The Role of Law in the Growing Realm of Artificial Intelligence Vis-A-Vis the Concern of Cyber Security

Ms. Manika Singh[1], Ms. Preetinder Pal Sodhi[2]

[1]Research Scholar, School of Law, CHRIST (Deemed to be University), Delhi-NCR, Nandgram Road, Mariam Nagar, Ghaziabad, U.P-201003, India.
[2]Research Scholar, Department of Law, University of Jammu, India

Abstract

Artificial intelligence (AI) is now an all-pervasive force in all industries, such as finance, agriculture, health, and education, minimizing human labor and stress with increased efficiency. But in its very extensive use, there are serious ethical and legal issues, especially privacy and cybersecurity. With increasing dependence on AI and the internet, there are growing risks such as data breaches and cybercrime. AI in India is a prime driver of economic growth and technological progress, but its regulation is an imminent concern that requires governments to maintain a balance between innovation and legal protection. In this research, the legal infrastructures for regulating AI in India and other countries are examined under the lenses of cyberspace governance and protecting privacy. Strong AI regulation hinges on thorough risk assessments to prevent possible threats and ensure maximum benefits. As AI goes on to revolutionize the virtual world, strong cyber laws and policies are a must to promote security, accountability, and ethical compliance. This book critically analyses the opportunities and challenges of AI in cyber law, focusing on the imperative for clearly defined legal frameworks for governing AI responsibly.

Keywords: AI, Cyber Law, Information, Data, Privacy.

1. Introduction

Robots, particularly computers, can mimic human intellect, which is known as artificial intelligence. “One definition of AI is the ability of robots to mimic human or animal intelligence. Self-driving vehicles (e.g., the Tesla Model S), sophisticated online search engines, recommendation systems (used by YouTube, Amazon, and Netflix), voice recognition (e.g., Siri or Alexa), and strategic gaming system competition are all examples of how AI is being put to use today. The AI impact refers to the trend of formerly regarded intelligent jobs becoming less so as robots improve.” Even though using AI in the legal system is still in its early stages, more and more countries, law firms, and judicial bodies are starting to accept it. It helps attorneys save money by highlighting flaws in rulings and offering support for things like contract writing, due diligence, legal analytics, and more. Similarly, AI could help the justice system handle less work, especially when it comes to minor crimes so that human judges can focus on more difficult cases.

1.1.Artificial Intelligence (AI)

Artificial intelligence (AI) has created tremendous benefits and improvements over the last decade, and its impact is set to increase as it becomes an intrinsic component of the digital services we use on a daily basis. To aid in their operations and, more specifically, to aid in the detection and prevention of crime, governments all over the globe are seriously contemplating using AI systems and apps. Also, intelligence and security agencies have come to realize that AI can help them reach their goals for national and public safety. Significant advances in AI technologies, such as "facial recognition in the criminal justice realm, the use of drones, lethal autonomous weapons, and self-driving vehicles, can be used for disruptive purposes and harm individual rights and freedoms if they are not properly configured or managed with appropriate oversight mechanisms in place."

International policy and legislative circles are currently debating the responsibility framework and threshold for AI systems and technology, but "due to the complexity of the topic and the different legal approaches around the world concerning civil liability, there will likely not be a consensus on a harmonized and uniformed response in the near future. Artificial intelligence (AI) and machine learning (ML) also have the potential and offer the possibility of detecting and responding to cyberattacks aimed at critical infrastructure sectors like water, energy, and electricity supplies and the proper management of cybersecurity solutions to help reduce and mitigate security risks." But there are still a lot of hard problems, and SMEs that can't afford to improve their cybersecurity are especially at risk.

A significant portion of the globally linked population was isolated because of the COVID-19 pandemic. As a result businesses and people increasingly rely on technologies, AI-powered systems, and apps for everything from remote work and education to online payments and leisure alternatives like streaming video on demand. "Unfortunately this circumstance also prompted organized criminal groups to rethink and re-organize their criminal operations to explicitly target a variety of stakeholders. International organizations, research and health sector institutions, supply chain firms, and individuals are examples. Organized criminal organizations have significantly developed their "CasS (crime as a service) skills and transformed their actions into larger financial rewards", with extremely low possibilities of being caught and prosecuted by law enforcement." Cybercriminals have discovered a new way to profit from their illegal actions and a plethora of new options to plan and execute attacks on governments, businesses, and people via the use of artificial intelligence technology. In spite of the lack of proof that criminal Organizations possess substantial practical knowledge in the "management and manipulation of AI and machine learning systems for criminal purposes, such organizations have indeed recognized their enormous potential for criminal and disruptive purposes." Additionally, today's organized criminal organizations actively seek out and hire technically savvy hackers to access their data, where they can then "manipulate, exploit, and abuse" these systems in order to launch attacks and conduct illegal activity at any time, from anywhere in the globe.[1]

