RISKS OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY CRIMES

ALI KABOL FAGHIRI,
Department of Graduate Studies, Imam Malik College, Academic City, Dubai, United Arab Emirates,

Abstract

Information technology and communication have brought about a revolution that affects the economic, political, social, and cultural sectors, just like previous revolutions. This revolution relies on information, which is the basis of human knowledge. Modern information technologies allow for monitoring, processing, and distributing this information in various written, visual, and auditory forms, overcoming the obstacle of information volume and reducing the time required for distribution. This technology has led to a new way of working that facilitated the emergence of a new concept, the concept of the information society, which aims to extensively and optimally utilize information in various aspects of life. This society is considered the result of the technological convergence between informatics and communication technologies. It has opened doors for interaction among several global operators who exchange information through the Internet network.Through this wide openness in the field of communication and information transfer, it is necessary for us to know how to safeguard this transferred information from one party to another, and this is where the concept and term "Information Security" originated.The definition of security largely depends on the context, as the term "Security" refers to a wide range of areas within and outside the field of information technology. For example, we may talk about security when describing preventive measures on public roads or when reviewing a new computer system that has high immunity against software viruses. Several systems have been developed to address different aspects of the security concept. In the race between artificial intelligence and information security, researchers are questioning the risks that artificial intelligence can cause in information security crimes.

1. INTRODUCTION

Today, the world stands on the threshold of a new revolution that will inevitably change the shape of human life, and this revolution is driven by artificial intelligence. It is a comprehensive revolution on various securities, economic, social, and other levels, due to the multiple and increasing applications of artificial intelligence, which are difficult to quantify (Jeong, D., 2020). Therefore, we find that it intersects with all human fields. It is astonishing that there has been no objective understanding or evaluation of the consequences of these applications, especially considering the division between civilian and military applications and the different impacts they have in each sector. It can be said that some civilian applications of artificial intelligence, which are supposed to make individuals' lives easier and faster, can be employed for spying on and tracking them. The topic was chosen based on the contemporary reality in which artificial intelligence poses significant risks to all aspects of human life. It can interfere in both small and large matters and can potentially lead to committing major crimes, especially those related to information security (King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L., 2020). Therefore, the choice was made to study and research this topic. In this research, the researcher followed a descriptive and analytical approach by discussing ideas related to the topic, measuring them, extracting important findings and legal principles from them, and providing an accurate description of them. The researcher also adopted a comparative approach when comparing different legislations, and conducted research on the meanings of some terms related to the study, examining them within the framework of laws and the opinions of jurists. In this paper, the concept of artificial intelligence and its applications will be explained, followed by a discussion of its uses. At the end of the paper, the concepts of cybercrime and information security will be defined.

Artificial intelligence can be defined as a branch of computer science that deals with simulating human behavior in machines. It is a science focused on creating computer devices and programs capable of thinking in the same way as the human brain, learning like humans, and making decisions like humans. Artificial intelligence is also defined as the study and design of smart systems that can perceive their environment and take actions to increase their chances of success. John McCarthy, who coined this term in 1955, defines it as the science and engineering of making intelligent machines. This is the intelligence exhibited by machines and software that imitate human mental abilities and patterns of work, such as the ability to learn, infer, and react to situations that have not been programmed into the machine. This is a field of study that focuses on creating computers and programs capable of exhibiting intelligent behavior. Similarly, artificial intelligence is defined as the simulation of human intelligence and understanding by creating computer programs capable of mimicking intelligent human behavior. Artificial intelligence is currently present in various aspects of our lives, including self-driving cars, drones, translation software, and many other applications (Cheatham, B., Javanmardian, K., & Samandari, H., 2019). One of the skills of artificial intelligence is its ability to recognize images, shapes, and different sounds and match them with databases and expert systems to identify the owner of the image or sound based on the information stored in various databases. Researchers believe that this skill is highly suitable for robots to perform actions related to crime prevention, crime control during the commission of a crime, or searching for suspects in a specific crime for interrogation and determining their level of involvement in the crime.

