken to third parties. The Insecure database allowed the hackers to access the phone numbers, user's name, gender, and location of around 419 million users that were linked to their Facebook accounts.

Cyber-attack on Air India:
One of the biggest cyber-attacks India has seen in 2021 is on India's biggest airline Air India. The Security of Indian Airlines data was compromised when the confidential information of its passengers like ticket information, passport details, and credit card information of more than 4.5 million customers was stolen by the hackers.
LinkedIn Phishing Scam:
Another big attack of 2021 was a phishing scam attack on the social networking site LinkedIn. The company was perturbed when the data of 500 million LinkedIn users were under a security breach. The data of these account holders were sold online. The attackers had sent these users fake job offering mail which forced them to click the link and instilling malicious software on their systems.

Attacks on India's CoWIN app:
Amidst the pandemic, CoWIN app emerged as a ray of light for the people of India, by helping them and streamlining the complete vaccination process of the huge country. Hackers used the CoWin app to misguided users into downloading fake apps. In January many incidents came up in light of fake Aarogya Setu apps created by hackers. It was used to implant malware into end user's systems. The fake CoWIN app lured many users to download this fake app in an urge to get vaccinated.

INTERNATIONAL LAWS ON AI & CYBERCRIMES

The regulation of artificial intelligence is the development of public sector policies and laws for promoting and regulating artificial intelligence (AI); it is therefore related to the broader regulation of algorithms.[274] [275] [276] [277] [278]

A. DEVELOPMENT

According to AI Index at Stanford, the annual number of AI-related laws passed in the 127 survey countries jumped from 1 passed in 2016 to 37 passed in 2022 alone.[279] [280]

In 2017, Elon Musk called for regulation of AI development.[281]

[274] Nemitz, Paul (2018)."Constitutional democracy and technology in the age of artificial intelligence" (https://doi.org/10.1098%2Frsta.2018.0089).
[275] Cath, Corinne (2018).
"Governing artificial intelligence: ethical, legal and technical opportunities and challenges" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6191666).
[276] Buiten, Miriam C. (2019). "Towards Intelligent Regulation of Artificial Intelligence"
[277] Erdélyi, Olivia J.; Goldsmith, Judy (2020).
"Regulating Artificial Intelligence: Proposal for a Global Solution". arXiv:2005.11072 (https://arxiv.org/abs/2005.11072)
[278] Ebers, Martin (2020). "Regulating AI and Robotics: Ethical and Legal Challenges".
[279] Vincent, James (3 April 2023). "AI is entering an era of corporate control". The Verge. Retrieved 19 June 2023. (https://www.theverge.com/23667752/ai-progress-2023-report-stanford-corporate-control)
[280] "Artificial Intelligence Index Report 2023/Chapter 6: Policy and Governance" (PDF). AI Index. 2023.Retrieved 19 June 2023. (https://aiindex.stanford.edu/ wp-content/uploads/2023/04/HAI_AI-Index-Report-2023_CHAPTER_6-1.pdf
[281] "Elon Musk Warns Governors: Artificial Intelligence Poses 'Existential Risk'" . NPR.org. Retrieved 27 November 2017. (https://www.npr.org/section s/thetwo-way/2017/07/17/537686649/elon-musk-warns-governors-artificial-intelligence-poses-existential-risk)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

2017 – The development of a global governance board to regulate AI development.

2018 – Canada and France announced plans for a G7-backed International Panel on Artificial Intelligence, modelled on the International Panel on Climate Change, to study the global effects of Aion people and economies and to steer AI development[282].

2019 – The Panel was renamed the Global Partnership on AI[283].

2020 – The Global Partnership on Artificial Intelligence (GPAI) was launched in June, stating a need for AI to be developed in accordance with human rights and democratic values, to ensure public confidence and trust in the technology, as outlined in the OECD Principles on Artificial Intelligence (2019)[284].

2020 – In February the European Union published its draft strategy paper for promoting and regulating AI[285]. At the United Nations (UN), several entities have begun to promote and discuss aspects of AI regulation and policy, including the UNICRI Centre for AI and Robotics[286]. In partnership with INTERPOL, UNICRI's Centre issued the report AI and Robotics for Law Enforcement in April 2019[287] and the follow-up report Towards Responsible AI Innovation in May[288].