1.2.Development of AI Around the World: History

"Artificial intelligence was started as an academic study in 1956, and in the years thereafter has witnessed multiple waves of excitement, followed by disappointment and the loss of funding, followed by new methods, success, and renewed investment.[2]"

Throughout its history, artificial intelligence research has attempted and abandoned many different strategies, such as "brain simulation, modelling human problem solving, formal logic, vast libraries of information, and behavioural mimicry. In the early decades of the 21st century, highly mathematical statistical machine learning dominated the sector, and this method has been very effective, helping to tackle many hard issues across business and academia. Human intelligence can be so clearly characterized that a computer may be constructed to imitate it, the founding principle of the area.[3]" This gives rise to moral and ethical questions about the creation of artificial creatures with human-level intellect. These topics have been studied by myth, literature, and philosophy since antiquity. Even in science fiction and future stories, artificial intelligence (AI) is often shown as a threat to the very survival of humans because it can do so much.

1.3.Trends in current cybercrime

"Current trends and data show that hackers are increasingly depending on IoT to construct and distribute malware and target ransomware attacks, which are considerably enhanced by AI technology. More than 2.5 million devices, including industrial equipment and operators of vital infrastructure, are predicted to be completely linked online in the next 5 years, making businesses and consumers more susceptible to cyberattacks." The topics of prejudice and discrimination are also hotly debated in various national and international policy forums about AI. Even though "facial recognition may seem appealing to some governments as a way to boost public security and safety in order to prioritize national security activities, including terrorist activities, this technology may as well raise relevant and polemic issues concerning the protection of fundamental rights, including privacy and data." This calls for more international policy considerations.

The use of artificial intelligence tools, often referred to as "bots," to spread false information is a widespread phenomenon that shows no signs of abating. In particular, bots are used to disseminate false information and content across the web and social media, which has the chilling effect of misinforming the public at large and, more specifically, the younger generations, who are less able to distinguish between reliable and questionable sources of information. Further, the use of "bots" can undermine confidence, challenge the "integrity of the media, and disrupt democratic and government institutions." Humans still struggle with the task of examining and confirming the reliability of the sources, even if AI has the potential to improve the processing of massive amounts of data in order to prevent the spread of incorrect information on social media. Content moderators of media outlets and technological corporations that have no direct ties to the government generally carry out this activity. This circumstance has prompted pertinent policy-making entities to put in place extensive and all-encompassing scepticism measures.

There is growing worried in national politics and among law enforcement agencies about the possibility of deepfakes being abused or misused. Many high-profile figures in politics, entertainment, and business have fallen victim to deepfakes, which may be used in conjunction with social engineering and system automation to commit false crimes and cyberattacks. Cybercriminals all over the world are taking advantage of how dangerous deepfake technology is getting. In order to safeguard society against cyberattacks based on AI systems, the dangers associated with the use of AI for criminal objectives must be well recognized. "Criminals may be able to make their attacks easier and better with the help of AI by increasing their chances of making money in less time and coming up with more creative ways to make money illegally while making it harder for law enforcement to find them and identify them."

1.4.AI and Cyberlaw in Different Nations

Sovereign countries around the world have made a modest effort to design rules addressing their sector of cyberspace to ensure that their people's rights, national security, and sovereignty are maintained in the borderless web. That's why many cyber laws outlining online restrictions and safety precautions have been written over the last several decades. Rights to privacy, free expression, and open data are only a few examples of the issues addressed by these statutes. There are parallels and contrasts between the various cyber laws and regulations in place across the globe.

The United States of America has the longest-standing and, possibly, most effective cyber legislation and cyber security frameworks. Compared to the United Arab Emirates, which is still in its infancy as a cyber security arena, Germany has a rapidly developing technological infrastructure and legislative framework. Existing rules, although helpful, are inadequate to fight the massive financial losses and security dangers posed by cybercrime and fraud in these nations [4]. While the national legal systems in each of these nations are important, it is equally important to call for an international cyber law framework that is both comprehensive and globally recognized.

