ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 11, Issue 9, September 2024

Artificial Intelligence and Cybercrime in the EU

[1] Dr. Adriana-Iuliana STANCU

[1] Associate Professor PhD "Dunărea de Jos" University of Galati, Romania Head of Department of Legal Science, Faculty of Law and Administrative Sciences

Corresponding Author Email: [1] vittalgondkar@gmail.com, [2] harshsaptel@gmail.com

Abstract— Objectives: AI can be used to identify vulnerabilities in computer systems and provide better security solutions. Machine learning algorithms can be used to analyze application source code and identify potential security vulnerabilities. This can help eliminate these vulnerabilities before they are exploited by cyber attackers. Overall, the collaboration between AI and cybersecurity can lead to greater protection of users' personal data and integrity. This can help prevent cyber-attacks and reduce their impact on users and computer systems. Proposals and methodology: People's daily lives are being impacted by artificial intelligence more and more, and digital modelling is one area where it is especially significant due to its automatic decision-making capabilities. The beneficial results of this unpredictable technology are great, but so are the concerns they raise. Thus, it is useful to highlight the role of cybersecurity in creating a reliable competitive AI, as well as in achieving a trust-inducing AI. While it is possible to modify AI techniques and systems to produce desired results, it is important to keep in mind that applying AI security can have unexpected consequences. Results and implications: Artificial intelligence affects people's daily lives and plays a crucial role in digital transformation through its automated decision-making capabilities. Both the advantages and the drawbacks of this new technology are substantial. Therefore, it's important to emphasize how important cyber security is to achieve the legitimacy and integration of a reliable AI. We must be conscious of the fact that the technological potential of AI systems might produce unfavourable outcomes and can be altered to distort our expectations when thinking about the security of the system that may be impacted by AI. While this is undoubtedly fortunate, we shouldn't ignore the fact that artificial intelligence (AI) and its applications, such as automated decision-making or algorithms created through AI, can impose new and occasionally completely unforeseen risks on people or organizations. AI can also introduce new attack techniques and opportunities for data protection. This is especially true for safety-critical deployments like autonomous vehicles, intelligent production or manufacturing, eHealth, etc.

Index Terms: decisions; artificial intelligence; digitization; cyber security; European legislation; techniques.

I. INTRODUCTION

This paper will adopt a dual perspective on artificial intelligence (AI), emphasizing the potential advantages of AI in the fight against crime as well as the concerns associated with its potential to be used as a tool for criminal activity. Lastly, we will examine the legislative strategies that are currently in use at the national, European, and international levels and provide some real-world instances to highlight the nuanced nature of the interaction between AI and crime.

The term artificial intelligence (AI) describes a system's capacity to carry out particular tasks that would typically need human intelligence. These include of data analysis, facial recognition, natural language processing, and more. Contrarily, cyber security focuses on defending computer networks and systems against online threats.

The collaboration between AI and cybersecurity can bring many benefits to technology and Internet users. AI can be used to detect cyber-attacks as well as to provide more effective security solutions. For example, machine learning algorithms can be trained to detect suspicious traffic patterns or unusual behavior in computer networks. They can help identify cyber-attacks quickly, which can lead to a faster and more effective response in managing security situations.

AI can also be used to identify vulnerabilities in computer systems and provide better security solutions. Machine learning algorithms can be used to analyze application source code and identify potential security vulnerabilities. This can help eliminate these vulnerabilities before they are exploited by cyber attackers.

In general, better protection of user privacy and data integrity can result from the cooperation of AI with cybersecurity. By doing so, cyberattacks can be avoided and their effects on users and computer systems can be lessened.

II. THE DEPENDABILITY OF A RELIABLE AI

The collaboration between AI and cybersecurity can bring many benefits to technology and Internet users. AI can be used to detect cyber-attacks and provide more effective security solutions. Algorithms for machine learning, for instance, can be trained to recognize anomalous activity in computer networks or questionable traffic patterns. They can aid in the prompt detection of cyberattacks, enabling a quicker and more efficient reaction when handling security-related issues.

IT security has made significant progress because of AI and cybersecurity working together, as evidenced by the following:

- Cyber-attack detection and prevention – AI can be used to detect unusual behavior in computer networks, thereby identifying potential cyber-attacks. AI can also be used to develop more effective security solutions to prevent such attacks.
- Improving application security – AI can be used to

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Vol 11, Issue 9, September 2024

analyze application source code and identify security vulnerabilities. This can help develop more secure and cyber-resistant applications.