- **THE BUDAPEST CONVENTION, 2001**

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations[289].

Objectives of Budapest Convention

This convention was the first International Convention on cybercrimes that basically dealt with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security[290].

The principal objectives of Convention were:

- Agreeing for a common substantive law related to cyber-crimes.
- Providing for domestic criminal procedural law powers necessary to deal with cases of cyber-crimes.
- Setting up an effective rule of international cooperation in cases related to cyber-crimes.

- **Legislative framework against cybercrime In Israel**

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

- The Computer Law, 1995[291]: This Law forbids the illegal access to computer material (Article 4), data and system interference (Article 2) and the misuse of devices (Article 6) alongside other offences.
- The Privacy Protection Regulations (Data Security), 2017 (based on the 1981 Privacy Protection Law)[292]: The regulations apply to both the private and public sectors, and they

[282] Innovation, Science and Economic Development Canada (2019-05-16). "Declaration of the International Panel on Artificial Intelligence". Gcnws. Retrieved2020-03-9 (https://www.canada.ca/en/innovation-science-economic-development/new s/2019/05/declaration-of-the-international-panel-on-artificial-intelligence.html).

[283] Simonite, Tom (2020-01-08). "The world has a plan to rein in AI—but the US doesn't like it". Wired. Retrieved 2020-03-29. (https://www.wired.com/story/world-plan-rein-ai-us-doesnt-like/)

[284] UNESCO Science Report: the Race Against Time for Smarter Development. Paris: UNESCO. 11 June 2021. ISBN 978-92-3-100450-6. (https://unesdoc.unesco.org/ark:/48223/pf0000377433/PDF/377433eng.pdf.multi)

[285] White Paper: On Artificial Intelligence – A European approach to excellence and trust (PDF). Brussels: European Commission. 2020. P. 1. https://commission.153uropa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[286] Babuta, Alexander; Oswald, Marion; Janjeva, Ardi (2020). Artificial Intelligence and UK National Security:Policy Considerations (PDF). https://web.archive.org/web/20200502044604/https://rusi.org/sites/default/files/ai_ national_security_final_web_version.pdf

[287] "High-Level Event: Artificial Intelligence and Robotics – Reshaping the Future of Crime, Terrorism and Security" . UNICRI. Retrieved2022-07-18. (https://unicri.it/news/article/AI_Robotics_Crime_Terrorism_Security)

[288] "Towards Responsible Artificial Intelligence Innovation". UNICRI. July 2020. Retrieved 2022-07-18. https://unicri.it/towards-responsible-artificial-intelli gence-innovation

[289] Convention on Cybercrime, Budapest, 23 November 2001

[290] Arias, Martha L., "The European Union Criminalizes Acts of Racism and Xenophobia Committed through Computer Systems Archived 2011-07-22 at the Wayback Machine", April 20, 2011.

[291]https://www.coe.int/en/web/octopus/countrywiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/israel

[292] https://www.gov.il/en/Departments/General/data_security

provide organizational procedures to ensure that data security is integrated into the management processes of all businesses that process personal data.

- The Copyright Law, 2007 – Amendment 5 (2019) on the procedure for the disclosure of the identity of internet users under certain circumstances[293].

- **Legislative framework against cybercrime in USA[294]**

Computer fraud and abuse are prohibited under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030: It's a piece of cyber-security legislation. It safeguards federal computers, bank computers, and Internet-connected systems. It protects them from trespassing, threats, vandalism, spying, and being exploited as fraud instruments by the corrupt.

Major Provisions:

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

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

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

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

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

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

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

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

- **The Homeland Security Act of 2002**

Established a framework that allows individuals of the private sector and others to voluntarily submit sensitive information.[295].

Health Insurance Portability and Accountability Act of 1996 (HIPAA)[296]:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that mandated the adoption of national standards to prevent sensitive patient health information from being revealed without the consent or knowledge of the patient.

