Malaysian Journal of Social Sciences and Humanities (MJSSH) (e-ISSN : 2504-8562)
2025, Volume 10, Issue 1, e003132
DOI: https://doi.org/10.47405/mjssh.v10i1.3132

REVIEW ARTICLE

The Challenge and Response of Network Security in The Era of Artificial Intelligence

Chen Mengru[1*], Mohamad Rizal Abd Rahman[2], Mohd Zamre Mohd Zahir[3]

[1]Faculty of Law, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia
Email: p129802@siswa.ukm.edu.my
[2]Faculty of Law, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia
Email: noryn@ukm.edu.my
[3]Faculty of Law, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia
Email: zamre@ukm.edu.my

CORRESPONDING AUTHOR (*):
Chen Mengru
(p129802@siswa.ukm.edu.my)

KEYWORDS:
Artificial intelligence
Cybersecurity
Law
Public

CITATION:
Chen, M., Mohamad Rizal Abd Rahman, & Mohd Zamre Mohd Zahir. (2024). The Challenge and Response of Network Security in The Era of Artificial Intelligence. *Malaysian Journal of Social Sciences and Humanities (MJSSH), 10*(1), e003132. https://doi.org/10.47405/mjssh.v10i1.3132

ABSTRACT

With the emergence of artificial intelligence, new situations, new problems, and new challenges in the field of network security are emerging one after another, affecting the global economic pattern, development pattern, and security pattern, also putting forward higher requirements for network security assurance. Nowadays, cases of using fake audio and video such as AI face-changing and AI voice-changing to commit new cybercrimes occur occasionally. From the individual level, artificial intelligence lowers the threshold for personal cybercrime. At the social level, artificial intelligence forges false information that misleads the public and poses a certain threat to people's property. This article aims to analyse the function of artificial intelligence and discuss the impact of emerging technologies on social development. This article by comparing domestic and foreign researches on artificial intelligence, using a qualitative research methodology with case studies and literature, and expresses views and ideas regarding the laws about artificial intelligence. The article finds that maintaining network security is the common responsibility of the whole society and requires the joint participation of governments, social organisations, and the majority of netizens. Therefore, it is suggested that other security risks that may be caused by artificial intelligence in the future, should be prevented based on risk prevention, and active use laws and regulations to regulate and guide. Secondly, by referring to the law, ensuring the protection of personal information, and standardise the cyber security environment is so significant. Finally, carry out online publicity and education to improve the network security awareness.

Contribution/Originality: This study contributes to the existing literature by discussing the laws on artificial intelligence cybersecurity in China and other countries and proposing three corresponding governance systems to address the cybersecurity risks caused by artificial intelligence crimes.

1. Introduction

With the emergence of artificial intelligence and the accelerated upgrading of network information technology, new situations, problems and challenges in the field of cybersecurity are emerging, affecting the global economic pattern, development pattern and security pattern, and putting forward higher requirements for cybersecurity protection. This is a revolution that affects the whole world, not only promoting the rapid development of artificial intelligence-related research, but also promoting the research in various fields related to artificial intelligence (Yadlapati et al., 2024). The popularization of the application of artificial intelligence technology has brought opportunities for national cybersecurity governance, but at the same time, it is also necessary to be vigilant about the harm of abuse and illegal use of artificial intelligence technology to personal safety and social security (Raimundo & Rosário, 2021).

At the individual level, AI lowers the threshold for individual cybercrime. Artificial intelligence not only brings convenience to human life, but also provides convenience for criminals to commit crimes (Abdel Razek, 2020). On the one hand, artificial intelligence has the ability to act independently, and its autonomy is gradually increasing, which allows criminals to use it to commit crimes, only need to set up procedures and instructions and other simple preparatory work, without appearing at the implementation site. For example, in the case of artificial intelligence infringing on citizens' personal information, criminals used artificial intelligence technology to identify picture verification codes and create matching databases to commit network fraud (Mikhailov & Kokodey, 2023). Human identity information is unique and private, once it is obtained by illegal elements, it will lead to the leakage of citizens' personal information, and even be improperly used by criminals. Artificial intelligence technology is to provide convenience for this crime, the application of artificial intelligence technology in criminal cases, greatly reducing the threshold of crime. At the societal level, artificial intelligence crimes are more efficient. When criminals carry out criminal activities, they are often hindered by various factors (Al Qatawneh et al., 2023). Artificial intelligence can not only capture a large amount of data in a short period of time, but also calculate the obtained data quickly to obtain the optimal solution. Even in the face of extremely complex crime scenes, the characteristics of high-speed computing of artificial intelligence can be used to make the best scheme in a very short time, thus greatly improving the efficiency of crime. For example, when conducting securities trading, artificial intelligence can be used to capture the information needed by criminals in a short time and process it to achieve the effect they want (Blauth et al., 2022). Therefore, the application of artificial intelligence has greatly improved the efficiency of crime. In addition, artificial intelligence crimes have a hidden nature. Artificial intelligence has very strong autonomy and data processing capabilities. If it is applied to crime, especially when it is used to carry out criminal activities such as illegal intrusion into the computer information system, it can secretly collect the information of the relevant target without attracting people's attention, and it can also use its powerful computing power to eliminate criminal traces, so as to complete a very hidden crime. For example, drug dealers have specially developed a miniature artificial intelligence drone, which can avoid the patrol of the drug police during drug trading, choose the best path and time according to the instructions of drug dealers, and transact with each other, reducing the possibility of drug dealers being detected (Solov'ev, 2023). The application of artificial intelligence makes crimes more covert and increases the difficulty of detection.