USA

The United States considers cyberspace to be an essential part of the American way of life, particularly in terms of national security and economic growth. The United States, as the birthplace of the Internet and a leading global cyberpower, was also among the first to recognize the potentially catastrophic dangers lurking online. Therefore, the issue of how to legislate the "un-governable" online has come up again and again in the nation. The nation's powerful cyberinfrastructure is the result of ongoing discussions. Cybersecurity issues in the United States are addressed at the federal level via industry-specific laws and guidelines. "The Federal Information Security Management Act (FISMA) of 2002, the Gramm-Leach-Bliley Act of 1999, and the Health Insurance Portability and Accountability Act (HIPAA) of 1996" are the most important laws pertaining to cyber security (FISMA).

In contrast to HIPAA's focus on healthcare issues, FISMA regulates the cyber-safety practices of federal departments and their contractors. In order to prevent data breaches, these regulatory frameworks mandate that healthcare providers maintain current cybersecurity procedures and regularly evaluate potential vulnerabilities [5]. The Veterans Affairs Information Security Enhancement Act of 2006 is an example of a law that was created to address a particular problem inside a single government department, specifically, the "Department of Veterans Affairs (VA). Furthermore, several populous states, like California, New York, and Massachusetts, have their unique cyber laws." However, some legislation has been criticized for being too prescriptive and intrusive. Legislation like the "Computer Fraud and Abuse Act (CFAA), passed by Congress in 1986, which makes it illegal to access and later distribute protected information, has been roundly panned for being unnecessarily restrictive and disincentivizing genuine security research. The Electronic Communications Privacy Act, which was passed in 1986," says that emails, social media messages, and other electronic communications can be called into court [6].

A clearly defined national cyber security framework is urgently needed since cyber threats are becoming more sophisticated and cross-sectoral. Since there are federal, state, and industry-specific cyber rules, compliance has been impacted since businesses must navigate a complex legal landscape. Thus, "Donald Trump, as president of the United States, signed the Cybersecurity and Infrastructure Security Agency Act of 2018 into law in 2018." [7] To deal with the growing dangers of the modern internet, the US has also pushed for more international cooperation and standardized rules.

European Union

As of April 2019, the European Union has established ethical guidelines in the form of regulations or a convention and a coordinated "European Approach to the Human and Ethical Implications of AI (European Parliament, 2019)." While many acknowledge AI's usefulness, others worry that the technology may usher in a new era of infringements on civil liberties and other human dignity forms. Global policymakers are exploring options for addressing the rise of AI. Furthermore, the European Union is likely to be a forerunner in developing a set of ethical guidelines for AI. The European Parliament requested the European Commission to make a recommendation on the civil law rules governing robotics in January 2017. This is because "without legal certainty, the rule of law will collapse into ethics and come to depend on the ethical inclinations of the powerful and the authoritative (Mireille Hildebrandt, 2019)." Parliament has established a code of ethics for robotics and engineering to ensure that the plan is carried out as intended. The European Commission, with the support of the Council of the European Union, has released a coordinated strategy to learn about the National Strategy in each EU Member State for 2019. The European Union's Artificial Intelligence Guidelines were developed with the intention of being used by the many different types of organizations and individuals involved in and impacted by AI in the European Union. These guidelines may be found both online and in hard copy across the region [8]. European Union (EU) Requirements for Safe AI Development include (European Parliament 2019) the following essential points:

- "Human Agency and Oversight
- Stability and safety
- Data Governance and Privacy
- Transparency
- Non-Discrimination and Diversity
- The well-being of society and the environment
- Accountability"