Gramm-Leach-Bliley Act[297]:

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

FISMA[298]:

FISMA 2002 mandates that each federal agency creates, document, and implement an agency-wide information security program for all information and systems that support the agency's operations and assets, including those

293 https://www.loc.gov/item/global-legalmonitor/2007-12-02/israel-new-copyright-law
294 https://www.everycrsreport.com/reports
295 https://itlaw.fandom.com/wiki/Critical_Infrastructure_Information_Act_of_2002
296 https://www.cdc.gov/phlp/publications/topic/hipaa.html
297 https://www.ftc.gov/tips-advice/businesscenter/privacy-and-security/gramm-leachbliley-act
298 https://csrc.nist.gov/projects/riskmanagement/fisma-background

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

provided or maintained by another agency, contractor, or other sources.

The Federal Information Security Modernization Act of 2014: These improvements result in less overall reporting, a stronger use of continuous monitoring in systems, a greater focus on agencies for compliance, and reporting that is more focused on security incident issues.

- **Legislative framework against cybercrime in UK**[299]

There are four critical legislation schemes that govern cybersecurity, data privacy, and data protection in the UK:

DPA (Data Protection Act 2018):

The DPA 2018 requires all UK data controllers (companies and organizations that control the processing of personal data) to implement and maintain proper security measures for safeguarding personal data. Both the UK-GDPR and the DPA 2018 work together in conjunction to regulate data protection and data privacy in the UK.

Cyber offenses covered by the DPA 2018 include the destruction, falsifying, unlawful use, or unlawful obtainment of personal data, as well as altering information to prevent disclosure to the data subject.

UK-GDPR (UK General Data Protection Regulation):

The UK-GDPR regulation applies to every country in the United Kingdom (England, Scotland, Wales, and Northern Ireland), and it mandates businesses to protect all personal data by only allowing third-party entities access to the personal data that are "subject to sufficient guarantees involving the security of the processing services."

The UK-GDPR recognizes seven main principles of how organizations process personal data:

Lawfulness, fairness, and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability.

NIS Regulations (Network and Information Security Regulations 2018):

The primary mandate of the NIS Regulations is to "detect and manage the threats to the security of network and information systems in an acceptable and proportional manner."

The regulations offer legal measures and impose cybersecurity obligations for:

Relevant digital service providers (RDSPs — cloud computing service providers and online marketplace providers)

Operators of essential services (OES — healthcare, energy, transport and infrastructure, and other public services)

Computer Misuse Act 1990:

The Computer Misuse Act 1990 is the main cybersecurity act that regulates the UK's digital relationship between individuals and malicious parties. It is enforced directly with the Data Protection Act 2018 and the UK-GDPR, which protect UK residents' personal data.

The Computer Misuse Act 1990 also prosecutes criminals for unauthorized access to computers for the purpose of modifying, removing, or tampering with data, as well as malicious cybercrime and cyber-attacks like ransomware and DDoS attacks.

Telecommunications (Security) Act 2021:

The Telecommunications (Security) Act, which came into effect in November 2021 (full implementation expected by March 2024).

The Telecommunications (Security) Act includes:

How CSPs (communication service providers) monitor activity and access;

How they monitor security and data protection investments;

How service providers inform stakeholders about data breaches or cyber incidents.

[299] https://www.upguard.com/blog/cybersecurity-laws-regulations-uk

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

UK eIDAS (Electronic Identification and Trust Services for Electronic Transactions Regulations 2016):

The eIDAS Regulation is a legal framework that outlines the requirements for trust service providers in regard to electronic signatures, time stamps, digital documents, and certificate services to achieve a qualified status as a trust service provider

PECR (Privacy and Electronic Communications Regulations):

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) is the UK's law for electronic communications networks and services in line with the Data Protection Act and the UK-GDPR, regulating privacy rights regarding electronic communication.

In March 2023, the UK released the white paper A pro-innovation approach to AI regulation. This whitepaper presents general AI principles, but leaves significant flexibility to existing regulators in how they adapt these principles to specific areas such as transport or financial markets[300].

- **Legislative framework against cyber-crime in Canada[301]**

- Bill C-26

An Act Respecting Cyber Security (ARCS). This proposed legislation will protect Canadians and bolster cyber security across the financial, telecommunications, energy, and transportation sectors.

This legislation introduces the Critical Cyber Systems Protection Act (CCSPA) which lays a foundation for securing Canada's critical infrastructure. It will help organizations better prepare, prevent, and respond to cyber incidents.

