

Chapter 15

Artificial Intelligence and Cyber Risks: Legal Challenges and Regulatory Responses in the Digital Age

Deep Mahata, Student of LLB (H), Department of Legal Studies, Swami Vivekananda University

Abstract

Artificial intelligence is increasingly becoming a major force in shaping the landscape of the digital world, offering many prospects as well as creating many obstacles in the field of cybersecurity. In this paper, the role played by AI technology will be analyzed in terms of both its benefits and risks. First of all, artificial intelligence helps in increasing efficiency in threat detection and response while contributing to better overall security measures. At the same time, the potential of AI to be used for conducting attacks on cybersecurity systems is becoming increasingly real.

The paper considers the legal issues that have emerged due to these AI-based cyber threats. It is becoming increasingly challenging to resolve these legal issues in light of current laws due to their tendency to trail far behind technological advances. Moreover, the absence of any legislation related to the usage of AI technology has become another obstacle in the way of proper risk management.

Also, this paper will consider the contemporary approach to managing cybersecurity risks at both national and global level and will emphasize that the creation of new instruments of law that could be easily adapted to new circumstances was crucial. Also, the significance of ethics in overcoming current problems will be underlined.

To conduct a balanced analysis of this problem, an interdisciplinary research strategy is employed here, which takes into account both technological factors and legal issues. Finally, it should be said that addressing cyber security risks linked to AI requires not only strict law and innovations but also morality.

Keywords: *Artificial Intelligence (AI), Cybersecurity, Legal Challenges, AI-based Cyber Threats, Ethics & Risk Management*

Introduction – Artificial Intelligence and Emerging Cyber Risks

Artificial intelligence (AI) is one of the technologies that have had a significant impact on the digital world, forming an integral part of modern life. The implementation of artificial intelligence through task automation and decision-making processes has made many operations much more efficient, thus taking an active part in various fields, including cybersecurity, enabling faster identification of threats and preparing for tackling any issues. However, despite being one of the best ways to ensure security of information resources, it has created new challenges in the sphere of cybersecurity.⁴⁰⁵

Among the topmost concerns which should be addressed are those of the two-way abilities of AI. While on one hand AI helps in improving cybersecurity, on the other hand it can be misused for wrong

⁴⁰⁵ Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).

purposes. There have been reports of cybercriminals resorting to the use of AI to initiate sophisticated attacks, which include automated hacks, deep fake-enabled identity thefts, and customized phishing operations. Such AI-powered attacks prove to be very challenging to combat since they tend to adapt and evolve rapidly.

In addition, the increasing use of artificial intelligence (AI) poses important issues relating to accountability and liability. In cases where the use of the AI system results in any kind of damage either due to a breach of security or the result of any deliberate tampering, it may become challenging to assign responsibility. Should the responsibility lie with the developer, the end-user, or the organization using the AI technology? This is a problem that hasn't been sufficiently regulated by current legislation.⁴⁰⁶

Moreover, the constant development and progress of AI systems create a number of challenges for regulation of AI technologies. Conventional cybersecurity legislation generally takes on a reactive and fixed form, while the risk generated by AI technologies is both proactive and continuously evolving. The difference in approaches creates a gap in regulations, making the system highly susceptible to exploitation. It is essential to develop laws that can evolve with technology.⁴⁰⁷

In this chapter, the reader is introduced to the complex interplay between artificial intelligence and cybersecurity. Not only does the chapter point out the promising role played by artificial intelligence in enhancing digital security but it also emphasizes the risks associated with its use. What makes the chapter more intriguing is its emphasis on the need for novel laws and regulations to manage artificial intelligence within the digital space.⁴⁰⁸

Nature and Types of AI-Based Cyber Threats

AI has drastically altered the way cyber threats function and increased their complexity and adaptability to make them much harder to recognize than ever before. While classic attacks require a specific approach to be executed, AI technologies allow cyber threats to run independently and change tactics depending on the current conditions and data gathered in the process. This development introduced the emergence of the new breed of cyber dangers that poses a threat both to our technological infrastructure and laws currently in effect.⁴⁰⁹

The first and foremost example of cyber threats generated by means of AI would be deepfake technologies that employ artificial intelligence to create convincing audio or video content that cannot be easily distinguished from the original. Such cyber threats may be used for various purposes including personal identity theft, fraud schemes, manipulation, or defamation. For example, a maliciously edited recording or video of a person may be quickly disseminated among the masses before anyone realizes that it is not authentic.⁴¹⁰

A further issue of note is the development of AI-based malware. Different from regular malware, which executes pre-programmed actions, AI-powered malware changes its course based on what happens

⁴⁰⁶ European Commission, Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act) COM(2021) 206 final.