How artificial intelligence affects cybersecurity governance and how it changes the mechanism and efficiency of cybersecurity governance is a real problem that urgently

needs to be studied. With the increasing cyber attributes of public security issues, the combination of artificial intelligence and cybersecurity governance issues will become the focus and difficulty of future cybersecurity governance research (Bokhari & Myeong, 2023). The study of the mechanism of artificial intelligence on cyber security governance and the identification of public risks brought by governance is of great significance and realistic research value for the future use of artificial intelligence technology to safeguard public security and social stability, and to promote the modernisation of the national governance system and governance capacity (Wang, 2024).

Nowadays, artificial intelligence has been deeply embedded in People's Daily life. The "intelligence" of artificial intelligence is based on powerful algorithmic operations, especially in the face of a large amount of information, artificial intelligence can quickly comb, analyse, and make correct decisions, which is difficult for humans (Neiroukh et al., 2024). The rise and rapid development of artificial intelligence has made those tasks that are time-consuming and labour-intensive for humans insignificant in the face of artificial intelligence. The wide application of artificial intelligence conforms to the development of The Times, and has a huge impact on human beings because of its powerful learning ability and the ease of its operation (Goralski & Tan, 2020).

First, in education, whether it is teachers' teaching, research tasks, or students' learning tasks, artificial intelligence has played a great role in helping. When teachers teach, artificial intelligence can calculate the most appropriate teaching method for students according to the different characteristics of different students and give feedback to the teacher, so that the teacher can teach the students in a targeted way. Meanwhile, the students can also use the feedback of artificial intelligence to have a clear understanding of themselves and carry out corresponding exercises, so as to achieve better teaching effects (Chen et al., 2020). Secondly, in the medical field, whether in work efficiency or in medical technology, artificial intelligence has occupied an absolute advantage. For example, in the treatment of patients, artificial intelligence can quickly obtain the patient's past medical records, and can quickly find the treatment method of similar cases, so as to arrive at the best management plan (Secinaro et al., 2021). In addition, in the field of transportation, the development and application of a large number of autonomous vehicles at home and abroad are also facilitating human production and life (Krysiuk, 2022). With the progress of science and technology, the degree of intelligence of artificial intelligence has gradually increased. The frequent appearance of artificial intelligence in our lives makes us realize that artificial intelligence should be taken seriously by human beings, because it has almost possessed one of the most important characteristics of human beings, that is, intelligence (Sadiku et al., 2020).

There is no denying that the risks brought by the development of science and technology are unavoidable for human beings. At this stage, artificial intelligence crimes are mainly concentrated in the fields of cybercrime, face recognition, medical treatment, automatic driving, etc., mainly manifested in criminals using artificial intelligence technology to invade computer systems, obtain citizens' personal information and illegally use it for personal gain. There are also criminals to steal patients' personal information, fraud or extortion (Caldwell et al., 2020). But artificial intelligence first appeared as a tool for humans, and its development should not deviate from the original intention of inventing artificial intelligence (Shahvaroughi Farahani & Ghasemi, 2024).

1.1. Research Objectives

The research objective of this paper aims to explore how to manage artificial intelligence technology through law in the context of artificial intelligence, to avoid the use of artificial intelligence by wrongdoers to commit crimes and to ensure the safety of network information.

2. Literature Review

2.1. Summary of Domestic Research

The development goal of artificial intelligence is to fully empower machines with the responsiveness of the human mind, that is, the ability to think, make decisions, make choices, and gain experience by completing work as required (Jeste et al., 2020). In 2023, seven departments including the Network Information Administration Office issued the Interim Management Measures for Generative Artificial Intelligence Services, which is the first normative policy for generative artificial intelligence industry in China. The method adheres to the principle of attaching equal importance to development and safety, promoting innovation and governing according to law, and takes effective measures to encourage the innovative development of generative artificial intelligence. The policy clearly encourages the innovative application of artificial intelligence technology in various industries and fields, generates positive and healthy quality content, explores and optimizes application scenarios, and builds an application ecosystem (Chen & Chen, 2024). In June 2023, the State Council announced that the Artificial General Intelligence Law would be included in the legislative agenda (Yang, 2024). In October 2023, China released the Global Artificial Intelligence Governance Initiative. The “Initiative” focuses on demonstrating China's valuable experience accumulated in the long-term practice of AI governance, and systematically expounds China's plan for AI governance from three aspects: AI development, security and governance (Gao & Yu, 2024). The Belt and Road Initiative is an important manifestation of China's active implementation of global development initiatives, global security initiatives, and global civilization initiatives. It is also a profound manifestation of China's profound insight and vision for the future global AI governance (Cheng & Zeng, 2023). In order to further enhance the awareness of the importance of science and technology ethics governance and effectively prevent science and technology ethics risks, China drafted the “Opinions on Strengthening Science and Technology Ethics Governance” in 2021. The opinions will help promote the unity of thought and consensus of the scientific and technological community and the whole society, further enhance the understanding of the importance of ethical governance of science and technology, effectively prevent ethical risks of science and technology, and accelerate the construction of an innovative country and a powerful country in science and technology (Ge & Li, 2022). Some scholars believe that the network security problems caused by artificial intelligence cannot be properly solved by relying on a single body of the government, and it is necessary to focus on the views of legal workers and generative artificial intelligence research and development experts, and realize the joint governance of multiple subjects to ensure its healthy development and use by people (Taeihagh, 2021). In the process of promoting the construction of an Internet governance system, some scholars have pointed out that multilateral participation, democratic consultation, transparency and fairness are the basic features of the new global Internet governance system, and have explicitly proposed that the principles of parallel rights and obligations, coordination between security and development, and sharing of peace and justice should be adhered to (O’Hara, 2021).