2. LITERATURE REVIEW

2.1 The use of artificial intelligence in Crime Prevention

In t1.his research, an important legal question is raised: Can artificial intelligence be used programmatically and scientifically to contribute to criminal justice, including measures taken before the commission of a crime, by activating effective means of crime prevention? It is worth mentioning that with the help of artificial intelligence, it is possible to gather a lot of information about crimes, their status, legal adaptation, and determining priorities and social information. It can be used to recommend specific judgments and identify perpetrators in committed crimes. Artificial intelligence can also identify individuals at risk through algorithms and large databases within artificial intelligence (Butkar, M. U. D., & Waghmare, M. J., 2023).

2.2 Using Artificial Intelligence in Crime Investigation

Can artificial intelligence be used to identify the perpetrator or criminals after a crime have occurred? Can AI track and catch criminals? These assumptions need to be explored and clarified from a legal perspective . This is important to determine the extent to which AI can contribute to detecting crimes if they are committed in front of a robot (guard), where it can see the culprit and apprehend them. If the robot is not present at the time of the crime, can artificial intelligence, through data analysis, discover the perpetrator? It does so by utilizing databases and knowledge management that are programmed into it (Brahan, J. W., Lam, K. P., Chan, H., & Leung, W., 1998).

2.3 Using Artificial Intelligence to Determine the Criminal's Identity

Artificial intelligence can also benefit law enforcement by providing a scientific perspective and evidence, particularly in DNA analysis. This has had an unprecedented impact on detecting criminals. Judicial systems have benefited in recent decades from analyzing biological substances such as blood, saliva, semen, and skin cells, which can be spread through contact during the commission of different crimes (Hallevy, G., 2010). With the advancement of DNA analysis technology using artificial intelligence, forensic scientists have been able to detect crimes and provide evidence resulting from DNA analysis, especially in cases of sexual assaults. Additionally, murder cases can now be sent to the laboratory for necessary DNA analysis, enabling the identification of perpetrators through the use of AI applications in this field.

2.4 Using artificial neural networks to predict criminal risk

Artificial neural networks can enable employees to predict criminal risk by unknown criminals. They have found a way to bypass alert triggers in rule-based security systems.

These artificial neural networks connect millions of data points from databases that appear to be unrelated. They include everything from social media posts to internet protocol addresses used in Wi-Fi networks and other data that is programmatically linked through the knowledge bases of artificial intelligence. They can also form self-opinions that enable them to make appropriate decisions and identify patterns that should be used (Walczak, S., 2021).

2.5 Concept of cybercrime and information security

Crime is mentioned in the language with two meanings: the first is guilt, we say a crime, and a criminal with one meaning. The second is felony, as they say, a crime to them and against them. Committing a felony: A crime means if its guilt is great, meaning sin. The term "crime" is one of the words used by jurists to describe some legal boundaries, such as the crime of fornication, the crime of defamation, the crime of murder. However, after investigation and research, it was noticed that the use of the term "felony" is more common instead of the crime (Hartel, P. H., Junger, M., & Wieringa, R. J., 2010). This may be due to their satisfaction with it, considering it the intended meaning of the crime. Every unlawful human behavior, whether positive or negative, intentional or unintentional, is punishable by criminal law.

2.6 The definition of crime in the law includes the following

First: Crime is an unlawful human behavior that infringes upon the rights and interests that should be protected and maintained for individuals and communities. Second: The emergence of a crime through the commission of an act that is prohibited, or the omission of an act that is required. Third: The existence of a legislative legal text that imposes a punishment on the act or omission that constitutes the crime, proportionate to the penalty deserved for the crime (Friedrichs, D. O., 2015). This field of security was known until the late 1970s as Communication Security (COMSEC), which was defined by the recommendations of information and communication systems security for the National Security Agency in the United States as follows: The standards and procedures taken to prevent unauthorized access to information through communications and to ensure the authenticity and integrity of these communications". The specific activities of communication security included four parts: Crypto security, Transmission Security, Emission Security, and Physical Security. The definition of communication security also included two properties related to the subject of this unit: confidentiality and identity verification.