- Bill C-27

In November 2022, Canada has introduced the Digital Charter Implementation Act (Bill C-27), which proposes three acts that have been described as a holistic package of legislation for trust and privacy: the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence & Data Act (AIDA).

- **Legislative framework against cyber-crime in European Union**

The EU is one of the largest jurisdictions in the world and plays an active role in the global regulation of digital technology through the GDPR, Digital Services Act, the Digital Markets Act. For AI in particular, the Artificial intelligence Act is regarded in 2023 as the most far-reaching regulation of AI worldwide.

- **Legislative framework against cyber-crime in Australia[302]**

- Online Safety Act 2021

In 2021, the Online Safety Act 2021 (Cth) was passed by Parliament which commenced in January 2022. The Act builds upon the existing online regulatory framework established in the Enhancing Online Safety Act 2015 (EOSA) and creates additional compliance obligations.

- Addressing harmful content
  The Act creates a first-of-its-kind cyber abuse scheme for Australian adults. Under the Act, independent regulator eSafety can require the removal of adult cyber abuse material if it is satisfied that the material is posted with the likely intention of causing serious harm.

- Protections for children
  The Act also enhances protections for Australian children, with eSafety now having the power to issue removal notices to a full range of online services, not just social media. This includes online gaming platforms, content sharing and messaging services.

- It also provides a scheme for the take-down of contravening material (for example, material falling within the refused classification, X18+ and R18+

[300] https://en.wikipedia.org/wiki/Regulation_of_artificial_intelligence

[301] https://www.canada.ca/en/public-safety-canada/news/2022/06/government-introduces-new-legislation-to-protect-canadas-cyber-security0.html

[302] https://www.landers.com.au/legal-insights-news/cybersecurity-in-australia-passed-and-pending-legislation

classifications of the Classification Act 1995 (Cth)), with additional powers to the removal of material from, or hosted outside Australia.

- Surveillance Legislation Amendment (Identify and Disrupt) Act 2021

In 2021, the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) was passed to introduce new law enforcement powers to enhance the ability of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to combat online serious crime.

The Act creates three new classes of warrants that the AFP and ACIC may apply for:

1. Data disruption warrants: enable access to data held on a computer(s) to undertake "disruption activities" to frustrate the commission of criminal activity.
2. Network activity warrants: enable the collection of intelligence on serious criminal activity being conducted by criminal networks operating online.
3. Account takeover warrants: enable the takeover of a person's online account to gather evidence of criminal activity.

- Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Bill 2021 (Cth)

In 2021, the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 was passed to amend the Autonomous Sanctions Act 2011 (Cth).

This is a notable new cyber-related law as thematic sanctions may now address malicious cyber activity.

The Act:

- sets out new thematic categories of conduct to which autonomous sanctions can be applied
- clarifies that autonomous sanction regimes established under regulations can be either country-specific or thematic
- specifies a decision-making process for imposing targeted financial sanctions and travel bans on persons and entities under thematic sanctions regimes.

B. AI – Regulatory Approach in the world[303] [304] [305]

An increasing number of countries worldwide are designing and implementing AI governance legislation and policies.

- USA:

The White House (**USA**) has released the Blueprint for an AI Bill of Rights, a set of guidelines to protect the rights of the American public in the age of AI and President Joe Biden signed an executive order on AI in 2023.

- CHINA:

The Cyberspace Administration of **China** issued some guidelines on generative AI services.

China's regulatory draft notes that generative AI must reflect "Socialist Core Values."

In its current iteration, the draft regulations say:

- developers "bear responsibility" for the output created by their AI, according to a translation of the document by Stanford University's DigiChina Project.
- restrictions on sourcing training data; developers are legally liable if their training data infringes on someone else's intellectual property.
- regulation also stipulates that AI services must be designed to generate only "true and accurate" content.
- The country's internet regulator also announced restrictions on facial recognition technology in August 2023.

[303] European Parliamentary Research Service Author: Tambiama Madiega, www.europarl.europa.eu/thinktank (internet): http://epthinktank.eu (blog)
[304] https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/
[305] https://en.wikipedia.org/wiki/Regulation_of_artificial_intelligence

- BRAZIL:

Brazil has a draft AI law that is the culmination of three years of proposed (and stalled) bills on the subject.

