The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2024
Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

AI AND CYBERCRIME: EMERGING POSSIBILITY IN THE TECHNOLOGY LAWS

Abstract

In the era of Artificial Intelligence Cybercrime has become a global common. This research paper on AI and cybercrime, focusing on emerging possibilities in technology law, delves into the intersection of artificial intelligence (AI) and cybercrime, highlighting the implications for technology law and cybersecurity. The paper further discusses the significant role of AI in cybercrime, and different types of crime emphasizing how AI can be used both to commit crimes and to enhance security measures against them. It addresses the challenges posed by the rapid advancement of AI and its potential to automate cyberattacks on a large scale, necessitating a proactive approach to counter these threats effectively. Furthermore, the paper explores the need for strategic partnerships between law enforcement, and the private sector to combat the misuse and abuse of AI for criminal purposes. The technology laws in India and the proposed acts are also discussed. At the end of the paper, the reader is able to understand the concepts of AI, cybercrime, cybersecurity and the laws regulating them.

Introduction

"The development of full artificial intelligence could spell the end of the human race…. It would take off on its own, and re-design itself at an ever-increasing rate. Humans, who are limited by slow biological evolution, couldn't compete, and would be superseded."- Stephen Hawking[1]

The above lines by Stephen Hawking highlight various facets of the emerging technology and issues associated with it. The present era is a living example of a gradual shift from human resources to relying on technology for work. Before dwelling on the concept of Artificial Intelligence one needs to pay heed to the origin of the cyberspace and issues

associated with it. The term "cyber" originates from the ancient Greek word "kubernetikos," which means "good at steering or piloting." It morphed in French to

[1] https://hub.packtpub.com/stephen-hawking-artificial-intelligence-quotes/

"cybernetique" and was used to describe the art of governing. The usage of cyber prefixes majorly began in the late 1980s specifically in science fiction, due to a cultural fixation with technology and computers. It was associated with describing various aspects of technology and its impact on society. Later, the term cybersecurity emerged in 1989 and today the term cyber is frequently used as prefix to describe various aspects of technology and dedicatedly in the sphere of cybersecurity and cyberspace.

Cyberspace and crimes associated with it

Cyberspace entails the component of the virtual environment created by interconnected computers and networks, where communication, information dissemination, and entertainment take place. It is a sphere of human interaction, communication, and information exchange that transcends the physical limitations of the tangible world. Cyberspace is characterized by its seamless, flexible, and non-material nature, lack of clearly and unambiguously identifiable boundaries, decentralization, lack of a centre of control and supervision over it as a whole, universal accessibility, digital information processing and calculations in real-time with high accuracy, and numerical, hypertext, interactive, and virtual nature. Cyberspace includes various infrastructures and telecommunications devices that allow for the connection of technological and communication systems, computer systems and related software, networks between computer systems, networks of networks that connect computer systems, access nodes of users and intermediaries routing nodes, and constituent data. From dropping a mail to running a business through social media all come under the ambit of cyberspace.

Cybercrime and its types

The motive of cybercrime and criminals associated with it is simple i.e., to exploit digital technologies for illegal activities. Cybercriminals use unauthorized access to computer systems to steal information or disrupt operations. The following are the types of cybercrime:

1. Unauthorized Access and Hacking:

Any information viewed/accessed without the permission of the rightful authority means means any kind of access without the permission of either of the rightful or the person in charge of the computer, computer system or computer network. Whereas, Hacking means an illegal intrusion into a computer system and/or network for any illegal activities. Every act committed to breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destroy and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing credit card information, and transferring money from various bank accounts to their own accounts followed by the withdrawal of money. Government websites are the most targeted sites for hackers[2].

2. Virus attacks:

Just as the way humans get infected with the viral and whole body is affected similarly the computer virus have the capability to infect other programs and make copies of itself and spread into other programs. And the programs that duplicate like viruses but spread from computer to computer are called as worms. They come under the category of malicious software. Viruses, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Trojan Horse is a program that acts like something useful but do the things that are quiet damping. Trojans come in two parts, a client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

3. Web Hijacking:

It means taking control or access to another person’s website without their acknowledgement. In this case, the owner of the website loses control over his website and its content.

4. Cyber Stalking:

[2] https://www.proofpoint.com/us/threat-reference/cyber-crime

Stalking is a simpler terms referring to as repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victim's pet, vandalizing the victim's property, and leaving written messages or objects. It may turn into serious harm like physical harm to the victim. And the act can be done both online and offline.

5. Phishing:

An act done so confidently that it almost traps the victim. It is associated with sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. In a way the sent e-mail directs the receiver to a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has.