Integrity reflects the quality of any information system in terms of the correctness and reliability of the operating system, the logical integration of equipment and software that provides protection mechanisms, and the compatibility of the data structure with stored data. Reliable access to data and information services when needed by authorized individuals. Later, in the 1990s, the concepts of security (telecommunications security and computer security) were integrated to form what is now known as Information Systems Security (INFOSEC). The concept of information systems security includes the four previously known characteristics of telecommunications security and computer security: confidentiality, authentication, integrity, and availability, as well as a new feature: non-repudiation.

2.7 Artificial Intelligence's Responsibility for Information Security Crimes

In the second section, civil responsibility is explained in (article 1), followed by legal responsibility in (article 2), and then criminal responsibility in (article 3). Civil liability, in general, refers to accountability and taking responsibility for one's actions. This liability can be moral or legal, which is the focus of our discussion here. Legal liability occurs when there is a legal violation or a breach of legal obligation, and the offender is subject to legal punishment. It is also divided into criminal liability and civil liability according to the legal system (Hallevy, G., 2010). This division is based on the type of error that resulted in this liability and the resulting punishment. This is because legal punishment, which requires accountability, may be a penalty when it is related to the interests of society. Thus, the liability in this case is criminal. On the other hand, it may require compensation when it is related to individual interests, and thus the liability is civil.

Civil liability arises when disciplinary or legal punishment requires compensation, which is the subject of discussion here. Furthermore, compensating for damages is considered one of the essential functions of civil liability, which is achieved through compensation. Therefore, civil liability is the obligation to pay compensation, which falls on the responsible party for the benefit of the affected party. It is also a legal situation for a person who commits an error resulting in harm to the interests of others. This liability is divided into two parts, namely, contractual liability and tort liability. Contractual liability, being a type of civil liability that depends on the existence of a valid contract that must be executed, is a penalty for failure to perform the contractual obligation or to be performed in a certain way that harms the customer. This liability is realized if he refrains from performing the contractual obligation imposed on him or its execution in a certain way that leads to harm to the customer. This liability is defined as a penalty for the contract. Liability for damage resulting from negligence is established if there are three basic elements represented by error, damage and the causal relationship between them, and is known as the elements of individual liability for damage resulting from his negligence.

2.8 Criminal liability of a robot under artificial intelligence

The crimes of artificial intelligence are the crimes of the near future, if some of them have not started now, the technological development during the past years, which has accelerated its pace in the current period, has helped the emergence of these crimes, as the advanced programming of some machines powered by artificial intelligence has given capabilities of up to the severity to build a subjective experience that enables them to make individual decisions in any situations they face, such as human. There are many and varied artificial intelligence crimes, and every day a new type and classification of those crimes appears, but what is currently of interest is the classification of artificial intelligence crimes in reality and the virtual world, and one of the most famous criminal crimes committed by self-driving cars belonging to the Uber company was a woman on the road, which led to her death from her injuries, and in 1981 a Japanese employee at a motorcycle factory, aged 37, was killed by one of the robots working near him, the robot was identified incorrectly, the employee felt a threat to his mission, and he figured that the most effective way to eliminate this threat he pushed him to a nearby operating machine using his extremely powerful hydraulic arm, and the robot smashed the sudden worker in the operation of the machine, which killed him instantly, and then resumed his tasks without anyone interfering with his task (Hallevy, G., 2010).

2.9 Opposition to the criminal responsibility of the robot

Traditionally, only a human being is asked, and perhaps this rule seems the most logical and most consistent with the concept of crime and the social function of criminal law as well, a crime is committed only by a human being, and this is self-evident because the latter has the will required to create the behavior that constitutes the material pillar of the crime, which is also the strength of the moral pillar, and therefore there is no blame on the one who committed a crime without his will, because the law does not count unless she is conscious aware of what she is doing, so it is difficult to recognize the criminal responsibility of the machine (robot). The purpose of the Penal Code is to activate a set of commands and prohibitions that need to be understood, as well as the purposes of punishment, which sees everyone badly the consequence of whoever commits the crime again; these goals can only be achieved by a natural person and not by a machine (robot). Contemporary trend: calls for the need to establish the appropriate criminal liability of the machine (robot). Today, criminal liability is no longer derived from concepts related to the supernatural and nature, but from psychological, social, and utilitarian considerations. From the perspective of the contemporary philosophy of criminal legislation, the objective of determining criminal liability remains to resist the crime committed and prevent the commission of more crimes by pursuing an objective criminal policy aimed at protecting society so that every human being can find safety and tranquility (Pagallo, U., 2013).