- The law puts onus on AI providers to provide information about their AI products to users.
- Users have a right to know they're interacting with an AI.
- Users can also contest AI decisions or demand human intervention, particularly if the AI decision is likely to have a significant impact on the user, such as systems that have to do with self-driving cars, hiring, credit evaluation or biometric identification.
- AI developers are also required to conduct risk assessments before bringing an AI product to market. The draft AI law also outlines possible "high-risk" AI implementations, including AI used in health care, biometric identification and credit scoring, among other applications.
- All AI developers are liable for damage caused by their AI systems, though developers of high-risk products are held to an even higher standard of liability.

- ISRAEL:

In 2022, Israel's Ministry of Innovation, Science and Technology published a draft policy on AI regulation.

Israel's draft policy says:

The development and use of AI should respect "the rule of law, fundamental rights and public interests and, in particular, [maintain] human dignity and privacy." Elsewhere, vaguely, it states that "reasonable measures must be taken in accordance with accepted professional concepts" to ensure AI products are safe to use.

- ITALY:

In March 2023, Italy briefly banned ChatGPT, citing concerns about how — and how much — user data was being collected by the chatbot.

- JAPAN:

Japan, like Israel, has adopted a "soft law" approach to AI regulation: the country has no prescriptive regulations governing specific ways AI can and can't be used. For now, AI developers in Japan have had to rely on adjacent laws — such as those relating to data protection — to serve as guidelines.

- UAE

In the United Arab Emirates' National Strategy for Artificial Intelligence, for example, the country's regulatory ambitions are granted just a few paragraphs. In sum, an Artificial Intelligence and Blockchain Council will "review national approaches to issues such as data management, ethics and cybersecurity," and observe and integrate global best practices on AI.

- UK:

The **UK** has announced a pro-innovation approach to AI regulation, which largely regulates AI via existing laws.

- OECD:

At international level, the Organisation for Economic Co-operation and Development (OECD) adopted some non-binding Principles on AI, in 2019.

- EUROPEAN UNION

In June 2023, the European Parliament voted to approve[306] what it has called "the AI Act." Similar to Brazil's draft legislation, the AI Act categorizes AI in three ways: as unacceptable, high and limited risk.

AI systems deemed unacceptable are those which are considered a "threat" to society. These kinds of systems are banned under the AI Act. High-risk AI needs to be approved by European officials before going to market, and also throughout the product's life cycle.

[306] https://www.washingtonpost.com/technology/2023/06/14/eu-parliament-approves-ai-act/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- GERMANY

In November 2020, DIN, DKE and the German Federal Ministry for Economic Affairs and Energy published the first edition of the "German Standardization Roadmap for Artificial Intelligence" (NRM KI) and presented it to the public at the Digital Summit of the Federal Government of Germany.

- G7

On 30 October 2023, members of the G7 subscribe to eleven guiding principles for the design, production and implementation of advanced artificial intelligence systems, as well as a voluntary Code of Conduct for artificial intelligence developers in the context of the Hiroshima Process.

- Spain

In 2018, the Spanish Ministry of Science, Innovation and Universities approved an R&D Strategy on Artificial Intelligence.

Thus, in 2020 the Secretariat of State for Digitalization and Artificial Intelligence (SEDIA) was created.

From this higher body, following the recommendations made by the R&D Strategy on Artificial Intelligence of 2018, the National Artificial Intelligence Strategy (2020) was developed, which already provided for actions concerning the governance of artificial intelligence and the ethical standards that should govern its use.

On 22 August 2023, the Government approved the internal regulations of the Agency. **With this, Spain became the first European country with an agency dedicated to the supervision of AI**.

LAWS IN INDIA TO TACKLE AI AND CYBERCRIMES[307]

The Information Technology Act, 2000 ("IT ACT") –The act's principal goal is Protection of private data and personal information of persons. It is based on the United Nations Model Law on Electronic Commerce (UNCITRAL Model), which was recommended by the United Nations General Assembly in a resolution dated January 30, 1997.