2.2. Summary of Foreign Studies

Compared with China, foreign artificial intelligence technology development is relatively advanced, the application field is more extensive, and the discussion of artificial intelligence in the academic circle is earlier and more in-depth. The National Artificial Intelligence Research and Development Strategic Plan released by the White House in 2016 became the world's first national-level artificial intelligence development strategy report, which focuses more on encouraging enterprise innovation and promoting industrial development (Bundy, 2017). In 2017, Harvard University's 'Artificial Intelligence and National Security' report pointed out that cyber weapons will be used more frequently in virtual warfare, and AI cyber weapons will be used maliciously if stolen or illegally copied. Increasing automation will increase unemployment and network attacks, which will affect political stability and national security (Burton & Soare, 2019). In 2018, the Center for Strategic and International Studies released 'Artificial Intelligence and National Security, the Importance of the Artificial Intelligence Ecosystem,' which believes that in areas such as cybersecurity or defence, humans may not be able to respond quickly, and the country that first masters the application of artificial intelligence will have a significant advantage (Moran et al., 2023). In 2019, the United States released a new version of the National Strategic Plan for Artificial Intelligence Research and Development, which lists problems that threaten artificial intelligence security such as algorithm confrontation, data poisoning, and model inversion, and requires that security issues be considered in the entire life cycle of artificial intelligence systems, covering initial design, data construction, evaluation, verification, deployment, operation and monitoring (Vogel et al., 2021).

At the end of October 2023, the America government signed the Executive Order on Safe, Reliable, and Trustworthy Artificial Intelligence. The executive order protects AI security and public privacy, prevents the exacerbation of inequity and discrimination caused by artificial intelligence, protects individual rights, and improves government control over artificial intelligence data and technology (Villasenor, 2023). At the first Global Summit on Artificial Intelligence Security in November 2023, more than 20 major countries and regions, including China, the United States and the United Kingdom, jointly signed the Bletchley Declaration, which is the world's first artificial intelligence security statemen (Patarlapati, 2023). The Artificial Intelligence Act, the world's first comprehensive law on artificial intelligence, was formally voted through by the European Parliament in March 2024, which classifies AI systems according to risk levels to define 'high risk' AI systems that pose a significant risk to human health and safety or fundamental rights. For certain AI systems, only minimal transparency obligations are proposed. The main objective of the law is to prevent any AI from posing a threat to health and safety and to protect fundamental rights and values (Cantero Gamito & Marsden, 2024).

The issue of network security in the era of artificial intelligence has become a theoretical hotspot for research. It is concluded through the study of AI governance at home and abroad that, first of all, the formulation of AI-related policies in China is mainly concentrated at the level of the State Council, on which other local departments make supplementary improvements and are responsible for specific implementation. However, in the actual promotion process, the regions may have inconsistent goals and non-sharing of resources in policy formulation and implementation, which to some extent affects the effective implementation and overall effect of policies. Secondly, due to the lagging nature of the law, there is still a large gap in the regulation of AI in China, and there is an urgent need to establish a more perfect and sound regulatory system in order to strengthen the

supervision and management of AI technologies and applications. Finally, compared with other major developed countries or regions, China's legislation on the regulation of science and technology ethics is lagging behind in general. Although there are documents such as the Opinions on Strengthening the Ethical Governance of Science and Technology as a support, the norms on ethical and moral issues are more extensive, and it is difficult to effectively regulate the ethical issues of AI in actual operation (Li, 2024). In order to cope with the various risks brought by AI, such as technology misuse, violation of ethics or discrimination, it is necessary to strengthen the risk prevention and control in the process of AI development in order to cope with the various challenges brought by the era of AI (Mou & Yang, 2023).

3. Research Methods

This article uses literature research method and case study method. Literature research method is a method to study a certain field by reviewing and analyzing the literature, through reading and studying the relevant literature, extracting the content with reference significance for this article, and improving the scientific of this article's research. The research literature and data on the legal subject status of artificial intelligence at home and abroad are checked and collected, and the relevant arguments and results are summarized, based on which the interpretation of artificial intelligence and network security is carried out (Snyder, 2019). The case study method is a method to study representative things in depth to obtain a general understanding. By searching for relevant popular events on the Internet and taking specific cases as the basis, we can derive the problems faced through the cases, analyze the problems in a comprehensive way, summarize our own views and give the corresponding basis (Rashid et al., 2019).