According to Yas, N., & Hareb Alkuwaiti, H. H. (2021), Since the traditional trend has ended up not recognizing the criminal responsibility of the machine (robot), another trend has begun on the horizon that decides on the need to hold the robot criminally accountable. Taking into account the logic of traditional jurisprudence on its launch means that it is also impossible to hold a moral person accountable because he is not a human being, which contradicts the modern legislative policy embraced by most countries of the world.

2.10 criminal liability and the dangers of artificial intelligence

The term responsibility is used to denote the meaning of the obligation of a person to bear the consequences of his behavior that he committed a violation of legal norms or rules, and the concept of responsibility in general applies with the concept of accounting and the person's responsibility for his actions and actions, the behavior can be positive or negative contrary to the rules of liability here is a legal liability and in this case a legal penalty determined by the public authority in the state shall be imposed (Yas, N., Al Qaruty, R., Hadi, S. A., & AlAdeedi, A., 2023). It is worth noting that the moral circle is broader than the legal circle, because the former expands to include human behavior towards his Lord, towards himself and towards others, that is, it includes all aspects of his life, it commands the good and looks at the intentions and intentions of man, it works to approve him on what these intentions and intentions are heading towards. As for the circle of law, it is much narrower, because it is limited to regulating a person's relationship with others or regulating his life from a social point of view, since the framework of this relationship does not extend the perimeter of the circle of law only to what takes the form of concrete external activity, because the law is not held accountable for intentions only, it is held accountable for external actions that appear into existence. That is, moral responsibility falls within the circle of morality, while legal responsibility falls within the circle of law, and the latter regulates actions and generally carries a legal obligation or sanction, as a result of behavior or conduct for which the law entails its effects and certain sanctions (Yas, N., Dafri, W., & Rezaei Gashti, Z., 2022).

The steadily increasing complexity of attacks on information security: Virus attacks on corporate websites have increased, and have turned from annoying cases to harmful to the operations of these companies, and viruses previously infected limited devices, but today their effects are reflected on the majority of devices connected to the web, inflicting significant material losses on companies. This problem cannot be overlooked, as these attacks cost billions of dollars every year, for example, the love bug virus cost 75.8 billion dollars in 2005. The steadily increasing complexity of attacks on information security: Virus attacks on corporate websites have increased, and have turned from annoying cases to harmful to the operations of these companies, and viruses previously infected limited devices, but today their effects are reflected on the majority of devices connected to the web, inflicting significant material losses on companies. This problem cannot be overlooked, as these attacks cost billions of dollars every year, for example, the love bug virus cost 75.8 billion dollars in 2005 (Yas, N., 2021). The theft of private information is also considered an important information security risk, when individual property rights exist in electronic form and stored on a computer, it is easy to steal them, and this causes great numbers and a great dilemma to preserve the secrets of commercial and industrial companies (Khadragy elt., 2022).

2.11 Government legislation and industrial regulations:

The increasing reliance on the internet and the information security incidents that have increased in recent years have prompted governments to introduce additional legislation to regulate the systems environment, and this legislation included several axes, such as private customer information, and legislation specific to certain professions such as health and financial services (Yas, H., Mardani, A., & Alfarttoosi, A., 2020). Therefore, it is not important to apply the laws and legislations related to information security in the country where the companies are located, but all the legislation and binding laws must be applied in the countries where the customers of those companies are located. In short, companies are obliged to apply the legislation of their own country and the legislation of other countries of the world where their customers are located.