6. Child Pornography:

Child Pornography is one of the most heinous crimes which is done on an online platform. It leaves a huge impact on the victim’s life. The Internet is being highly used as a medium to sexually abuse children. The children are viable victims of cybercrime. Because of the easy accessibility to the computers and internet these days becoming a necessity, the children have got easy access to the internet. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. They sometimes contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence. Thereafter they meet them in person and start their exploitation.

7. Cyber Terrorism:

Cyberspace is operative at every nook and corner, online crime takes the form of terrorism where the targets

Target the attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks and critical information Infrastructure are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyberterrorism is an attractive option for modern terrorists because of its easy accessibility. All countries are affected to some extent by the digital divide, and as a key enabler of the economy, society, and government, which rely on digital systems, cybersecurity should be a high priority.[3]

Best practices for protecting against cybercrime include 1. Keeping software and hardware up-to-date: To ensure safety regular updates of software and hardware are required to ensure they have the latest security patches and features.

2. Using strong build passwords: Creating complex and unique passwords for each account and keeping it secret helps in protection from cyber criminals. 3. Implementing multi-factor authentication: Add an extra layer of security by requiring a second form of authentication, such as a fingerprint or a code sent to a trusted device.

4. Securing your network: Network theft is common practice hence securing a Wi-Fi network with a strong password and encryption builds up strong security. Using a virtual private network (VPN) provides added security.

5. Being cautious with emails and attachments: opening of suspicious emails and attachments, must be avoided they may be infected with some virus. 6. Establishing clear powers for computer emergency response teams (CERT) to prevent and investigate cybersecurity breaches[4]

Cybercrime is a protentional disease and has become a global common affecting all the sectors across the globe. While cybercrime remains a concern one new technology seeks attention which is an emerging technology that has a huge potential for both construction and destruction and it is referred as Artificial intelligence, in a literal sense it may actually sound as Intelligence operated by some Artificial personality other than human. This paper ahead talks about AI and its role, positives and issues associated with it.

Artificial Intelligence and Cyber Security

Anything which is done artificially without direct human intellect can be referred as artificial and its usage as Artificial Intelligence. It is a wide-ranging tool that enables

[3] https://www.techtarget.com/searchsecurity/definition/cyberterrorism
[4] https://www.techtarget.com/searchsecurity/definition/cyberterrorism

people to rethink how we integrate information, analyse data, and use the resulting insights to improve decision-making—and already it is transforming every walk of life. The usage of AI is like a double-edged sword as it has both positives and negatives. This emerging

technology plays a significant role in transforming various aspects of society, the economy and governance is technically a simulation of human intelligence processes by machines, particularly computer systems. It enables machines to learn from experience, adapt to new inputs, and perform tasks that typically require human intelligence. In this era, AI seems to be omnipresent as it is used from the smallest of devices like smartphones to big machines. But a question arises here is AI making human work simpler or it is erasing the entire role of humans?

AI has become a powerful tool in the digital age, transforming industries and revolutionizing the way we live, work, and interact. However, the rapid advancement of AI has also opened new avenues for cybercrime, posing significant challenges for technology law and cybersecurity. Following are a few sectors where Artificial Intelligence is being applied[5]:

1. Chatbots

The coming up of inventions like ChatGPT4 and a lot of other AI tools has undoubtedly made one's work simpler. It has actually given a taste of what future chatbots could look like. ChatGPT interacts with the user just as a human does to be more precise and quicker than a human and provides multiple solutions to a single problem. It is an advanced, experimental iteration of a previous technology: AI chatbots. Thousands of companies have adopted AI-based chatbots to provide 24/7 customer support and resolve quick issues. As AI continues to evolve, it's likely that chatbots' language processing will grow more sophisticated.

2. Agriculture

One may wonder how a technical thing can be used for a non-technical purpose but that is what AI is . The aspect of Computer vision and machine learning have produced apps that can identify soil deficiencies and provide planting recommendations. It also aids Precision agriculture, farmers use AI to get predicted weather forecasts, addressing pest control, suitability of crops, etc.

[5] https://www.forbes.com/sites/qai/2023/01/06/applications-of-artificial-intelligence/?sh=229bb143be4e

3. E-commerce

The E-commerce sector is one of the most growing sectors and has inducted AI for various work. Companies use AI to predict trends, analyze performance, assist with inventory

management and more. AI provides for the best suitability for the benefit of the company.