Alternative AI-Related Groups That wraps up the most important goals for AI development in the European Union. Even if AI has its policy, the European Union has its cyber law in the form of the Budapest Convention on Cyber Law. The Convention on Cyber Law, on the other hand, hasn't caught up with the times and is still using outdated methods, making it difficult for it to serve as the basis for a comprehensive AI policy. The United Nations has created its international community, the "United Nations Commission on International Trade Law, which may assist the European Union in developing its AI policy (UNCITRAL). The United Nations Commission on International Trade Law (UNCITRAL) was created in 1966 by the General Assembly as one of the first international institutions to focus on technological progress (United Nations Commission on International Trade Law). While UNICTRAL will be concentrating on cybercrime, UNICRI is the United Nations agency responsible for research and development in artificial intelligence. The United Nations' Centre for Artificial Intelligence and Robotics (UNICRI) is also known as the United Nations' Interregional Crime and Justice Research Institute. The United Nations Interregional Crime and Justice Research Institute (UNICRI) was established in 1968 to assist international, national, and non-governmental organizations in the areas of crime prevention and criminal justice policymaking. The United Nations Interregional Crime and Justice Research Institute (UNICRI) opened its Centre for Artificial Intelligence and Robotics in September 2017 with support from the Municipality of The Hague, the Ministry of Foreign Affairs of the Netherlands, and 1QB Information Technologies, Inc." We can't rule out the possibility that some kind of artificial intelligence would commit cybercrime in the future, so it seems logical that the European Union would look to these two groups as benchmarks as they work to integrate AI and cyber law.

Germany

Data privacy and the right to personal freedom have a long and well-implemented history in Germany.

The German government's ability to monitor citizens in cyberspace is constrained by the country's stringent data privacy regulations. While cyber assaults on businesses and people are on the rise, recent legislative developments and debates highlight the need for a delicate balancing act between online security and privacy. Many laws in Germany address cyber security. "Sections 202a and 303a of the Strafgesetzbuch [German Criminal Code] protect data and communication from abuse, hacking, and sabotage. To that aim, Section 303b of the same legislation requires legal repercussions for any type of cyber sabotage. The German IT Security Act of 2015 is the major piece of cyber security law in Germany." "The Federal Office for Information Security [BSI]" is Germany's national cyber security agency, and the legislation requires critical infrastructure operators to notify the agency of any incidents involving a breach of IT security. In addition, the federal government or one of the sixteen state or regional data protection agencies in Germany monitors any firm that handles personal data in the country [9].

Germany's new Federal Data Protection Act was signed into law in 2017. (Datenschutz-Anpassungs-und-Umsetzungsgesetz EU, the Act). The Act, which came into effect on May 25, 2018, incorporates the "European Union's General Data Protection Regulation (GDPR)." It's the new German data protection law that replaced the old one (BDSG). Even though the Act is just a supplement to the GDPR, it has a number of extra rules that must be followed, such as those about the appointment of "Data Protection Officers (DPOs), sensitive personal data, the rights of data subjects, the changing of the processing's purpose, video surveillance, fines and sanctions, creditworthiness and scoring, etc." [10] Legal authorities in Germany have, so far, been effective in their battle against the growing threats posed by cybercrime. The balance between safety and liberty online is complex, especially considering that Germany has one of the world's strongest data privacy regimes. Germany, on the other hand, has put in place a strict set of cyber laws to protect its digital sovereignty and data security.

UAE

Cybercriminals have been increasingly focusing on the United Arab Emirates (UAE) in recent years due to the country's robust economy, thriving oil sector, and rapid technical improvements. Concerns and financial instability were caused, for example, by malicious cyberattacks on company systems during the recent COVID-19 outbreak [11]. The UAE has one of the most advanced cyber law infrastructures in the Arabian-Middle Eastern area. Law No. 5 of 2012 of the United Arab Emirates (UAE) is the Cyber Crimes Law 2012. The Cyber Crimes Law of 2006 was superseded by this new legislation. To aid the UAE government in exchanging information on cyber security and bettering the state of cyber security across the board, the Telecom Regulatory Authority of the UAE formed a group called UAE CERT (Computer Emergency Response Teams). Together with other law enforcement organizations, they devise strategies and methods to combat cybercrime. As a result of CERT's cooperation and information sharing with CERTS from other nations, researchers are given the chance to develop new approaches to bolstering cyber security. "The National Electronic Security Authority (NESA) is in charge of the cyberspace of the United Arab Emirates (UAE)." The United Arab Emirates National Cyber Security Strategy 2019 intends to "build a secure and robust cyberinfrastructure in the UAE that allows residents to accomplish their goals and empowers enterprises to prosper" [12]. Data privacy, security, AI, blockchain, cloud computing, digital signatures, and other related topics will all be addressed under the law.