4. Results

4.1. Legislation to Regulate AI Crimes

In the digital age, in the face of the challenge of artificial intelligence crimes, it is necessary for China to establish a legal governance system on artificial intelligence to safeguard the healthy development of artificial intelligence technology and make it better available to people. First of all, the punishment requirements and standards for illegal and criminal acts should be clearly defined at the legal and policy level, and the abuse of artificial intelligence should be cracked down on to achieve legal compliance, and gradually improve the legal and regulatory system to ensure the sound development of AI. Secondly, in the process of continuously advancing AI technology, it is important to adequately protect the personal privacy rights of citizens. Finally, raise public awareness of AI crimes. Through publicity and popularization of artificial intelligence knowledge, to remind the public to pay attention to network security and prevent artificial intelligence crimes (Wang, 2021).

AI technology is humanoid and not really human, so do the laws that apply to humans properly apply to AI technology and its products themselves? The legal subject qualification of AI robots and the infringement caused by them have brought about gaps and gaps in the legal system. There are two points of view here. On the one hand, it is necessary to affirm the possibility of the application of laws to robots, open up the content applicable to artificial intelligence by modifying and improving the existing legal system, transform the traditional system of strengthening legal regulations, and establish a strict supervision and control policy system to form an institutional and law-based AI

governance system (Leenes & Lucivero, 2014). The affirmative view is that, firstly, artificial intelligence is similar to natural human beings, and when it develops to a certain extent, it can generate autonomous will to control its behaviour, which means that artificial intelligence already has the ability to assume criminal responsibility (Ellamey & Elwakad, 2023). Again, with the progress of science and the continuous development of neuroscience and other technologies, artificial intelligence will acquire human-like thoughts and generate will and morality through extensive learning and imitation of human beings. If the artificial intelligence has its own thoughts and morality, then it can logically have the qualification of criminal responsibility subject (Northoff et al., 2022). Finally, it took millions of years for apes to evolve into human beings, and human beings, as a kind of living creatures, have limitations in their evolutionary speed, whereas artificial intelligence is very rapid in its renewal (Li, 2020). Therefore, it is a trend for artificial intelligence to have the status of a subject. On the other hand, the legal applicability of robots is denied, and the legal rights and responsibilities of artificial intelligence are regulated from human beings by adopting necessary preventive systems to avoid the negative effects caused by the use of AI in the process of criminal governance (Kumar, 2023). The negative view is that the natural person, as a unique individual being in society, is neither reproducible nor comparable. If weakening the status of natural persons as subjects of criminal responsibility is to weaken human values to a certain extent, then it is unwise and an inappropriate abandonment of human values and human dignity, as well as a step backward in the development of human civilisation to date (Jeppsson, 2014). This paper argues that artificial intelligence is not a subject of law. Because artificial intelligence makes decisions based on algorithm procedures and results supported by data, it does not have rational perception of things as humans, nor does it have human morality and conscience. In addition, China's Civil Code has clearly established a three-way civil subject structure, that is, natural persons, legal persons, and unincorporated organizations, and there is no gap for artificial intelligence (Wang, 2022).

In the face of artificial intelligence crimes, for crimes that are as harmful to society as traditional crimes, to a certain extent, China's existing criminal legislation can still regulate them. However, in the face of criminal crimes with a high level of intelligence, the current criminal law either cannot achieve the effect of crime, responsibility and punishment, or it cannot be punished directly, so it appears that the heart does not follow the heart. Therefore, in the face of this dilemma, the criminal law community is required to respond actively to avoid the expansion of risks. Strengthen the theoretical research on artificial intelligence safety, and carry out legislative research on the “Artificial Intelligence Safety Law”. In order to ensure the safety and controllability of AI systems, the United States has issued consecutive reports in 2016, such as Preparing for the Future of Artificial Intelligence, National Strategic Plan for Artificial Intelligence Research and Development, Artificial Intelligence, Automation, and the Economy, which set out seven strategies for AI research and development in the United States (Bundy, 2017). To protect individuals from AI systems, four U.S. states have enacted legislation (Rachel, 2023). China has not yet issued special laws and regulations on artificial intelligence, and the provisions involving artificial intelligence are scattered at the overall level of the country and the policies and regulations of various fields of The State Council ministries and commissions. In terms of local legislation, Beijing, Shanghai, Hangzhou and other cities have successively issued local policies on artificial intelligence. However, the content does not make systematic provisions for the infringement liability of artificial intelligence (Veglianti et al., 2022). Artificial intelligence is the frontier product of the new era, and it is necessary to accelerate the legislative process and improve the artificial intelligence charge system to ensure network security (Chen, 2024). On the one hand, the Chinese law should consider adding

charges, accelerate the promotion of science and technology legislation, establish and improve data content management, artificial intelligence information protection mechanism, in view of the illegal application of artificial intelligence, we must first consider the applicability of civil law, administrative law and other departmental laws, and kill the risk of criminal crimes in the cradle in advance. On the other hand, the state should strengthen the responsibility regulation of artificial intelligence developers and designers from the legislative level, avoid taking "robots" as the subject of responsibility, and pay attention to cutting off data support for illegal applications of artificial intelligence with the individual information protection system to reduce the possibility of personal information being infringed.