The Act mainly focusses on the Electronic Governance, Digital Signature and Electronic Signature, along with the regulation of certifying authorities and duties of subscribers and penalties, compensation and adjudication, for any violation of rules thereto.

The Information Technology (Certifying Authorities) Rules, 2000[308] – The set of rules regulating the application and other guidelines for the Certifying Authorities.

The Information Technology (Certifying Authorities) Regulations, 2001[309] – In exercise of the powers conferred by clauses (c), (d), (e) and (g) of section 89(2) of the IT Act, 2000 the Controller after consultation with Cyber Regulations Advisory Committee has enlisted regulations that deals with terms and conditions of licence to issue digital signature certificates and the standards to be followed by the certifying authority thereto.

The Information Technology (Security Procedure) Rules, 2004[310] – In exercise of the powers conferred by clause (e) of section 87 read with section 16 of the IT Act, 2000 the Central Government has enlisted a set of rules regarding secure electronic record and secure digital signature

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009[311] – In exercise of the powers conferred by clause (y) of section 87(2) read with section 69(2) of the IT Act, 2000 the Central Government has enlisted a set of rules regarding prohibition of interception or monitoring or decryption of

[307] "International Legislative Framework of Cybercrimes- A Comparative Study Of India, Israel, And USA
Nuruddin Khan1, Dr. Shobha Gulati"; Journal of Positive School Psychology, http://journalppw.com; 2023,
Vol. 7, No. 1, 782-800

[308] vide notification No. G.S.R. 789 (E), dated 17th October, 2000, Gazette of India, Extraordinary, Part II, sec. 3(i).
[309] vide notification No. G.S.R. 512 (E), dated 09th July, 2001, Gazette of India, Extraordinary, Part II, sec. 3(i).
[310] vide notification No. G.S.R. 735 (E), dated 26th October, 2004, Gazette of India, Extraordinary, Part II, sec. 3(i) dt 05th Nov. 2004.
[311] vide notification No. G.S.R. 780 (E), dated 27th October, 2009, Gazette of India, Extraordinary, Part II, sec. 3(i) No 618, dt.27th Oct. 2009.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

and/or disclosure of information without authorisation.

The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic data or Information) Rules, 2009[312] – In exercise of the powers conferred by clause (za) of section 87(2) read with section 69(B)(3) of the IT Act, 2000 the Central Government has enlisted a set of rules regarding prohibition or collection and/or disclosure of traffic data or information without authorisation and maintenance of confidentiality.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[313] – In exercise of the powers conferred by clause (ob) of section 87(2) read with section 43(A) of the IT Act, 2000 the Central Government has enlisted a set of rules regarding privacy and disclosure of personal information and collection, disclosure and transfer of personal data or information.

The Information Technology (Preservation and Retention of Information by Intermediaries providing Digital Locker Facilities) Rules, 2016[314] – In exercise of the powers conferred by section 87(1) and clause (x) of section 87(2) read with section 6(A) and section 67(c) of the IT Act, 2000 the Central Government has enlisted a set of rules regarding operation of digital locker system, control of digital locker account credentials and security of the confidential information of the subscriber.

DIGITGAL PERSONAL DATA PROTECTION ACT, 2023[315]

The Act[316] shall apply to the processing of Personal Data in India, including both online and digitized offline data, and shall further extend to the processing of such data outside India relating to the offering of goods or services in India. **The Act also lays the foundation for various other laws such as the Digital India Act and other industry-specific laws around privacy and data protection to augment India's march towards the adoption of Artificial Intelligence (AI) and other future technologies while protecting Personal Data.**

CERT-In[317]

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

The following are the functions of the agency as defined by the Ministry of Electronics and Information Technology:

• Information about cybersecurity incidents is collected, analysed, and disseminated.

• Cybersecurity incident forecasting and notifications;

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

• actions for cybersecurity incident response cooperation; and

• issuing guidelines, advisories, vulnerability notes, and white papers on information security practices, processes, cybersecurity incident prevention, response, and reporting[318].

COUNTER USE OF AI AGAINST CYBERCRIME[319]

1. Zero-Trust[320]: It is a security model that assumes that no user or device can be trusted by default, and that access to resources must

[312] vide notification No. G.S.R. 782 (E), dated 27th October, 2009, Gazette of India, Extraordinary, Part II, sec.1 11th Aug.2023.