India

Being a developing country, India is yet to reach the initial stages of (AI) adoption. The emergence of social networking sites and foreign investment by multinational companies in the 21st century have stimulated AI research and development in the nation, leading to technological growth. As we can see, this cutting-edge equipment works wonders on the human mind. There is no evidence of AI deployment across the board in today's business. Because it makes use of intelligent technology, it has not only lightened the load but also improved productivity. The Indian government's policymaking agency, Niti Aayog, has placed a premium on AI. [13] India does not yet have a comprehensive legal framework for AI, but it is making indirect use of the Information Technology Act of 2000 to regulate and oversee the development of AI [14]. The government recently enacted the Data Protection Law 2019 to formalize its approach to digital governance and privacy issues pertaining to data and cyberspace. This will have direct implications for the use of AI and associated ethical considerations.

1.5.Current Position in India

Individuals' privacy is guaranteed by "Sections 43A and 72A of the Information Technology Act," even though India does not have data protection regulations. Like GDPR, it provides a remedy for damages caused by the wrongful disclosure of personal data. The Right to Privacy was established as a fundamental right under the Indian Constitution by the Supreme Court in 2017. Potentially, by 2035, India's GDP might increase by $957 billion thanks to AI, which is equivalent to almost 15% of the country's present gross value. In the future, AI will be able to affect everyone in some way. The NITI Aayog (Policy Commission) started a number of projects in 2018 that had to do with artificial intelligence (AI) [15].

The Ministry of Electronics and Information Technology set up four committees to focus on and investigate various AI-related ethical concerns. With an eye toward finalizing data protection legislation, a Joint Parliamentary Committee is now reviewing the PDP Bill-Personal Data Protection Bill 2019. Legislation becomes legislation when both chambers have approved it in Parliament. The rate of AI deployment in India is outpacing the country's ability to draft regulations for the technology. To compete in today's global economy, businesses have started to include artificial intelligence training for their employees. The newly introduced New Education Policy prioritizes starting computer programming instruction as early as Class VI. India will be on the cutting edge of artificial intelligence (AI) technology in the future.

Cyril Amarchand Mangaldas is the first law practise in India to use artificial intelligence (AI) for the purpose of analyzing and improving contracts and other legal documents. In addition, current CJI SA Bobde has spoken out in favour of using more AI in the judicial system, particularly in docket administration and decision-making in a gathering hosted by the Supreme Court Bar Association (SCBA). Nonetheless, resistance to change means that AI may not be widely adopted in poorer nations like India. Concerns have also been raised about the potential consequences of AI in a country like India, where a large portion of the population is undereducated and living in abject poverty due to the country's labour excess.

1.6.Cyber Security and AI

"Since AI and machine learning can quickly analyze millions of data sets and hunt down a broad range of cyber risks," from malware menaces to shady conduct that can result in a phishing attempt, they are more important to information security. Currently, AI is the best option for online companies to protect their data. Security professionals require robust assistance from intelligent computers and cutting-edge technology such as AI to do their jobs well and protect their organizations from attacks. AI can speed up the process of identifying and mitigating risks by automating incident response in cybersecurity. AI is also capable of analyzing vast amounts of data, searching for patterns and anomalies that can aid in the prediction and prevention of cyberattacks [16].

- **Case Laws**

a) Unauthorized Use of AI-generated likeness

(Case: Anil Kapoor v. Unknown Defendants (Delhi High Court, India)) [17]

In a milestone ruling, Indian actor Anil Kapoor received a favourable verdict from the New Delhi High Court against the unauthorized use of his AI-generated image. The court ruling safeguards Kapoor's image, voice, and signature catchphrase from being misused without his agreement. The case establishes a key precedent for personality rights in the age of AI, particularly as the entertainment industry faces challenges from deepfake technology.

b) Theft of AI Trade Secrets

(Case: U.S. v. Linwei Ding (Northern District of California, USA)) [18]

Former Google engineer Linwei Ding was charged with economic espionage and trade secret theft. Ding is accused of stealing confidential information about Google's AI and cloud computing technologies to help Chinese companies he was secretly working for. This case highlights the vital need for strong cybersecurity measures to safeguard intellectual property in the AI industry.