- Improving authentication – AI can be used to develop more secure authentication solutions, such as authentication based on facial or voice recognition. These solutions can be more secure than passwords, which can be easily guessed or stolen.
- Identifying cyber security threats – AI can be used to identify patterns and trends in cyber-attacks. This information can be used to develop more effective cyber security solutions.
- Security data analysis – AI can be used to analyze security data, such as access and activity logs, to identify potential security issues. This information can be used to develop better cyber security solutions.

These are just a handful of the accomplishments resulting from the combination of AI and cybersecurity, which have improved user integrity and personal data.

In order to strengthen information security and safeguard personal data, several well-known cybersecurity tools also make use of artificial intelligence technologies, such as:

1. Darktrace – It is a cyber security tool that uses Artificial Intelligence to detect cyber-attacks and respond in real time, helping to prevent data loss and cyber-attacks.

2. IBM Watson for Cybersecurity – This is a cybersecurity tool that uses IBM Watson technology to identify and prevent cyber-attacks. Using advanced data analysis and machine learning, IBM Watson can quickly and efficiently detect potential security threats.

3. Cylance – It is a cyber security tool that uses Artificial Intelligence technology to identify and prevent cyber threats. Cylance uses machine learning and behavioral analytics to identify and prevent cyber-attacks.

4. McAfee – It is a cyber security tool that uses Artificial Intelligence technology to protect personal data and security information. McAfee uses behavioral analysis and machine learning to identify security threats and prevent data loss.

Cybersecurity officials say the biggest fear is a deepfake technology that uses images and video footage to associate strange similarities or unknown metamorphoses. IT specialists are afraid that technology itself can produce images and films that deceive people into thinking that what they are seeing is real. “If cybercriminals can find various ways to take and use your identity or even create someone from scratch, an identity that doesn't exist and that's fake, and then use online verification processes, then there's a huge risk”, he ruled Philipp Amann, Group Chief Information Security Officer of the Austrian Post at the International Digital Security Forum in Vienna 2023. He points out that Artificial Intelligence is now being used to facilitate money laundering and defrauding online platforms. In the most recent case investigated, a person used deepfake technology to deceive a mid-level corporation into believing they were an executive and conned them out of millions of dollars.

However, there are now other uses for this technique. For instance, a number of European lawmakers were charged with being deepfakes after they fell for a con to attend a meeting with Leonid Volkov, the chief of staff of Alexei Navalny, who was publicly claiming to be a representative of the Russian opposition.

It's frequently unknown how much of this technology is used. This suggests a low level of long-term and contextual trust. Frequently, the aim of cybercriminals is to sow doubt and undermine our faith in our sensory and cognitive capabilities.

III. ARTIFICIAL INTELLIGENCE AND THE POWER IT GENERATES

The danger is genuine and beyond our capacity to assess. AI can be used in a variety of ways by whoever controls it, from password cracking to the creation of social networks that don't match real accounts, to software intended to harm or interfere with computers. Back in December, Europol announced that it had found a program on the “Deep Web” that reads passwords using Artificial Intelligence technology. This program can analyze up to several billion access keys, enabling hackers to gain access to any information that needs to be secured. Other Internet “hackers” are developing tools that use AI to generate fake “phishing” content that they upload to an email and trick people into giving them their personal bank account credentials (Russell & Norvig, 2010).

In the specialized literature, AI is understood as representing the ability of a machine to perceive and respond independently to tasks that would normally require human intelligence in decision-making processes (Rigano, 2018). Patrick Winston (1992) defines AI as “*algorithms enabled by constraints, exposed by representations that support targeted models of loops that link thought, perception and action*”. As another author argues, AI is a broader branch of computer science, concerned with building intelligent machines capable of performing tasks that usually require human intelligence (Stănilă, 2020).

The capacity to learn from experience is one aspect of human intelligence, as noted by Bernard Marr (2016). Machine learning, on the other hand, is an application of AI that mimics learning and allows software to learn from practice. The fact that AI can identify potential criminals is nothing new. For example: “risk assessment tools”, a class of algorithmic tools, called risk assessment tools (RAIs), are designed to predict a defendant's future risk of committing antisocial acts (Chohlas-Wood, 2020).These predictions help judicial bodies, for example, to know whether the defendant should be incarcerated or not.