[313] vide notification No. G.S.R. 313 (E), dated 11th Apr, 2011, Gazette of India, Extraordinary, Part II, sec. 3(i) dt.11th Apr. 2011.

[314] vide notification No. G.S.R. 711 (E), dated 21st July, 2016, Gazette of India, Extraordinary, Part II, sec. 3(i) dt. 21st July,2016.

[315] The Digital Personal Data Protection Act, 2023 (act 22 of 2023); vide notification No. G.S.R. 788 (E), dated 17th October, 2000.

[316] https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023

[317] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBWEL01

[318] "International Legislative Framework Of Cybercrimes- A Comparative Study Of India, Israel, And USA
Nuruddin Khan1, Dr. Shobha Gulati2";Journal of Positive School Psychology http://journalppw.com; 2023, Vol. 7, No. 1, 782-800

[319] https://www.darkreading.com/vulnerabilities-threats/how-ai-shaping-future-cybercrime

[320] https://www.cisa.gov//sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

be verified at all times. This model is in contrast to the traditional security model, which assumes that users and devices are trusted within the network perimeter.

2. Machine learning and AI may be used to track unlawful and ill-intentioned activities by comparing the actions of entities through a similar environment thus using AI in security systems to distinguish "good" from "bad."

3. Anomaly Detection: This is, understanding the baseline of what normal behaviour is and then identifying when someone deviates from that behaviour. When someone logs into an account from a different location than usual or if the accounting department is mysteriously using a PowerShell system normally used by software developers, that could be an indicator of an attack.

5. Detection Response: Using AI systems, cybersecurity tools and services like managed detection and response (MDR)can better detect threats and communicate information about them to security teams. AI helps security teams more rapidly identify and address legitimate threats by receiving information that is succinct and relevant.

6. Password Protection and Authentication: AI tools, such as CAPTCHA, facial recognition, and fingerprint scanners enable organizations to automatically detect whether an attempt to log in to a service is genuine. These solutions help prevent cybercrime tactics like brute-force attacks and credential stuffing, which could put an organization's entire network at risk.

7. Phishing Detection and Prevention Control: AI within email security solutions enables companies to discover anomalies and indicators of malicious messages. It can analyse the content and context of emails to quickly find whether they are spam messages, part of phishing campaigns, or legitimate.

8. Vulnerability Management: AI-powered security solutions such as user and entity behaviour analytics (UEBA) enable businesses to analyse the activity of devices, servers, and users, helping them identify anomalous or unusual behaviour that could indicate a zero-day attack.

CONCLUSION

When it comes to AI, the Indian legislative seems to lack the foreseeability as compared to the rest of the world. Some of loopholes in the Indian Legislation against misuse of AI are: **Comprehensive AI-Specific policy:** Presently, India lacks any comprehensive AI-Specific policy that could cater the use of AI in cybercrimes. While certain provisions within existing laws like the Information Technology Act, 2000, and the Personal Data Protection Bill, 2019, touch upon AI-related aspects, they do not comprehensively address the unique challenges and complexities posed by AI technologies as compared to European Union's "Artificial Intelligence Act". Existing laws in India concentrate basically upon the data security and use of internet i.e., the basic cyber-crimes. However, specialised laws like those in countries like USA, UK, Canada, Australia, China and Brazil are still lacking and needs urgent care.

Enforceability and Ethical Guidelines: The absence of well-defined, enforceable ethical guidelines for AI development and usage in India is yet another setback in this field of law. This dearth of comprehensive guidelines may lead to inconsistent practices and potential misuse of AI systems. **Accountability and Liability:** Due to the complexity of AI systems and lack of comprehensive law and ethical guidelines it is very difficult to assign liability to anyone in case of harm or errors caused to victim.

Essential Legislative Requirements: Based on the above, the following points are noteworthy for an urgent reform in the laws related to Cyber-crimes in India:

1. An independent statutory body, having its own court proceedings, needs to be created to deal with cyber-crimes and trap the cyber-criminals without the

interference of any other Governmental bodies.