4.2. The Protection of Personal Information

The excessive use of artificial intelligence exacerbates personal privacy security risks. The original intention of artificial intelligence application is to serve human society, national governance and national security. But today, the abuse and illegal use of artificial intelligence problems occur frequently, increasing cybersecurity risks. In July 2021, due to the illegal collection of personal information by the "Didi Chuxing" App, the Cyberspace Administration of China required the entire online App store to remove the "Didi Chuxing" app, and required it to comprehensively rectify and protect the security of user information. Didi app uses artificial intelligence and big data analysis technology to easily grasp user behaviour trends through user travel data (Shi, 2021). Artificial intelligence continuously obtains users' personal data and behavioural preferences through information recognition and super algorithms, and may outline users' thoughts and behavioural trends through algorithm analysis, which constitutes a violation of users' privacy and even personal safety.

Legislative protection is an important way to improve the legal protection of personal information in the age of artificial intelligence. China's current Personal Information Protection Law provides for some information collection or processing personnel to use artificial intelligence technology to infringe on personal information rights, but because of the lack of systematic and scattered in various chapters, it is urgent to improve the legislative system related to artificial intelligence personal information (Li et al., 2023). Because compared with the general network information infringement, the amount of personal information collected by artificial intelligence is large, more accurate and comprehensive, so if the problem of personal information infringement occurs, a large number of relevant information will be infringed. Therefore, while improving the basic legal provisions, it is also necessary to clarify specific personal information security protection measures and methods. For example, the law should clarify the concept of personal information in the age of artificial intelligence, specify the scope and ways of reasonable handling of personal information in the age of artificial intelligence, and propose special legal provisions on the protection and management of personal information security in artificial intelligence (Zhang, 2023). According to the Personal Information Protection Law, in the process of collection and use, information processors must not violate basic principles such as "legality, legitimacy and necessity", clearly inform the owner of the data collection, purpose of use, scope and way of use, and obtain the consent of the collected person before subsequent processing of the data. This regulation effectively maintains the security of personal information (Li et al., 2022). Therefore, by referring to the Personal Information Protection Law, we can improve the legislative protection system of artificial intelligence personal information, and put forward the collection standards and use standards of artificial intelligence data, so as to provide

guarantee for the maintenance of personal information security. Based on the needs of artificial intelligence security management and governance, special laws and regulations shall be formulated to set the ways of personal information security protection and infringement relief in the field of artificial intelligence.

4.3. Publicity and Education

With the rapid development of artificial intelligence technology, it is difficult to fully predict the social problems that may be caused by its extensive application. Improving the public's understanding of artificial intelligence technology can help strengthen the ability to identify and resist, and avoid the manipulation of public opinion by artificial intelligence technology to a certain extent, which helps to enhance national public opinion and social security (Oprea et al., 2024). To enhance public awareness of AI crimes, the core is to popularize AI knowledge through education and publicity, remind the public to pay attention to network security and prevent AI crimes, including adding relevant courses in school education, and carrying out science popularization activities in communities, enterprises and institutions. It is reported that China has opened artificial intelligence majors in several universities, which is an important part of improving the public's artificial intelligence literacy (Zhang et al., 2022). In addition, it is also necessary to strengthen network security education, improve the public's awareness of network security, and teach the public how to identify online fraud, protect personal information, and prevent network attacks.

Artificial intelligence crime is a worldwide problem. Therefore, it is necessary to exert the strength of the whole society to strengthen crime prevention, strengthen the publicity of community rule of law, and clarify the system norms. On the one hand, it is necessary to actively explore a new mode of crime prevention and control by mass prevention, give full play to the technological advantages of Internet enterprises, encourage the participation of the network masses, use it as an important force to prevent and combat artificial intelligence crimes, prevent the extension of crimes to virtual space, and cooperate with political and legal organs at all levels to jointly maintain the security of physical and virtual space. In the face of pictures and other information under the use of artificial intelligence and other related technologies, we must pay attention to identifying the source channels of information content as well as its objectivity, authenticity and accuracy, and remember not to blindly follow or blindly believe. On the other hand, we should promote the introduction of artificial intelligence technology into grassroots communities, so that ordinary people can prevent the technical risks generated by artificial intelligence technology, and explore a new crime prevention model combining artificial intelligence and community prevention. For example, the “community correction supervision robot” in Chengdu uses feature extraction technology and computer vision to collect the biometric characteristics of residents in the jurisdiction and identify the fingerprints, voice prints, portraits and chips of different individuals, effectively strengthening the daily management, tracking and monitoring, learning and training of high-risk groups in the community and the whole process of psychological assessment. This artificial intelligence model is a good example of the combination of AI and crime prevention (Dimovski & Grujić, 2024).