Incidentally, we can mention the chatbot Sweetie, an AI program, whose purpose is to combat online pedophilia - acts with explicit sexual content involving children, carried out via webcam, by identifying suspects, offenders and victims. This chatbot was created by the organization Terre des Hommes in the Netherlands in 2003 (Chohlas-Wood, 2020).

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 11, Issue 9, September 2024

In its first version – Sweetie 1.0 – the chatbot transformed into a 10-year-old girl from the Philippines and was used to find and expose sex tourism pedophiles. Since its first version was not automated, Sweetie was handled by a human agent. The discussions with the pedophiles were done with the police, Sweetie only having the role of their avatar.

The use of the first version of Sweetie was also limited because it was operated by a police officer as a human actor, which led to a minimal number of online conversations held at the same time. However, the number of suspects - webcam sex amateurs - was more than 2,000 per hour. Under such conditions, the human resources of the police were insufficient, which is why Sweetie 2.0, a more refined version of the chatbot, was created. "The biggest difference between Sweetie 1.0 and Sweetie 2.0 relates to the fact that the latter is no longer operated by a police officer as a human agent, being a semi-autonomous AI system that can actively converse with a suspect." Sweetie 2.0 is actually a hybrid model that cannot be used without a human actor. The biggest advantage of using Sweetie is that investigators can come into direct contact with pedophiles without putting anyone in danger, in other words, there are no victims in the process, only future suspects. It is the same as discovering a crime while it is still in the attempted stage.

Even though Sweetie's investigative innovation has created excitement, there are serious issues with the legal qualification of the "facts" she found: since there has been no completed or attempted crime and no human victim, the criminal law cannot be applied. To punish "sexual predators" as a result of using Sweetie in accordance with criminal procedural requirements and standards, substantial legislative interventions are needed.

Thus, the interaction with Sweetie would require, at the very least, to be qualified by law as attempted criminal behavior. "Without this, it will be much more difficult, or almost impossible, to infer that the suspect has committed or attempted to commit a criminal act. In turn, this fact will make it much more difficult to justify using Sweetie in the investigation. This method of using Sweetie as a method of investigation led to the formation of two camps of opinions: the camp of supporters formed by members of civil society and the camp of those who oppose this innovation formed by legal specialists and supported by a non-profit organization, the European Police Agency Europol, as it expressed reservations about its use. According to Soren Petersen, "We believe that criminal investigations using intrusive surveillance measures should be the sole responsibility of law enforcement agencies" (Schermer, Georgieva, Van der Hof, & Koops, 2016, p. 10).

In a similar spirit, what we're discussing here are software solutions that employ a lot of data, processed by software algorithms, to inform choices. We are discussing statistical and historical data that forecasts the location and time of a criminal act in the future. This is the key difference from past computer systems: they predict the chance that criminal activity will occur. In the ideal scenario, a police officer, who is informed by such a system, will be at the exact place and time when a criminal would have intended to commit a crime. In this way, crime will be prevented (Baiaș, 2020).

On the other hand, AI can play an essential role in committing criminal acts (King, Agarwal, Taddeo, & Floridi, 2019). This is why the doctrine speaks of a new type of criminality: "AI Crime" (AIC). AIC emphasizes the use of AI as a means or method of committing the crime, with the possibility that in the future crimes of any type committed by AI will be included as a subject of law (Stănilă, 2020). The existence of AIC was demonstrated by researchers through experiments in which they convinced social media users to click on phishing links. Phishing is a method of online deception that attempts to obtain personal or confidential data from customers of various organizations. These can then be used illegally by criminals to make transactions on that customer's account. These kinds of experiments make it clear that AI is a serious and fundamentally new threat (King, Agarwal, Taddeo, & Floridi, 2019).

IV. ANALYSIS OF THE RISKS OF ARTIFICIAL INTELLIGENCE AS A SUBJECT OF LAW

Once this phenomenon is recognized, it is necessary to analyze the risks that AIC represents in the development of social relations and ensure an appropriate and effective criminal protection for the social values threatened by AIC. In the realm of solutions, it must be checked whether the current incriminations are sufficient to protect social relationships and values from criminal acts that are carried out through AI. Domestic regulations "must reflect the transnational idea of order, justice and solidarity" (Cotterel, 2017, p. 22).