It's a well-known fact that the place "Jamtara" (also called phishing capital of India) in Jharkhand is the central hub of cyber criminals who fraud Citizens all over India through cyber means since years. Yet, the racket hasn't been busted till date for reasons unknown.

2. Statutory binding must be imposed upon the cloud memory and cyber security providers to insure their subscribers against any cyber-crime like the breach of their data, provided its not due to any lapses made by the subscriber himself.
3. Provision for Punishments in IT-Act 2000, under section 67 (punishment for publishing or transmitting obscene material in electronic form- 3 years imprisonment with fine of Rupees 5 Lakhs on first conviction and 5 years imprisonment with fine of Rupees 10 Lakhs), section 67(A) (punishment for publishing or transmitting of material containing sexually explicit act., in electronic form- 5 years imprisonment with fine of Rupees 10 Lakhs on first conviction and 7 years imprisonment with fine of Rupees 10 Lakhs) and section 67(B) (punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form- 5 years imprisonment with fine of Rupees 10 Lakhs on first conviction and 7 years imprisonment with fine of Rupees 10 Lakhs) is not sufficient and needs to be stricter since such crimes violate Art 21 (Right to Live with Dignity) and Art 51(A)(e) of the Constitution of India.

   As per the "Bharatiya Nyaya Sanhita, 2023", section 294 the offence of sale, etc., of obscene books etc. includes the display of any content (…deemed to be obscene if it is lascivious or appeals to the prurient interest…..[321]) in electronic form. Such an act has been declared as Cognizable-Bailable-Triable by Magistrate-Non-Compoundable with imprisonment of 2 years and fine upto Rs 5000 on first conviction and imprisonment of 5 years and fine upto Rs 10000 on subsequent conviction.

   The provision for punishment is very less as compared to the IT Act-2000. Although the Bharatiya Nyaya Sanhita has been enacted in 2023.

   Thus, in cases where sections of IPC/Bharatiya Nyaya Sanhita as well as sections of IT-Act are simultaneously applicable, the provisions of IT-Act must be made to supersede.
4. As per the "Bharatiya Nyaya Sanhita, 2023", section 295 the offence of sale, etc., of obscene to Child etc. includes the display of any content (…deemed to be obscene if it is lascivious or appeals to the prurient interest…..[322]) in electronic form.

   Such an act has been declared as Cognizable-Bailable-Triable by Magistrate-Non-Compoundable with imprisonment of 2 years and fine up to Rs 5000 on first conviction and imprisonment of 5 years and fine up to Rs 10000 on subsequent conviction.

   Where a child means a person who has not completed the age of 18 years.

   System using AI may be developed such that the actual age of the child may be ascertained in real-time mode before the child gains access to such materials which may otherwise be considered as lascivious or appeals to the prurient interest except otherwise proved to be explicitly for academic purpose.

[321] Bharatyia Nyaya Sanhita, 2023 (act 45 of 2023); dated 25th December, 2023, Gazette of India, Extraordinary, Part II, sec. I, dt. 25th December, 2023

[322] Bharatyia Nyaya Sanhita, 2023 (act 45 of 2023); dated 25th December, 2023, Gazette of India, Extraordinary, Part II, sec. I, dt. 25th December, 2023

For this purpose, a "Classification Act" may also be enacted like that of Australia that would ensure each website to be rated, as that of movies (by provide CBFC) such as U, U/A and A.

5. Such Acts may be enacted that mandates the adoption of national standards to prevent sensitive patient health information from being revealed without the consent or knowledge of the patient such as those of HIPPA-1996 in USA.
6. An Online Safety Act may be enacted as that of Australia Online Safety Act-2021 that would provide eSafety to adults as well as children against cyber abuse over a full range of online services by mandating removal of the materials if satisfied that it was posted with the intention to cause serious social, political, financial harm to the person.
7. A statutory body may be formed to control the use of generative-AI so that AI use maybe monitored and limited to maintain "social and religious core values" and the users may have the following right and/or restrictions to the use and propagation of AI:

- All AI service providers must provide detailed information about the extent of use of AI in their products.
- Users must have the right to know that they are using/interacting with AI and that this should come under the "Right to Knowledge".
- All AI developers and service providers should be made liable for any damage caused by their systems to the users of such AI.