4. Education

The gradual shift from books to smartphones, tablets, and laptops has led to the usage of AI in the education sector. Though this sector is still led by human personnel, but AI has boosted the potential of educators. It is used in multiple works like making PowerPoint presentations, analyzing results, etc. It also helps students learn simply by giving accurate and simple methods of studying.

5. Healthcare

Usage of AI is utmost effective in this sector. As it has grown more accurate, it's made its debut in the medical field as well. On the less interesting side, AI helps administrators process data, schedule meetings, organize files and transcribe medical notes. AI can assist in medical diagnoses by tracking health using wearable devices and indicating problems before patients are aware. Some programs have also adopted AI to help interpret body scans (like MRIs) to detect harmful growths with greater speed and accuracy.

Pharmaceutical companies even use AIs to analyze historical and modern data to discover new potential drugs.

6. Internet of Things

The combination of AI and the Internet of Things (IoT[6] has given rise to a new concept of Artificial Intelligence of Things i.e., AIoT. It helps in integrating AI technologies with IoT devices to enhance human interactions, improve data management and enable good decision-making. It is used in various industries and to simple daily home applications.

AI and Cybercrime

AI and its easy access has given cybercriminals opportunities to exploit AI and to enhance the scope and scale of their attacks, evade detection, and abuse AI both as an attacker sector and an attack surface.AI initiates the first steps of an attack through content generation, improve business intelligence gathering, and speed up the detection

[6] https://builtin.com/internet-things

rate at which both potential victims and business processes are compromised.AI can also be used in cyberattacks, conducting cyber terrorism and also to manipulate cryptocurrency trading practices and harm or inflict physical damage on individuals. Instances such as AI-powered facial recognition drones carrying explosives can be used for targeted bombings, highlighting the potential for AI-driven cybercrime to cause physical harm. The smartness

of AI clubbed with cybercriminals' usage leads to the conduct of cybercrime.

AI-Powered Cyberattacks

1. Deepfakes

Deepfake is usage of AI to craft or manipulate any audio/visual media to appear original. It is a combination of "deep learning" and "fake media," refer. Cybercriminals already use this technology to craft non-consensual pornography of celebrities or spread political misinformation and even tricked a UK-based energy firm into transferring €220,000 to a Hungarian bank account in 2019.[7]There are various instances of deep fake attacks on social media questioning the security of one's own individual identity.

2.AI-Powered Password Cracking

Cybercriminals are employing machine learning (ML) and AI to improve algorithms for guessing users' passwords. While some password-cracking algorithms already exist, cybercriminals will be able to analyze large password datasets and generate different password variations.

3.AI-Assisted Hacking

Apart from password cracking, cybercriminals are also using AI to automate and enhance various hacking activities. AI algorithms enable automated vulnerability scanning, intelligent system weakness detection and exploitation, adaptive malware development, etc. It is used to get controlled access to one personal information.

4.Supply Chain Attacks

AI can also be used to compromise the software or hardware supply chain of an organization, such as inserting malicious code or components into legitimate products or services.

Cybersecurity from AI and Cybercrime

[7] https://mixmode.ai/what-is/ai-generated-attacks/

As discussed above AI and cybercrime possess a strong threat and is used for committing illegal activities. Therefore, the role of cybersecurity plays a crucial role in protecting against AI and cybercrime, as AI can be used both for malicious purposes and to enhance cybersecurity measures. Cybersecurity involves protecting computer systems, networks, and data from unauthorized access, use, alteration, interference, or destruction. Cybercrime laws provide enforcement powers against such violations, covering a wide range of criminal conduct directed against the confidentiality, integrity, and availability of computer

systems and networks, as well as the data stored and processed on them.

AI can be used to automate cyberattacks, making them faster and more accurate, and can also be used to manipulate cryptocurrency trading practices and harm or inflict physical damage on individuals. To counter these threats, strategic partnerships between law enforcement, international organizations, and the private sector are essential, facilitating information sharing, enhancing capabilities, and promoting collaborative efforts to combat AI-driven cybercrime[8].To protect yourself against cybercrime, you can follow some sensible tips, such as keeping your software and operating system updated, using anti-virus software and keeping it updated, using strong passwords, never opening attachments in spam emails, not clicking on links in spam emails or untrusted websites, not giving out personal information unless secure, and contacting companies directly about suspicious requests.

To address these challenges, a proactive and collaborative approach from lawmakers, technology companies, and law enforcement agencies is necessary, to ensure the safety, security, and accountability of AI and IoT systems. By understanding the emerging possibilities and implications of AI and cybercrime, technology law can evolve and adapt, ensuring the safe and responsible development and deployment of AI and IoT systems, and protecting individuals, businesses, and society from the potential harms of AI-driven cyber-crime. The paper ahead talks about the last segment i.e., about the emerging possibility in the technology laws.