At this moment, it is necessary to measure critically and permanently the effects produced by some artificial agents that have a faulty or inadequate function, or that give results that violate fundamental human rights, in general. As artificial agents, the behavior of these systems cannot be evaluated against the moral standards of individuals. There are contemporary authors (Stănilă, 2020), who noticed that judgment with moral implications always attracts elements involving options, human empathy or cooperative capacities. It is impossible to expect morality from artificial agents; their behavior is causally determined through technology by human specifications. In this regard, AI applications in government decision-making, especially those in the criminal justice system, should be of concern. Existing evidence suggests that algorithms "inherit" and sometimes intensify existing biases and inequities. Then there are the negative consequences of AI that play out in terms of democratic discourse and politics. This is not only due to algorithmic disinformation in social media, but also the increasing ability of companies and governments to monitor and manipulate the behaviors of millions of people, which is incompatible with true democracy (Acemoglu, 2021).

Relatively recently, on June 29, 2021, a review draft on AI in criminal law and its use by police and judicial authorities in criminal matters was brought forward and adopted by the Committee on Civil Liberties, Justice and Home Affairs by 36 votes for and 24 against. Although the possible benefits that AI brings are recognized, the report highlights, in the same way, the most important risks and effects that the Team AI Regulation (2021) can bring - European Parliament. According to psychology, there are risks associated with AI for users' mental health, and these risks could lead to criminal behavior. This fact was demonstrated by Joseph Weizembaum (1976), after conducting experiments aimed at human-bot interaction, in which people revealed the most intimate details, being under the influence of AI.

Like many other technologies, AI can serve multiple purposes, being used both for the good of society and for harmful actions. AI can perform many tasks that are normally performed by humans, and in some cases even surpass human performance in terms of efficiency and speed and objectivity. This means that crimes that until now required human skills can be committed on a much larger scale through AI. One of the main aspects of AI as a means of committing the crime is, as pointed out in the legal literature, the fact that it can increase the distance between the offender and the victims, and therefore also increases the difficulty of investigating and proving the fact. Looking from this point of view, AI is seen as a true "vector" of crime (Dupont, Stevens, Westermann, & Joyce, 2018, p. 7).

AI systems could enable human actors to commit "invisible" crimes. For example, most people are not capable of realistically imitating other people's voices or manually creating audio files that resemble recordings of human speech. However, significant progress has recently been made in the development of AI speech synthesis systems that learn to imitate the voices of individuals. There is no obvious reason why the results of these systems could not become indistinguishable from authentic records in the absence of specially designed safety measures (Polito & Pupillo, 2024, pp. 10-13).

Europol's serious and organized crime threat assessment report (SOCTA 2017) highlights the ways in which technological crime tends to correlate with certain types of criminal organizations (King, Agarwal, Taddeo, & Floridi, 2019). The doctrine, moreover, highlights that AI and technological crime tends to become a new area of specialization for organized crime, thus, AI can play a role in criminal organizations such as drug cartels (Stănilă, 2020). An understanding of these phenomena will inevitably lead to the adoption of some preventive measures. In this sense, the Romanian legislator has incriminated some acts that can be committed by or through AI. On the European level, the Treaty on the functioning of the European Union itself refers to the concept of "computer crime", in the content of art. 83 para. (1) regarding the competence of the legislative forums of the European Union to legislate, through directives, regarding the definition of crimes and sanctions in areas considered to be particularly serious and having a cross-border dimension. In this sense, Directive 2018/1673/EU on combating money laundering through criminal law measures includes in the range of relevant criminal activities "computer crime", including any crime provided for in Directive 2013/40/EU of the European Parliament and of the Council "[art. 2 par. 1 letter (v) of the Directive]. From this wording, it can be deduced that the European legislator interprets this concept extensively, not limiting it only to the crimes that are the subject of art. 360-365 Criminal Code (Zlati, 2020, p. 10)

Moreover, cybercrime has been the subject of numerous judicial decisions issued by national courts, decisions that have also analyzed the issue of the use of these tools in the criminal process. The decision of July 25, 2019, of the Supreme Court in Glasgow (United Kingdom), by which a person was convicted for the first time, for sexual abuse of children that was transmitted live, and which took place in Philippines, as well as the December 14, 2018 Decision of the Court of Appeal of Amsterdam (Netherlands), where the defendant received a maximum sentence of 10 years and 243 days in prison, among other crimes it was also included the possession, production, distribution of materials with pornographic content with minors, accessing and possessing software programs for this purpose, blackmail and deception (Schweizer, 2014).