⁴⁰⁷ World Economic Forum, Global Risks Report 2023 (2023).

⁴⁰⁸ United Nations, Report of the Secretary-General on Digital Cooperation (2019).

⁴⁰⁹ European Union Agency for Cybersecurity, Threat Landscape for Artificial Intelligence (2021).

⁴¹⁰ National Institute of Standards and Technology, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (2019).

around it, making it capable of adapting and modifying its tactics in response to the situation it encounters in order to evade security solutions. In addition, the malware itself decides the best way to proceed in an attack, thus making such malware more hazardous as it will be able to penetrate through any security measures used.

Finally, the issue of automated vulnerability scanning needs mentioning in terms of the dangers posed by AI. On one hand, cybersecurity experts can employ AI technologies to scan vulnerable parts in systems and fix them before the hackers have a chance to do anything; however, on the other hand, AI technologies enable cybercriminals to scan huge networks and find entry points in the shortest possible time.

The evolution of social engineering tactics in conjunction with AI has also taken place. Typically, the attacks were based on simple methods involving deception and, in particular, phishing emails. Modern AI technologies enable hackers to create highly targeted, personalized, and effective communications based on analysis of a victim's online activities, interests, and communication habits. Such intelligent phishing technology can write convincingly mimicking certain styles and producing targeted communications.⁴¹¹

It is vital to emphasize that AI is a useful tool not only for hackers but also for cybercrime fighters. AI technologies are extensively applied in cybersecurity practices to detect threats, analyze anomalies, and operate automated response systems. It provides an ability to process huge amounts of data quickly and to react promptly to suspicious behavior.⁴¹²

Nonetheless, the ability of AI to protect against cyber threats also raises concerns due to its dual capabilities. In other words, the technology capable of protecting the network from cyberattacks can simultaneously be employed to conduct an attack. Therefore, defining the boundaries between legal and illegal applications of AI becomes complicated.

Moreover, the dynamic nature of AI cyber threats poses major difficulties for the law enforcement system. Typically, legislative measures and regulations are aimed at controlling static cyber threats, which are easily identifiable and classified under certain categories. In contrast, AI cyber threats are characterized by their dynamicity and flexibility. In addition, some AI cyber threats may act autonomously, meaning that there will be no person to take responsibility for any negative consequences.

To sum up, the emergence of AI-based cyber threats adds another layer to contemporary cybersecurity issues. Notably, the nature of such threats and their types call for specific measures in dealing with AI cyber threats.⁴¹³

Legal Challenges in Regulating AI and Cyber Risks

The development of Artificial Intelligence technology has led to a number of legal issues that cannot be easily solved using the existing systems of laws. Even though artificial intelligence promises many advantages, it has its fair share of problems that cannot be ignored in fields such as responsibility,

⁴¹¹ Kaspersky, Spam and Phishing in 2021 (2022).

⁴¹² IBM, IBM Security: AI in Cybersecurity Report (2021).

⁴¹³ World Economic Forum, Global Risks Report 2023 (2023).

privacy, and legal authority. Since the law is meant to guide humans, it is faced with the challenge of adapting to this new reality of machine decisions.