Laws governing cybersecurity and technology in India

8

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybe rcriminals-misuse-abuse-ai-and-ml

Laws are the most crucial aspect to control the menace of any crime. And Cybersecurity laws in India are primarily governed by the Information Technology (IT) Act, 20009 which deals with cybersecurity, data protection, and cybercrime. The IT Act is supplemented by rules and regulations framed under it, which regulate different aspects of cybersecurity. These rules include the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.[9]

The IT Act of 2000 defines cybercrime as any unlawful act wherein the computer is either a tool or a target or both. Cybercrimes can involve traditional criminal activities, such as theft, fraud, forgery, defamation, and mischief, as well as new-age crimes that involve the abuse of computers, such as hacking, virus/worm attacks, DOS attacks, cyber terrorism, IPR violations, credit card frauds, EFT frauds, and pornography. The act further provides for the establishment of the Indian Computer Emergency Response Team (CERT-In). It is a nodal agency for the coordination and handling of cyber incident response activities. CERT-In is responsible for monitoring and responding to cybersecurity incidents, issuing alerts and advisories, and coordinating with other agencies and stakeholders to enhance cybersecurity.

Apart from the IT Act,2000 the Indian Penal Code,1860 now referred as Bhartiya Nayaya Sanhita, 2023 provides for various provisions like organised crime.[10] It is defined as any continuing unlawful activity committed by groups of individuals singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence, intimidation, coercion, corruption or related activities or other unlawful means to obtain direct or indirect, material benefit including a financial benefit. The act further punishes offences committed in cyberspace, such as defamation, cheating, criminal intimidation, and obscenity. The Companies (Management and

9 https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf 10 https://www.thehindu.com/news/national/bharatiya-nyaya-sanhita-has-specific-provisions-on-organised-crime-in-a-first-for-national-laws/article67755898.ece#:~:text=However%2C%20a%20major%20difference%20is,less%20than%20%E2%82%B910%20lakh

Administration) Rules, 2014, require companies to ensure that electronic records and data are maintained in a secure manner.

The new proposed Digital India ACT,2023

As the Information Technology Act, 2000 (IT Act), a 22-year-old legislation, has been criticized by experts and industry bodies for its inadequacy in addressing contemporary technological issues. Due to this, the DIA is envisaged to completely replace the IT Act, of

2000. Amendments in the IPC are also proposed to include new forms of cybercrimes such as trolling, cyberbullying, hate speech, and curbing fake news amongst other crimes. The act seeks to propose the new age crimes which the old act of 2002 lacks. The DIA will be part of an Umbrella regulatory framework which will apply alongside the Data Governance Policy and the Digital Personal Data Protection Bill, 2022 (DPDPB)[11], DIA rules and the amendments in IPC. The act will focus upon the following areas like:

1. Regulate new technologies

The new technologies such as IoT,5G , metaverse, robotics and quantum computing, etc., these areas will be looked after in the proposed act of 2023.

2. Classifying Intermediaries

It covers reclassifying intermediaries into distinct categories with different set of rules applicable thereon such as social media platforms, internet service providers, OTT providers, etc.

3. New cybercrimes

The most prominent part of the act will be covering up of new cybercrimes such as unauthorised sharing of personal information, deepfakes, cyberbullying, doxing, fake news, catfishing, trolling, etc.

Various other areas like the rights of users, protecting Children's data and the adjudication system will be covered in the DIA Act.

Conclusion

The era of technology came up with easy accessibility and with both positives and negatives. The things look as simple as they are done but there is a price for everything. In the field of technology various crimes, and frauds are conducted for causing individual harm and personal gains by the cybercriminals. In order to cope up with these stringent

11 https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

laws is a need of the hour. The intersection of AI and cybercrime requires a proactive and collaborative approach from lawmakers, technology companies, and law enforcement agencies. Understanding the emerging possibilities and implications of AI-driven cybercrime is crucial for developing effective strategies and policies to combat this evolving threat. The proposed Digital India Act, 2023 has certain provisions to regulate AI

such as regulating high-risk AI systems, zero-day threat and vulnerability assessments. In addition to this the Digital Personal Data Protection Act,2023[12], will boost the protection of data as it recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purpose. Therefore, AI can be as effective as it is but with the above-required needs it would shift to a positive side and cybercrimes can be eliminated leading with the development of technology and development with technology.

12 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023. pdf