2.12 Mobile workforce and wireless computing

Mobile computers have affected the daily lifestyle, wireless communication has enabled employees and customers to reduce dependence on the regular phone for communication, searching for the nearest phone booth or going to the office to check e-mail has become in decline, especially after the advent of mobile phone, internet browsing and e-mail via wirelessly connected mobile devices. In the past, there was a computer in the office for work purposes, and another personal computer at home for personal business, and there is a clear dividing line between the two, but with the development and availability of mobile devices, separation between them has become impossible. The protection of office devices has become centralized through the company, but it is difficult to protect, monitor and control mobile devices that may contain sensitive and important information for the company, which has resulted in new methods and practices to ensure the security of information on these mobile devices, which are inherently more complex and difficult to protect compared to stationary desktop devices (Yas, H., Alkaabi, A., ALBaloushi, N. A., Al Adeedi, A., & Streimikiene, D., 2023).The other dimension is the emergence of new protocols with standard specifications that facilitate the communication of mobile devices with each other, which facilitated communication between individuals ' mobile devices such as: mobile devices, and laptops. And these protocols are such as: (Bluetooth, WiFi... This is a disaster for information security officials, especially if these devices contain sensitive information for the company, with which it is necessary to protect these mobile devices similar to the protection of office devices in the company.

2.13 The seriousness of aggression to the information environment

Cybercrimes have become a serious threat and challenge to national and international security as the escalating criminal phenomenon in light of the Computer Information Revolution, and the lack of many countries of the world of special laws to confront these destructive crimes in the vast cyberspace, with the presence of organized gangs constantly developing themselves to achieve their subversive goals for the economies of countries and the penetration of security systems and websites, as well as espionage, eavesdropping and snooping, or with the intent of fraud and stealing bank balances and currencies by penetrating the networks of banks and large financial institutions, especially in light of the expansion of electronic commerce, and trained terrorist groups are able to exploit the International Information Network to support their terrorist activities and spread its destructive ideas, or spying on security operations and major military, industrial and commercial institutions and stealing their secrets.

There are cybercrimes carried out by (mafia) drug dealers, weapons and human trafficking, organ sales and smuggling of migrants, money laundering crimes, public morality crimes and pornographic sites, crimes of swearing, libel, defamation, extortion and voyeurism, the establishment of sites to spread destructive ideas and contempt for religions, crimes of destroying databases and information and launching viruses, and many other crimes due to the amazing development in the world of communications and information, and this prompted those concerned with the information environment the establishment of computer programs under the name of (internet police) whose purpose is to block pornographic sites, or any other sites that do not fit the ethics of society, as well as the development of a special legal system for the internet and informatics and teaching it in law schools, as well as work to encourage research and specialized studies on the legal handling of this phenomenon (Yas, H., Jusoh, A., Nor, K. M., Alkaabi, A., Jovovic, N., & Delibasic, M., 2022).

2.14 Electronic piracy: Electronic piracy

There is no doubt that the internet is the pinnacle of human creativity in the field of communication, exchange and availability of information in the current era, today each of us can wander around the different countries of the world without moving from his place.

All these possibilities offered by the network are not without a dark side that many users of this technology are unaware (Taylor, A., 2006). The process of browsing global information resources on the web can leave traces that allow internet hackers to track the trace of all operations that the beneficiary of network services has performed so that they can tamper with his information and try to destroy or distort it. Electronic piracy is an act similar to stealing a product from the shelves of some stores, it is theft or distribution without authorization, or it is the use of a substance that has intellectual property rights, as this phenomenon has spread to all countries of the world, as hackers of information today can access the computers of the White House and the American Research Center "NASA" and this is only with the availability of a computer and a modem "Modem", and an American University had to pay a phone bill estimated at: 200,000 dollars, more than half of which for hacked communications (Panas, E. E., & Ninni, V. E., 2011).

2.15 Future prospects of the impact of artificial intelligence technologies on information organizations

Information security and other organizations working in content management have adopted three main tasks, which were the construction and development of groups, information operations and Information Services. Building and development of collections and information sources: the most prominent sources of information security were represented in archival materials, in various forms, including film miniatures, audio-visual materials, information databases, and other forms of information sources. It should be noted that all these sources can be organized and structured according to database systems, thus providing the elements of search and retrieval in them through various search tools and techniques (Zhang, C., & Lu, Y., 2021).