Another significant problem is that of accountability. In the case where the AI makes its own decisions, detects a threat, or takes action, it can be hard to determine who is liable for any mistake that occurs. For example, if an AI-driven cyber security software program does not succeed in stopping an attack or even causes one, whose fault would it be? Who will be accountable for any failure—a person who programmed the software, the company who implemented it, or the individual who trusted it? The current laws cannot easily be applied to autonomous machines.⁴¹⁴

The other important problem that arises in connection with this type of technology is that related to data protection. It involves huge quantities of data that must be used for the purpose of successful work of the artificial intelligence. Personal data is involved, creating problems related to violation of personal rights as well as potential abuse. Some attempts have been made to solve the problem by means of such measures as data minimisation, consent, as well as right to explanation. Nevertheless, these laws were not initially designed for AI technologies, and as a result of this, they do not take into account such issues as algorithmic bias, black box decision-making, and huge amounts of data processing.⁴¹⁵

Another important problem in terms of law related to AI and cyber security is that related to jurisdiction. The nature of cyberattacks makes it rather hard to identify the jurisdiction applicable to the case, as it usually spans across several jurisdictions at once. It is possible that an AI-based cyberattack can be launched from one country while victims belong to another and use servers of third parties.

Another aspect which further complicates the issue under discussion is the absence of a single set of unified legal norms on how to regulate the use of AI technologies. Although some legislative frameworks in various countries and regions start being developed, there is no internationally recognized legal act that could guide the activities related to the use of AI.⁴¹⁶

In addition, the ever-changing character of the technologies used poses another significant challenge as laws tend to be quickly outdated in this case. In other words, unlike traditional problems discussed in courtrooms and addressed by legislators, artificial intelligence and all of its implications should be regulated much more flexibly.

Summarizing everything said above, it should be stated that the issue of AI and the legal regulation of this technology is rather complicated and needs thorough discussion and cooperation on both national and international levels. The aspects of liability, cyber risks and data protection mentioned above illustrate perfectly the problems that arise from the current legal practices.⁴¹⁷

National and International Regulatory Responses

In the process of advancing and embedding itself within people's lives, there have been efforts from many governments around the world to acknowledge the dire need for regulatory measures on the use

⁴¹⁴ Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).

⁴¹⁵ General Data Protection Regulation, Regulation (EU) 2016/679.

⁴¹⁶ Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence* (2019).

⁴¹⁷ United Nations, *Report of the Secretary-General on Digital Cooperation* (2019).

of Artificial Intelligence technology. It is not anymore an idea of the future; rather, it is impacting the economy, the form of governance, and even the cyber security framework.⁴¹⁸

On a national scale, many nations have developed AI policies and cybersecurity strategies designed to foster innovation yet protect the public's interest. For instance, most countries' policies involve developing initiatives that encourage innovation and the development of digital infrastructure and ensure that there is no misuse of AI technologies. Many nations are now increasingly engaging in cybersecurity practices that utilize AI capabilities to mitigate security threats. Some nations have already started working on developing regulations concerning certain areas such as data protection and algorithms.⁴¹⁹

Nevertheless, each country employs its own methods of regulating artificial intelligence. There are those who value progress, which means that they have adopted a lenient regulation system where the development of technology is not impeded in any way. Then there are those who prefer a cautionary attitude, putting their emphasis on the protection of personal information and ethics. Each method has its own merits, but their differences may become a problem for international collaboration.⁴²⁰

Internationally speaking, institutions have been instrumental in establishing guidelines regarding the issue. The United Nations and the Organisation for Economic Co-operation and Development have devised various ethical principles for the use of artificial intelligence in different fields. These guidelines stress the importance of transparency, accountability, fairness, respect for human rights, and other such factors. Although they are non-binding recommendations, these ethical guidelines may be considered when a country establishes its own regulations.

Despite all the mentioned actions, one of the most difficult obstacles in regulating AI is the absence of universal norms on an international scale. At the moment, there is no unified set of international legal standards that could control the use of AI technologies. The process of regulating AI technologies takes place in a fragmented way, when each country develops its own norms. Such regulation leads to uncertainties that could become obstacles to the activities of multinationals that work on an international scale. Additionally, such regulation complicates resolving cross-border issues like cybercrime or misuse of technologies. Another essential point that requires attention is the need for international cooperation. Since cyber risks related to AI are not limited to any territory, their isolation and separate regulation do not solve the problem.⁴²¹

Alongside harmonization, the need for adaptability and flexibility of regulation becomes increasingly more obvious too. Technologies are dynamic and rapid changes within the realm of AI require an equally agile response from the legislative branch, lest they find themselves outmoded very soon. It is therefore vital to develop regulatory methods that are able to cope with technology and its constant changes in time. For instance, soft law instruments and regulatory sandboxes might prove useful in such cases.⁴²²

It would be fair to conclude that considerable progress has been achieved in tackling the problem of AI on both domestic and international scales. However, there is still a long way ahead of us towards solving this problem once and for all. As of now, one of the major drawbacks in AI regulation is its

⁴¹⁸ World Economic Forum, Global Risks Report 2023 (2023).