5. Conclusion

Network security has entered the era of artificial intelligence, the first priority of development is network security (Zhao, 2024). General Secretary Xi proposed that

artificial intelligence should not only focus on technological development, but also take people as the bottom line, effectively protect the interests of users, and for the heavy risks it faces in the development process, it should be correctly screened to do a good job of prevention in advance, and do a good job of solving the aftermath of the risk when it occurs (Chen, 2023). In the report of the 20th National Congress, China has both summarized the historic achievements about the Internet and looked forward to the grand blueprint for a new era of network power. The Ministry of Justice has also clearly put forward the requirements for the construction of the "digital rule of law". Thus, how to build the digital rule of law and how to guarantee the legitimate exercise of digital rights of individuals has become an important issue in the construction of digital China and a smart society (Liu, 2024). At present, China has issued a number of policy documents on network security governance, but the provisions are too simple and do not make it clear that the relevant provisions are applicable to the development stage of artificial intelligence. Therefore, China should continuously improve the relevant laws and regulations to regulate the development and application of AI, so as to effectively avoid the risk of AI in the process of development and application, and effectively resolve and eliminate the conflicts and disputes that may arise. At the same time, by strengthening legislation and improving the technical support system, we can ultimately achieve the purpose of promoting China's economic development and social stability.

The development of artificial intelligence technology has indeed brought challenges to traditional legal theories, but the law must not threaten human development under any pretext, and the development and formulation of law must always adhere to the "human-centered" principle, and artificial intelligence should be limited to the object. The rapid development of artificial intelligence technology is a double-edged sword, bringing opportunities and changes as well as challenges and risks. In the future, the intelligent society based on artificial intelligence should be guided by further theoretical research and relevant policies. Legislation should clarify the legal object status of artificial intelligence as soon as possible, and build a corresponding normative system and strict supervision system to ensure the realization of the legal object status of artificial intelligence while fully considering the particularity of artificial intelligence (Khalifa & Sabry, 2024), so as to ensure that artificial intelligence is always a powerful tool for human beings.

At present, the development of artificial intelligence has become an irreversible trend of The Times (Wang & Wu, 2024). While artificial intelligence promotes social progress, its potential risks cannot be ignored. The correct use of artificial intelligence will undoubtedly bring great convenience to mankind, but if artificial intelligence is abused, it may seriously disrupt the social order. Maintaining network security is a common obligation of the whole society, including the government, enterprises, social organisations and netizens, as well as the common responsibility of all parties, including the government, enterprises, social organisations and netizens. In order to effectively support the progress and innovative application of artificial intelligence technology, it is necessary to improve the relevant regulations and systems as soon as possible, and do a good job of risk assessment and safety management of the relevant technologies, so that the progress and application of artificial intelligence technology can better support the construction of a digital society, and so that mankind can better benefit from the progress of artificial intelligence.

Ethics Approval and Consent to Participate

Not applicable.

Acknowledgement

I sincerely thank my two supervisors for their guidance and my parents for their encouragement and unwavering support during this journey.

Funding

This study received no funding.

Conflict of Interest

The authors reported no conflicts of interest for this work and declare that there is no potential conflict of interest with respect to the research, authorship, or publication of this article.

References

Abdel Razek, R. (2020). The Effect of Artificial Intelligence on Cybercrime. *Humanities and Management Sciences - Scientific Journal of King Faisal University*, 1–8. https://doi.org/10.37575/h/mng/2417

Al Qatawneh, I. S., Moussa, A. F., Haswa, M., Jaffal, Z., & Barafi, J. (2023). Artificial Intelligence Crimes. *Academic Journal of Interdisciplinary Studies*, *12*(1), 143. https://doi.org/10.36941/ajis-2023-0012

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/ACCESS.2022.3191790

Bokhari, S. A. A., & Myeong, S. (2023). The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. *IEEE Access*, *11*, 69783–69797. https://doi.org/10.1109/ACCESS.2023.3293480

Bundy, A. (2017). Preparing for the future of Artificial Intelligence. *AI & SOCIETY*, *32*(2), 285–287. https://doi.org/10.1007/s00146-016-0685-0

Burton, J., & Soare, S. R. (2019). Understanding the Strategic Implications of the Weaponization of Artificial Intelligence. *2019 11th International Conference on Cyber Conflict (CyCon)*, 1–17. https://doi.org/10.23919/CYCON.2019.8756866

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 14. https://doi.org/10.1186/s40163-020-00123-8

Cantero Gamito, M., & Marsden, C. T. (2024). Artificial intelligence co-regulation? The role of standards in the EU AI Act. *International Journal of Law and Information Technology*, *32*(1). https://doi.org/10.1093/ijlit/eaae011

Chen, B. (2024). Analysis of the Difference between the Liability for Infringement of Artificial Intelligence Products and the Liability for Subsequent Observation Obligations. *Journal of Economics and Law*, *1*(2), 83–87. https://doi.org/10.62517/jel.202414211

Chen, B., & Chen, J. (2024). China's Legal Practices Concerning Challenges of Artificial General Intelligence. *Laws*, *13*(5), 60. https://doi.org/10.3390/laws13050060

Chen, L., Chen, P., & Lin, Z. (2020). Artificial Intelligence in Education: A Review. *IEEE Access*, *8*, 75264–75278. https://doi.org/10.1109/ACCESS.2020.2988510

Chen, Q. (2023). Risk Reflection and Correction Path of Artificial Intelligence from the Perspective of Law. *Open Journal of Legal Science*, *11*(06), 6460–6464. https://doi.org/10.12677/OJLS.2023.116927

Cheng, J., & Zeng, J. (2023). Shaping AI's Future? China in Global AI Governance. *Journal of Contemporary China*, *32*(143), 794–810. https://doi.org/10.1080/10670564.2022.2107391