According to Dudnik, O., Vasiljeva, M., Kuznetsov, N., Podzorova, M., Nikolaeva, I., Vatutina, L., ... & Ivleva, M. (2021), Organization of information: it consists in the technical operations carried out by these institutions in order to create access for the beneficiaries of their services to the content of their information sources. The most prominent of these processes is the characterization of data and includes the rules and standards of content characterization, which is called indexing in both descriptive and objective, and there is an analysis and organization of content, which includes classification, disclosure, concept maps (ontology) and others. Information services: the most prominent services provided by Information institutions are guidance, guidance and Training Services, internal and external lending, reference services, selective broadcasting of information, bibliographic services, ongoing briefing, photocopying and reproduction, special category services, and other services. The question arises as to what impact artificial intelligence technologies have on the main tasks of information organizations.

3. Research Methodology

In this research, the researcher followed a descriptive and analytical approach by discussing ideas related to the topic, measuring them, extracting important findings and legal principles from them, and providing an accurate description of them. The researcher also adopted a comparative approach when comparing different legislations, and conducted research on the meanings of some terms related to the study, examining them within the framework of laws and the opinions of jurists.

4. Results

Artificial intelligence is defined as it is one of the branches of computer science that deals with how machines simulate human behavior, therefore it is a special science to create computer devices and programs capable of thinking in the same way as the human brain works, learn as we learn, decide as we decide, and so on. The researcher believes that this skill is very suitable for the robot to carry out special procedures in the field of crime prevention, the field of criminal control during the commission of a crime, or the search for suspects in a particular crime to investigate them, and find out the extent to which any of them contributed to the commission of a crime. Artificial intelligence can benefit the law enforcement community by confirming a scientific point of view and evidence, and this is especially evident in forensic DNA testing (DNA analysis), where this has an unprecedented effect in detecting criminals, and judicial systems have benefited in the past few decades from the analysis of biological materials such as blood, saliva, semen, and skin cells, which can be spread by contact during the commission of various crimes, and with the advancement of DNA analysis technology using artificial intelligence, this has allowed forensic scientists to detect crimes and provide evidence resulting from DNA analysis, especially in crimes sexual assaults, and murders can now be brought to the laboratory for the necessary acid analyzes, so that the perpetrators can be detected by DNA analysis and artificial intelligence applications in this field.

5. CONCLUSION AND RECOMMENDATIONS

Artificial neural networks can allow employees to predict the criminal severity by unknown criminals who have found a way to avoid alarm triggers in binary rule-based security systems. Jurists have used the term "felony" instead of crime, perhaps this is due to their sufficiency with it, considering the meaning intended to be released for the crime, and it is thus more practical and comprehensive than the use of Jurists. Civil liability occurs when the disciplinary or legal penalty is due for compensation and is the subject of consideration here, and reparation of damage is considered one of the basic functions of civil liability, which is achieved through compensation, and therefore civil liability is the payment of compensation, which is the responsibility of the actor for the benefit of the injured, and it is also a legal case of a person who commits a mistake resulting in damage to the interest of others. Criminal liability is the obligation of a person to bear the legal consequences of committing an act that is considered a crime from the point of view of the law and the result of violating this obligation is the punishment or precautionary measure imposed by law on the perpetrator of the crime or responsible for it. Accordingly, criminal liability is no longer purely material liability as it was in the old criminal legislation, but is nowadays based on moral or ethical responsibility. I recommend my fellow researchers and scholars to intensify various studies and research to examine the risks of artificial intelligence in general and its risks regarding information security crimes in particular, because this is of great importance in practice.