⁴¹⁹ NITI Aayog, National Strategy for Artificial Intelligence (2018).

⁴²⁰ European Commission, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust COM(2020) 65 final.

⁴²¹ Council of Europe, Convention on Cybercrime (Budapest Convention) (2001).

⁴²² Financial Conduct Authority, Regulatory Sandbox Lessons Learned Report (2017).

inconsistency and multiplicity, which makes it difficult to control. What should be done to solve this problem? Harmonization of laws and cooperation between countries seems to be the key.

Ethical Dimensions and Risk Management in AI Cybersecurity

Now that Artificial Intelligence is being deeply integrated into cybersecurity, it is time for the significance of ethics not to be underestimated. Although law creates an enabling framework for any activity and serves as its basis, ethics makes sure that whatever technology gets implemented is done so ethically and is based on certain standards that correspond to human values and human rights. Ethics plays the role of a compass within the sphere of AI-based cybersecurity.⁴²³

Another critical issue that arises in relation to ethics and artificial intelligence (AI) is the problem of algorithmic bias. AI is trained based on the information that exists in the dataset, and if there are any biases present in the data, then the predictions made by the algorithm will also be skewed. For instance, when it comes to the domain of cybersecurity, there can be instances where the threat posed to users is not properly evaluated, which might lead to the unjustified targeting of some individuals.

Transparency is yet another crucial ethical value. Many AI applications operate on a “black box” basis, which means that their decision-making process involves sophisticated mechanisms whose workings cannot be fully comprehended by people. In cybersecurity, this can become problematic if organizations find themselves incapable of elucidating the reasoning behind their decisions, such as identifying an emerging threat or choosing a particular course of action. It becomes particularly relevant if the decisions made by the organization have serious implications, including denying entry, labeling individuals, or dealing with cyber attacks.⁴²⁴

The issue of accountability in itself raises a vital point. As mentioned in previous sections of the book, it may prove challenging to define who should be held responsible for the activities performed by artificial intelligence. Ethical guidelines try to resolve this problem through highlighting the significance of having humans in charge. Regardless of how independent a particular algorithm might seem, there should always be ways to hold humans accountable for its decisions and actions.

A number of ethical frameworks designed by different organizations emphasize such concepts as accountability, responsibility, fairness, and human supervision. The purpose of promoting these approaches is to promote responsible innovation while developing new technologies. This way, innovations can help people without compromising their fundamental rights and well-being. Cybersecurity technologies, in turn, need to be created to protect personal information and ensure that no harm is done to any party involved.

Aside from ethics, risk management becomes crucial in combating AI-driven cyberattacks. Companies should become proactive in dealing with such threats by recognizing, assessing, and controlling any risk at an early stage. The first thing for companies to do is to establish a strong cybersecurity strategy that makes proper use of AI technologies. It includes safe design, timely risk identification through assessment, and appropriate access controls.⁴²⁵

⁴²³ United Nations Educational, Scientific and Cultural Organization, Recommendation on the Ethics of Artificial Intelligence (2021).

⁴²⁴ Royal Society, Explainable AI: The Basics (2019).

⁴²⁵ International Organization for Standardization, ISO/IEC 27001 Information Security Management Systems (2013).

Monitoring also becomes necessary for companies dealing with risks associated with AI technologies. Since these technologies work under dynamic conditions, risks may emerge quickly and require fast actions to be undertaken. Thus, continuous monitoring helps companies stay aware of what happens within the system and react to the problems in time.⁴²⁶

The inclusion of ethical principles in the development of AI also needs to be considered. Known as 'ethics by design', it allows embedding ethical principles right in the process of the development of the technology and, hence, developing a system that would be not only effective but also responsible.