Dimovski, D., & Grujić, Z. (2024). Possibilities of using artificial intelligence in crime prevention. *Bezbednost, Beograd*, *66*(2), 67–88. https://doi.org/10.5937/bezbednost2402067D

Ellamey, Y., & Elwakad, A. (2023). The criminal responsibility of artificial intelligence systems: A prospective analytical study. *Corporate Law and Governance Review*, *5*(1), 92–100. https://doi.org/10.22495/clgrv5i1p8

Gao, D., & Yu, D. (2024). Challenges and Cracks: Ethical Issues in the Development of Artificial Intelligence. *Science, Technology and Society*, *29*(3), 415–434. https://doi.org/10.1177/09717218241246372

Ge, H., & Li, Z. (2022). Integrating ethical concepts into scientific and technological development. *Cultures of Science*, *5*(3), 131–133. https://doi.org/10.1177/20966083221118115

Goralski, M. A., & Tan, T. K. (2020). Artificial intelligence and sustainable development. *The International Journal of Management Education*, *18*(1), 100330. https://doi.org/10.1016/j.ijme.2019.100330

Jeppsson, S. M. I. (2014). Responsibility problems for criminal justice. *Frontiers in Psychology*, *5*. https://doi.org/10.3389/fpsyg.2014.00821

Jeste, D. V., Graham, S. A., Nguyen, T. T., Depp, C. A., Lee, E. E., & Kim, H.-C. (2020). Beyond artificial intelligence: exploring artificial wisdom. *International Psychogeriatrics*, *32*(8), 993–1001. https://doi.org/10.1017/S1041610220000927

Khalifa, M., & Sabry, M. (2024). The Challenges of The Artificial Intelligence of Law in The Context of Technological Development. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, 1–5. https://doi.org/10.1109/ICETSIS61505.2024.10459547

Krysiuk, C. (2022). Autonomous cars, development of modern transport technology. *Journal of Civil Engineering and Transport*, *3*(1), 17–27. https://doi.org/10.24136/tren.2021.002

Kumar, P. (2023). Determination of Civil and Criminal liability of Artificial intelligence. *DME Journal of Law*, *4*(01), 48–55. https://doi.org/10.53361/dmejl.v4i01.06

Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*, *6*(2), 193–220. https://doi.org/10.5235/17579961.6.2.193

Li, Q., Jiang, T., & Fan, X. (2023). Examining Sensitive Personal Information Protection in China: Framework, Obstacles, and Solutions. *Information & Culture*, *58*(3), 247–273. https://doi.org/10.7560/IC58302

Li, W. (2020). On preventive criminal law legislation in the age of artificial intelligence. *Journal of Dalian University of Technology (Social Science Edition)*, *41*(5), 96–103. https://doi.org/10.19525/j.issn1008-407x.2020.05.012

Li, X., Cong, Y., & Liu, R. (2022). Research under China's personal information law. *Science*, *378*(6621), 713–715. https://doi.org/10.1126/science.abq7402

Li, Y. (2024). Prevention and Regulation of Artificial Intelligence Risks in the Context of Overall National Security Outlook. *Dispute Settlement*, *10*(05), 175–180. https://doi.org/10.12677/ds.2024.105268

Liu, M. (2024). Personal Data Risks of Generative Artificial Intelligence and Its Legal Regulation. *Open Journal of Legal Science*, *12*(01), 231–241. https://doi.org/10.12677/OJLS.2024.121034

Mikhailov, M., & Kokodey, T. (2023). Risks of the Malicious Use of Artificial Intelligence and the Possibility of Minimizing Them. *Russian Journal of Criminology*, *17*(5), 452–461. https://doi.org/10.17150/2500-4255.2023.17(5).452-461

Moran, C. R., Burton, J., & Christou, G. (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, *8*(2). https://doi.org/10.1093/jogss/ogad005

Mou, B., & Yang, X. (2023). Analysis of the Role of Compliance Plan in AI Criminal Risk Prevention-Take AI Criminal Risk in Network Communication as Example. *International Journal of Communication Networks and Information Security (IJCNIS)*, *15*(3), 154–167. https://doi.org/10.17762/ijcnis.v15i3.6242

Neiroukh, S., Emeagwali, O. L., & Aljuhmani, H. Y. (2024). Artificial intelligence capability and organizational performance: unraveling the mediating mechanisms of decision-making processes. *Management Decision*. https://doi.org/10.1108/MD-10-2023-1946

Northoff, G., Fraser, M., Griffiths, J., Pinotsis, D. A., Panangaden, P., Moran, R., & Friston, K. (2022). Augmenting Human Selves Through Artificial Agents – Lessons From the Brain. *Frontiers in Computational Neuroscience*, *16*. https://doi.org/10.3389/fncom.2022.892354

O'Hara, K. (2021). Governing the Internet. In *Four Internets* (pp. 36–50). Oxford University Press New York. https://doi.org/10.1093/oso/9780197523681.003.0003

Oprea, S., Nica, I., Bâra, A., & Georgescu, I. (2024). Are skepticism and moderation dominating attitudes toward AI-based technologies? *The American Journal of Economics and Sociology*, *83*(3), 567–607. https://doi.org/10.1111/ajes.12565