V. CONCLUSIONS

Less happens in the field of technology in two years than we anticipate, but we should also consider the concept of exponential growth over a little period of time. AI works in a similar way. Whether we like it or not, there is already and always will be a relationship between AI and crime. The most crucial factor is how we manage to protect ourselves, and we can only accomplish this through a well-thought-out and comprehensive legal framework that ensures the preservation of fundamental freedoms and rights - the essential foundation for peaceful cohabitation with artificial intelligence. We believe that discussions on this topic should be handled ethically. Ethical handling is necessary while having conversations on this matter. We must consider our beliefs regarding awareness, human worth, and the distinction between natural and artificial. We have previously demonstrated why creating a machine that mimics the human mind is not appropriate, since artificial intelligence is already a cause for concern.

VI. ACKNOWLEDGEMENT

The paper was achieved within the project unfolded by "Dunărea de Jos" University of Galati entitled: "*Developments and Perspectives in Contemporary Law*", financing Contract no RF2469/31.05.2024.

REFERENCES

[1] Acemoglu, D. (2021). Opinion: The AI we should fear is already here. The Washington Post. Retrieved 08 18, 2024, from https://www.washingtonpost.com/opinions/2021/07/21/ai-we-should-fear-is-already-here/

[2] Baiaș, I. (2020, 2024 08). How you can catch a criminal using artificial intelligence (AI) algorithms and techniques. Retrieved 04, from HotNews.ro: https://www.hotnews.ro/stiri-superputerile_tehnologiei-24433285-interviu-cum-poti-prinde- criminal-using-technical-algorithms-artificial-intelligence-vlad-niculescu-since-researcher-the-hague-important-we-find-balance-between-the-need-of-forces-effective-order-the-need-of-society.html

[3] Chohlas-Wood, A. (2020, 08 08). Understanding risk assessment instruments in criminal justice. Retrieved from Brookings: https://www.brookings.edu/articles/understanding-risk-assessment-instruments-in-criminal-justice/

[4] Cotterel, R. (2017). The concept of "crime" and transnational networks of community. In V. Mitsilegas, P. Alldrige, & L. Cheliotis, Globalization, Criminal Law and Criminal Justice (p. 22). Bloomsbury.

[5] Dupont, B., Stevens, Y., Westermann, H., & Joyce, M. (2018). Artificial Intelligence in the Context of Crime and Criminal Justice. Korean Institute of Criminology, Canada Research Chair in Cybersecurity, 7. Retrieved 03 08, 2024, from https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf

[6] King, T., Agarwal, N., Taddeo, M., & Floridi, L. (2019). Artificial Intelligence Crime. An Interdisciplinary Analysis of Forseeable Threats and Solutions. Science and Engineering Ethics, 14 February.

[7] Marr, B. (2016). What Is the Difference Between Deep Learning, Machine Learning and AI? Forbes. Retrieved 04 08, 2020, from https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference -between-deep-learning-machine-learning-and-ai/?sh=3781af0726cf

[8] Polito, C., & Pupillo, L. (2024). Artificial Intelligence and Cybersecurity. Forum Journal, Vol. 59, 10-13.

[9] Rigano, C. (2018). Using Artificial Intelligence to Address Criminal Justice Needs,. National Institute of Justice. Retrieved 08 09, 2024, from https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

[10] Russell, S., & Norvig, P. (2010). Artificial Intelligence: A Modern Approach. 3rd Edition. Prentice-Hall: Upper Saddle River.

[11] Schermer, B., Georgieva, I., Van der Hof, S., & Koops, B.-J. (2016). Legal Aspects of Sweetie 2.0. Leiden/Tilburg: TILT.

[12] Schweizer, K. (2014, April 26). Avatar Sweetie exposes sex predators. Retrieved from The Age: https://www.theage.com.au/-world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html

[13] Stănilă, L. (2020). Artificial intelligence and the criminal justice system – Criminal risk assessment tools. Romanian Journal of Business Law. Retrieved 08 18, 2024, from http://rrdpa.ro/numarul-3-2019/inteligenta-artificiala-si-sistemul-de -criminal-justice-criminal-risk-assessment-tools/

[14] Winston, P. (1992). Artificial Intelligence. 3rd edition. London: Pearson.

[15] Zlati, G. (2020). Tratat de criminalitate informatică/Treatise on Computer Crime, Vol 1. Bucharest: Solomon.