Finally, when dealing with cyber risks associated with AI technologies, it is necessary to find a balance between legal and ethical approaches. Whereas legal frameworks define what behaviour is not acceptable and outline basic rules, ethics goes further and encourages fair and honest actions in addition to merely complying with the law. As seen from above, a purely legal strategy cannot solve all issues related to AI in cybersecurity, while ethics allows having an even broader perspective on the matter.⁴²⁷

To conclude, ethics plays an important role in AI in cybersecurity just like any other aspect under discussion. Bias, transparency, accountability, among others, should definitely be taken into consideration when addressing ethical questions in relation to AI in cybersecurity. In addition to that, risk management is of critical importance for ensuring cyber safety as well.

Future Directions and Conclusion – Towards a Resilient Legal Framework

In view of the ever-evolving nature of AI technologies, the future of cybersecurity legislation and policy regulation is going to be highly dependent on how efficiently legal institutions are able to keep up with these changes. Current laws, which have been tailored to a much less dynamic environment, will continue to prove themselves incapable of dealing with the problems that have arisen. Thus, the need for creating new laws and frameworks becomes inevitable.⁴²⁸

A major step to take in order to ensure success for the future is the creation of laws that are technology-neutral. In other words, laws should concentrate on addressing the problem itself rather than some particular type of technology being involved. The idea is that these laws should be able to maintain their relevance despite any rapid development of technology. Due to the fact that AI technologies are currently developing rapidly, laws may lose their value quickly if they are focused on addressing certain issues associated with a certain technology.

On the other hand, issues relating to accountability cannot be ignored. As AI becomes more and more autonomous, questions relating to responsibility and liability will be of growing importance. Future laws on the use of AI will need to address these questions by setting out clear rules on who will be responsible in what situations, as well as procedures for oversight, auditing, and redress. Without such clarity, AI technology will not be trusted, thereby limiting its usefulness.

The role of judicial interpretation in relation to AI and cybersecurity will be of increasing importance in years to come. Courts will have to interpret existing laws in light of emerging technologies, especially in areas where the legislature has not made any provision. The rulings of the courts will be

⁴²⁶ National Institute of Standards and Technology, AI Risk Management Framework (2023).

⁴²⁷ European Union Agency for Cybersecurity, Cybersecurity and AI: Opportunities and Challenges (2021).

⁴²⁸ World Economic Forum, Global Risks Report 2023 (2023).

significant for filling legal gaps, as well as developing legal principles pertaining to AI and cybersecurity.⁴²⁹

Another key point concerning future regulation would be the importance of multidisciplinary. Risks in the cyber sphere associated with artificial intelligence cannot be tackled purely legally. Instead, there should be an interaction between specialists in law, technologies, policy-making, and ethics. Each discipline has its unique contribution to make – technologies give an idea of what artificial intelligence entails and what tools may be used to tackle its dangers, while law is about structure and implementation of these ideas into practice, while ethics makes sure human value system remains the focus of innovation.⁴³⁰

International cooperation is also expected to play an increasingly important role. Cyber threats are by nature global and cross-border in their effects. Thus, separate efforts made by different countries will not suffice to address these issues. Instead, it would be necessary to cooperate on many levels in order to tackle AI-powered cyber risks.

In the end, it becomes necessary to maintain the proper balance between the two. On the one side, an excess of regulations may prove detrimental to development. On the other hand, lack of regulation may lead to misuse and other harmful effects on the user's side. The balance will allow for both development to take place and safety from various dangers.

In summary, the evolution of the world of AI and cybersecurity will depend upon the ability of the legal framework to adjust to new circumstances. It is important to create adaptive and technology-neutral legislation, encourage accountability and cooperation among experts in multiple fields and even between countries. Thus, through achieving the proper balance, it will be possible to make the most out of the technology.⁴³¹

-----*****-----

⁴²⁹ Supreme Court of India, Justice KS Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

⁴³⁰ United Nations Educational, Scientific and Cultural Organization, Recommendation on the Ethics of Artificial Intelligence (2021).

⁴³¹ NITI Aayog, National Strategy for Artificial Intelligence (2018).