Patarlapati, N. (2023). Unraveling the Bletchley Declaration - A Sociological Analysis of Artificial Intelligence. *International Journal of Science and Research (IJSR)*, *12*(11), 759–762. https://doi.org/10.21275/SR231105111311

Rachel, W. (2023, December 6). Artificial intelligence in the States: Emerging legislation. *The Council of State Governments*. https://www.csg.org/2023/12/06/artificial-intelligence-in-the-states-emerging-legislation/

Raimundo, R., & Rosário, A. (2021). The Impact of Artificial Intelligence on Data System Security: A Literature Review. *Sensors*, *21*(21), 7029. https://doi.org/10.3390/s21217029

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case Study Method: A Step-by-Step Guide for Business Researchers. *International Journal of Qualitative Methods*, *18*. https://doi.org/10.1177/1609406919862424

Sadiku, M. N. O., Ashaolu, T. J., & Musa, S. M. (2020). Essence of Human Intelligence. *International Journal Of Scientific Advances*, *1*(1). https://doi.org/10.51542/ijscia.v1i1.7

Secinaro, S., Calandra, D., Secinaro, A., Muthurangu, V., & Biancone, P. (2021). The role of artificial intelligence in healthcare: a structured literature review. *BMC Medical Informatics and Decision Making*, *21*(1), 125. https://doi.org/10.1186/s12911-021-01488-9

Shahvaroughi Farahani, M., & Ghasemi, G. (2024). Will artificial intelligence threaten humanity? *Sustainable Economies, 2*(2), 65. https://doi.org/10.62617/se.v2i2.65

Shi, F. (2021). Citizen Data Security Protection from the Perspective of "DiDi" Security Review. *Open Journal of Legal Science*, *09*(06), 663–669. https://doi.org/10.12677/OJLS.2021.96095

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Solov'ev, V. (2023). Criminological Risks Of The Use Of Artificial Intelligence Technology In Illegal Drug Trafficking. *Scientific Notes of V. I. Vernadsky Crimean Federal University. Juridical Science*, *7*(4), 349–360. https://doi.org/10.29039/2413-1733-2021-7-4-349-360

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137–157. https://doi.org/10.1080/14494035.2021.1928377

Veglianti, E., Li, Y., Magnaghi, E., & De Marco, M. (2022). Understanding artificial intelligence: insights on China. *Journal of Asia Business Studies*, *16*(2), 324–339. https://doi.org/10.1108/JABS-10-2020-0391

Villasenor, J. (2023). How the White House's AI Executive Order Could Increase U.S. Cyber Vulnerabilities. *International Journal of Innovative Research in Education, Technology and Social Strategies*, *10*(2), 147–149. https://doi.org/10.48028/iiprds/ijiretss.v10.i2.12

Vogel, K. M., Reid, G., Kampe, C., & Jones, P. (2021). The impact of AI on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability, and management. *Intelligence and National Security*, *36*(6), 827–848. https://doi.org/10.1080/02684527.2021.1946952

Wang, L. (2021). Global network security governance trend and China's practice. *International Cybersecurity Law Review*, *2*(1), 93–112. https://doi.org/10.1365/s43439-021-00025-8

Wang, Q. (2022). Der Allgemeine Teil des neuen chinesischen Zivilgesetzbuchs im Vergleich zum deutschen BGB (Teil 2): Eine rechtswissenschaftliche und -terminologische Untersuchung der Zivilrechts-, Rechtsgeschäfts- und Zivilhaftungsregelungen. *European Review of Private Law*, *30*(Issue 6), 1089–1122. https://doi.org/10.54648/ERPL2022041

Wang, X., & Wu, Y. C. (2024). Balancing Innovation and Regulation in the Age of Generative Artificial Intelligence. *Journal of Information Policy*, *14*. https://doi.org/10.5325/jinfopoli.14.2024.0012

Wang, Y. (2024). The Role of Artificial Intelligence Technology in Promoting Socio-Economic Development. *Journal of Progress in Engineering and Physical Science*, *3*(3), 85–93. https://doi.org/10.56397/JPEPS.2024.09.10

Yadlapati, V. S. A., Kethar, J., & Gochhayat, Dr. S. P. (2024). Artificial Intelligence's Effect on Cybersecurity. *Journal of Student Research*, *13*(2). https://doi.org/10.47611/jsrhs.v13i2.6613

Yang, T. (2024). Legal Regulation of Generative Artificial Intelligence in China. *Law & Digital Technologies*, *4*(1), 25. https://doi.org/10.18254/S278229070031786-0

Zhang, C., Wang, J., Dong, Z., & Wang, L. (2022). Study on the Construction Mode of Curriculum System of Intelligent Science and Technology under the New Engineering Discipline. *International Journal of Education and Humanities*, *4*(3), 64–66. https://doi.org/10.54097/ijeh.v4i3.1672

Zhang, Y. (2023). Research on Legal Protection of Data Privacy in the Age of Intelligent Media. *Open Journal of Legal Science*, *11*(06), 5512–5518. https://doi.org/10.12677/OJLS.2023.116788

Zhao, C. (2024). The role and challenge analysis of artificial intelligence in computer network security. *Electronic Communications and Computer Science*, *6*(7), 31–33. https://doi.org/10.37155/2717-5170-0607-11