1.7.Relationship between artificial intelligence, digital governance, and privacy

Due to the lack of comprehensive data protection legislation, India has seen a dramatic increase in cybercrime and privacy risk susceptibility with the emergence of artificial intelligence and digital governance. There has been a rise in cybercrime and data sharing thanks to the widespread use of AI the internet and other forms of digital governance without any kind of comprehensive data protection regulation. If you've ever done a web search for a product or service and had an overwhelming number of calls or emails thereafter, you have a decent idea of what I'm talking about. Here, we see an instance of private space and data being invaded. This is how AI can "penetrate and read" the user's thoughts, leaving them open to exploitative practices like financial fraud and account theft. When someone discloses private information on social media platforms like Facebook, Twitter, WhatsApp, etc., Digital and physical privacy are both threatened by the ease with which AI can identify all of this information and transform it into a form more useful to market operators. It is clear from the correlation between AI and digital governance that both are intertwined with IT law. Therefore, it is fair to say that AI is a part of digital governance. India's efforts to establish regulatory oversight for the positive deployment of its AI technology couldn't come at a better time. It is now challenging to foresee what the fundamental framework for creating "a regulatory system to bring positive use of cyberspace for managing the fair use of artificial intelligence would be." There is no doubt that AI will transform working productivity and reduce human suffering across all industries, from healthcare and agriculture to communications and education. However, it faces several difficulties in the realms of the Internet and digital governance. As a result, AI is connected to IT and is a component of the administration of the Internet.

1.8.The Regulatory Framework in India

"The Information Technology Act of 2000 and the Digital Media Ethics Code," now in effect in India, cover most issues relating to personal data security and online activity in the age of digital technology and AI. Adoption of digital online e-transactions in the market economy is critical to increasing trade and commerce; the "Information Technology Act's mandate is primarily aimed at providing recognition to electronic commerce and trade under the international obligation of the UNCTAD model code." Online banking, trade, and business throughout the world might be said to have their roots in this model UNCTAD code. [19] The consequent proliferation of transnational enterprises and digital businesses operating beyond national borders has facilitated trade and increased employment opportunities. The problems of privacy and cybercrime didn't emerge until the early 20th century, however. Due to the widespread adoption of cloud-based applications and the proliferation of AI-based automated systems and their operations around the world, AI has become a breeding ground for privacy threats, increasing the susceptibility of data, information, and personal sensitive information stored in cyberspace. [20] While India's growing population presents new difficulties, it also makes the country an attractive investment destination for businesses providing services like banking, trading, etc., online.

"The framework and regulations controlling data and online privacy in India are now in place to protect the aforementioned forms of identification as they are considered personal and sensitive information that must be protected and constitute an integral part of the right to privacy under Sec 43 A of the IT Act, 2000 [21]. In addition, Section 230 of the Information Technology Act establishes an intermediate role, with the power function and restrictions on service providers so that the latter cannot abuse the data or services they supply." As a bonus, liability-related clarifications have been made regarding intermediaries' roles and responsibilities, including:

- Data transfer via intermediaries will be encrypted and secure.
- Middlemen will not take advantage of the trust of their customers by using or sharing their private information.
- Will implement a reliable system for filing complaints and investigating incidents when sensitive data has been compromised and individual privacy has been compromised.
- In addition to being obligated to pay damages for violations of the digital media ethical code and "Section 79 of the Information Technology Act of 2000,"[22] they will be held financially accountable for such violations.

When it comes to keeping personal information secure online, who has the burden of doing so?

India's government is responsible for safeguarding all citizens' private and public information within the republic's democratic framework. Suppose the state's "sovereignty, integrity, morality, public order, peace, or health" are in jeopardy. In that case, the state may take any measure to breach privacy in accordance with "Section 69 of the Information Technology Act."[23] Everyone knows that the following can be affected by the exemption rules mentioned above:

- Sovereignty
- Friendly relations with other countries
- National security
- Public order
- Defence

Exceptions to the foregoing reasonable restrictions cases in which the state may use all measures necessary—are rare. Stalking and voyeurism are two examples of internet privacy crimes that are explicitly defined in the Indian Penal Code as non-bailable offences since they violate the modesty of women. [24] As internet privacy and personal agreements are of the utmost importance, section 72 addresses their violation. This provides a privacy protection system and demonstrates the direct control and management of a confidentiality provision. The enforceability of internet contracts was addressed by Section 10A of the Act of 2008, and numerous other key sections were added, including Sections 43A and 66A [25], after the latter was abused to unfairly put people in jail for exercising their right to free speech.

The Shreya Singhal case resolved this question, which was the true test of the tension between personal privacy and the First Amendment right to free speech.