REFERENCES

[1] *Brahan, J. W., Lam, K. P., Chan, H., & Leung, W. (1998). AICAMS: artificial intelligence crime analysis and management system. Knowledge-Based Systems, 11(5-6), 355-361.*

[2] *Butkar, M. U. D., & Waghmare, M. J. (2023). Crime Risk Forecasting using Cyber Security and Artificial Intelligent. Computer Integrated Manufacturing Systems, 29(2), 43-57.*

[3] *Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly, 2(38), 1-9.*

[4] *Dudnik, O., Vasiljeva, M., Kuznetsov, N., Podzorova, M., Nikolaeva, I., Vatutina, L., ... & Ivleva, M. (2021). Trends, impacts, and prospects for implementing artificial intelligence technologies in the energy industry: the implication of open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 7(2), 155.*

[5] *Friedrichs, D. O.(2015). Crimes of the powerful and the definition of crime. In The Routledge international handbook of the crimes of the powerful (pp. 39-49). Routledge.*

[6] *Hallevy, G. (2010). The criminal liability of artificial intelligence entities-from science fiction to legal social control. Akron Intell. Prop. J., 4, 171.*

[7] *Hallevy, G. (2010). The criminal liability of artificial intelligence entities-from science fiction to legal social control. Akron Intell. Prop. J., 4, 171.*

[8] *Hallevy, G. (2010). The criminal liability of artificial intelligence entities-from science fiction to legal social control. Akron Intell. Prop. J., 4, 171.*

[9] *Hartel, P. H., Junger, M., & Wieringa, R. J. (2010). Cyber-crime science= crime science+ information security. CTIT, University of Twente, Technical Report TR-CTIT-10-34.*

[10] *Jeong, D. (2020). Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. IEEE Access, 8, 184560-184574.*

[11] *Khadragy, S., Elshaeer, M., Mouzaek, T., Shammass, D., Shwedeh, F., Aburayya, A., ... & Aljasmi, S. (2022). Predicting Diabetes in United Arab Emirates Healthcare: Artificial Intelligence and Data Mining Case Study. South Eastern European Journal of Public Health.*

[12] *King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. Science and engineering ethics, 26, 89-120.*

[13] *Kouziokas, G. N. (2017). The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment. Transportation research procedia, 24, 467-473.*

[14] Pagallo, U. (2013). What robots want: Autonomous machines, codes and new frontiers of legal responsibility. In Human law and computer law: Comparative perspectives (pp. 47-65). Dordrecht: Springer Netherlands.

[15] Panas, E. E., & Ninni, V. E. (2011). Ethical Decision Making in Electronic Piracy: An Explanatory Model based on the Diffusion of Innovation Theory and Theory of Planned Behavior. International Journal of Cyber Criminology, 5(2).

[16] Taylor, A. (2006). Publishing and electronic piracy. Learned publishing, 19(3), 168-174.

[17] Walczak, S. (2021). Predicting crime and other uses of neural networks in police decision making. Frontiers in Psychology, 12, 587943.

[18] Yas, H., Alkaabi, A., ALBaloushi, N. A., Al Adeedi, A., & Streimikiene, D. (2023). The impact of strategic leadership practices and knowledge sharing on employee's performance. Polish Journal of Management Studies, 27.

[19] Yas, H., Jusoh, A., Nor, K. M., Alkaabi, A., Jovovic, N., & Delibasic, M. (2022). IMPACT OF AIRLINE SERVICE QUALITY ON PASSENGER SATISFACTION AND LOYALTY: MODERATING INFLUENCE OF PRICE SENSITIVITY AND QUALITY SEEKERS. Transformations in Business & Economics, 21(3).

[20] Yas, H., Mardani, A., & Alfarttoosi, A. (2020). The major issues facing staff in islamic banking industry and its impact on productivity. Contemporary Economics, 14(3), 392.

[21] Yas, N. (2021). Powers of Arbitrators in the Implementation of Arbitral Awards. PSYCHOLOGY AND EDUCATION, 58(2), 6900-6907.

[22] Yas, N., & Hareb Alkuwaiti, H. H. (2021). Exemption from Contractual Liability in Civil Obligations. Review of International Geographical Education Online, 11(9).

[23] Yas, N., Al Qaruty, R., Hadi, S. A., & AlAdeedi, A. (2023). Civil Liability and Damage Arising from Artificial Intelligence. Migration Letters, 20(5), 430-446.

[24] Yas, N., Dafri, W., & Rezaei Gashti, Z. (2022). An Account of Civil Liability for Violating Private Life in Social Media. Education Research International, 2022.

[25] Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224.