1.9.Advantages of AI

The following are a few of the benefits:

- **AI Improves Over Time**

Artificial intelligence (AI) technology, as the name implies, is smart, and it employs that smartness to improve network security over time. It employs ML and DL techniques to study the habits of business networks over time. It can spot trends on the internet and group related items together. Next, it looks for outliers and acts in response to any security problems.

- **Artificial Intelligence Identifies Unknown Threats**

One individual may not be able to recognize all of a company's possible risks. Every year hackers launch hundreds of millions of attacks for a variety of reasons. Unseen dangers have the potential to do a network great damage. Before they are found, recognized, and stopped, the harm they may do is far greater. Modern malware and social engineering attacks must be defended against using cutting-edge defences. One of the most effective methods for spotting and stopping the spread of unidentified dangers within an organization has been shown to be artificial intelligence (AI).

- **Artificial intelligence can process massive amounts of data.**

The network at an organization sees a lot of action. Even a typical middle-sized business receives a substantial number of visitors. That implies a substantial amount of information is sent "back and forth every day between the company and its clientele." We must safeguard this information from hackers and dangerous programs. However, cybersecurity workers can't inspect every bit of data sent.

- **Improved Vulnerability Management Capability**

The success of any network security strategy depends on how well it manages vulnerabilities. As was previously noted, a normal business faces a wide variety of dangers every day. To provide security it must be able to identify, detect, and thwart these threats [26]. Vulnerability management may benefit from AI research that analyses and evaluates current security methods.

- **Better Overall Security**

Threats to corporate networks are always evolving. Each day hackers adapt their methods. That makes it tough for businesses to decide how to prioritize security measures. Phishing attacks, DoS attacks, and ransomware are all possible at the same time.

These assaults are similar, but you need to distinguish between them in order to counter them effectively. "Human mistakes and neglect pose a greater risk to security systems than The best thing to do is add AI to your network so that you can find and prioritize possible threats."

1.10. Disadvantages of AI

- The benefits of AI in cybersecurity that we've talked about so far are just the tip of the iceberg.
- The use of AI in this area is promising, but it is not without its drawbacks. For an AI system to be built and kept up, a lot more time and money would need to be spent than is currently being spent.
- Furthermore, as AI is often educated using data sets, it's important to collect a wide variety of malware, benign, and anomalous code samples. Most businesses cannot afford the time and resources required to collect all of this data.
- Artificial intelligence systems can produce false positives and inaccurate outcomes if they lack access

to massive amounts of data and events. Inaccurate information from questionable sources might have unintended consequences.

- An official definition of a data breach is lacking from the IT Act.
- The requirements of the IT Act are only about information that is collected and shared by a "body corporate."
- Interception is not limited to times of public emergency or for reasons of public safety, as would be the case under the IT Act. Section 69 of the IT Act also says that anyone who refuses to help a designated agency intercept, monitor, decrypt, or give information stored in a computer resource can be fined and sent to prison for up to seven years.
- "Consent" is not defined under the IT Act.
- The rules and provisions of the IT Act were primarily intended to protect "personal information" and "sensitive personal data or information," including information related to:

a) "passwords,
b) financial information like bank account, credit card, debit card or other payment instrument details,
c) one's physical, physiological, and mental health condition,
d) one's sexual orientation,
e) one's medical records and history, and
f) biometric information. But "sensitive personal data or information" can't include things that the public already knows."

1.11. Recommendations

- Given that Section 4 of the Bill requires data fiduciaries to gather data reasonably and logically, the PDPB shall simply provide rules and guidelines for data fiduciaries to follow in order to follow fair and reasonable principles of data processing.
- Data Protection legislation should provide the Data Protection Authority with the power to declare permission template documents, and obliged organizations should use only such documents.
- Section 5(2) of the Bill, which includes the phrase "for incidental purposes," should be repealed because of the ambiguity it creates. Instead of using a broad word like "as soon as feasible," "Section 32 of the Personal Data Protection Bill" should provide a precise time restriction for the data fiduciary to disclose the breach of data to the data processor.
- The rules in Section 13 are quite broad, and it's possible that they could be used arbitrarily under the guise of state activities. Because of this, this section needs to define the scope of essential data in more detail and with more precision.
- For the sake of openness, data stewards may need to explain what happened when a data breach happened on their website.
- The GDPR requires that the Bill include a "qualified right to be forgotten," which will help people's privacy rights a lot.
- In order to keep things open, if there was a data breach, the Data Protection Authority might make public the data protection effect assessment and data audits that came out of it.
- The measure lays out some general guidelines for how consent should operate, but there's still room for improvement.

1.12. Conclusion

Based on the study of cyber security laws and regulations both the developed and developing worlds regularly address the topic of cyber safety. Even though many international laws are similar in principle, there are nevertheless important distinctions across states. India has a very different concept of cybercrime compared to the rest of the world. For instance, Germany and the European Union (EU) have a rather stringent policy on protecting the privacy of their residents, which constrains the monitoring capabilities of the state. It's illegal to get access to classified data in the United States. Criminal activity in India includes sharing illegally acquired information. Also, the two nations have quite different obscenity and decency regulations, which is a factor in how cybercrimes are dealt with in each.

Cyber-security is still a developing field, and in light of recent technological developments, governments must be ever-vigilant in the face of new dangers while also working to clarify current cyber laws. However, since the Internet is a "borderless" ecosystem, just passing laws at the national level won't address problems like international cyber terrorism, fraud, or jurisdictional disputes. Therefore, there is a need for an international cyber law standardization framework. Therefore, nations that understand the significance of cyber safety should work to include provisions for international collaboration in their cyber-security laws.

References

1. MIT Technology Review, "Transforming the Energy Industry with AI" (2021) https://www.technologyreview.com/2021/01/21/1016460/transforming-the-energy-industry-with-ai/.
2. Yim, I. H. Y., & Su, J., "Artificial Intelligence (AI) Learning Tools in K-12 Education: A Scoping Review" Journal of Computers in Education 1-39 (2024).
3. Appknox, T., "A Glance at Australia's Cyber Security Laws" (2022) https://www.appknox.com/blog/glance-australias-cyber-security-laws.
4. Ganguli, P., "The Rise of Cybercrime-as-a-Service: Implications and Countermeasures" SSRN 4959188 (2024).
5. Tonazzo, A., "From Cyber Law to Medical Law: Comparative Legal Theory and Its Societal Impacts" (2023).
6. Lieberfeld, J., & Richards, N., "Fourth Amendment Notice in the Cloud" 103 BUL Rev. 1201 (2023).
7. The White House, "National Cyber Strategy for USA" (2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
8. "Tackling Online Disinformation" Shaping Europe's Digital Future (n.d.) https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.
9. Germany: Land of Data Protection and Security – But Why? (2018, December 05). from https://www.dotmagazine.online/issues/security/germany-land-of-data-protection-and-security-but-why (last visited 28 Oct 2022).
10. Cyber Crime Law. from https://www.cybercrimelaw.net/Germany.html (last visited Sep 29, 2022)
11. Mahmood, S., Chadhar, M., & Firmin, S., "Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective" 14 Applied Sciences 11610 (2024).
12. "National Cyber Security Strategy" (2019) https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cybersecurity-strategy-2019.
13. Information and Technology Act, 2000, § 2(0).
14. Information Technology Act, 2000, § 67.

15. Niti Aayog, https://niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (last visited 15 Oct 2022).
16. Uzoma, J., Falana, O., Obunadike, C., Oloyede, K., & Obunadike, E., “Using Artificial Intelligence for Automated Incidence Response in Cybersecurity” 1(4) International Journal of Information Technology (IJIT) (2023).
17. Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023, Delhi High Court, Order dated September 20, 2023.
18. United States v. Linwei Ding, No. 24-cr-00141 (N.D. Cal. 2025).
19. Mishra, N., & Kugler, K., “International Community in the Global Digital Economy: A Case Study on the African Digital Trade Framework” 73(4) International & Comparative Law Quarterly 853-889 (2024).
20. Gupta, Rohit. (n.d.). An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective - Privacy - India. https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective (last visited 28 Oct 2022).
21. Information and Technology Act, 2000 , §43
22. Information and Technology Act, 2000 , §79
23. Information and Technology Act, 2000 , §69
24. Keswani, M. (n.d.). CYBER STALKING: A CRITICAL STUDY. Retrieved Sep 29, 2022, http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf (last visited 22 Oct 2022).
25. Information and Technology Act, 2000 , § 66
26. Laura DeNardis and Jennifer Daskal on Society’s dependence on the internet: 5 cyber issues the coronavirus lays bare, https://theconversation.com/societys-dependence-on-the-internet-5-cyber-issues-the-coronavirus-lays-bare-133679 (last visited 20 Oct 2022).