UDK 004.8:343.8
343.14:004.8
Review article

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: EXAMINING LIABILITY, CRIME DYNAMICS, AND PREVENTIVE STRATEGIES

Herke Csongor, PhD, Full Professor
University of Pécs, Faculty of Law
H-7622 Pécs, 48-as tér 1., Hungary
herke.csongor@ajk.pte.hu

Dávid Tóth, PhD, Assistant Professor
University of Pécs, Faculty of Law
H-7622 Pécs, 48-as tér 1., Hungary
toth.david@ajk.pte.hu

ABSTRACT

This research comprehensively explores the interplay between artificial intelligence (AI) crime and cybersecurity. The study aims to perform a criminological analysis to understand AI's impacts on cybersecurity, highlighting its benefits and potential risks.

A significant aspect of this research is investigating liability issues associated with AI's deployment. These concerns are not limited to specific applications, such as self-driving vehicles, but extend across various AI-utilizing sectors. AI's capability to autonomously make decisions, sometimes with severe implications for individuals, poses the critical question of responsibility. When AI-driven decisions lead to adverse outcomes, the dilemma arises: who should be held accountable - the developers, the users, or the AI itself?

Another vital research question examines how AI influences cybercrime. This study scrutinises AI's role in transforming cybercrime's nature and the new security risks it introduces. It questions the adequacy of current criminal laws in addressing novel crime forms emerging from AI advancements and explores how these laws might need to evolve. Moreover, the research investigates AI's role in amplifying or simplifying traditional crimes, such as through the creation of phishing programs or the use of DeepFake in identity theft.

The impact of AI on digital evidence forms another critical area of investigation. AI algorithms, capable of efficiently analysing vast data sets, can significantly aid in crime detection and perpetrator identification. However, this advancement also raises concerns about the *authenticity of digital evidence. Technologies like deepfake, capable of producing convincing fake images and videos, present a formidable challenge in distinguishing real from fabricated evidence, especially in legal contexts.*

Lastly, the research delves into AI's potential in crime prevention. It assesses how AI-driven predictive models can identify likely crime hotspots and timings, enabling more effective resource allocation by police and security services. The study also explores advancements in AI's facial and object recognition technologies, highlighting their potential in criminal identification.

In summary, this research offers a detailed examination of AI's multifaceted impact on cybersecurity, liability issues, cybercrime, digital evidence, and crime prevention, presenting a nuanced understanding of AI's challenges and opportunities in law enforcement and legal accountability.

Keywords: *Artificial Intelligence, Cybersecurity, Cybercrime and Digital Evidence, Crime Prevention and Detection, Liability and Accountability*

1. INTRODUCTION

The rapid development of information technology has manifested as a Janus-faced phenomenon. On one hand, it has significantly eased people's daily lives by introducing efficiencies and conveniences previously unimaginable. On the other hand, it has also provided criminals with new avenues to commit offenses, thus ushering in unprecedented challenges for states and their legislative efforts in combating cybercrime. This dichotomy lies at the heart of our research, which seeks to explore the nuanced interplay between artificial intelligence (AI), cybercrime, and cybersecurity.

The COVID-19 pandemic has highlighted our reliance on digital communication as never before. In our collective effort to maintain social distancing, digital platforms have become indispensable, enabling us to continue our professional and personal lives with some semblance of normalcy. However, this increased dependence on digital technology has also amplified vulnerabilities, offering cybercriminals enhanced opportunities to exploit these systems, thereby elevating the risks associated with cybersecurity. Just as with the emergence of smartphones[1], the development of artificial intelligence raises many questions. In our opinion, the rise and proliferation of artificial intelligence present various challenges and dilemmas, necessitating examination through both a criminal law and criminology lens. Our study is designed to address the following key areas:

- criminal law questions arise from using artificial intelligence, such as autonomous vehicles causing accidents.

[1] Andrea, K.; László, K.; Dávid, T., *Digital Dangers of Smartphones*, Journal of Eastern-European Criminal Law, Vol. 7, No. 1, 2020, pp. 36-49.

- The impact of artificial intelligence on crime, with a specific focus on cybercrime, including the emergence of new forms of criminal activities or methods of perpetration.
- An examination of how the gradual spread of artificial intelligence, for instance, through technologies like deepfake, could transform the landscape of digital evidence.
- Lastly, the potential roles of artificial intelligence in crime prevention and detection, enhancing law enforcement capabilities.

Our research systematically examines existing scholarly articles using a comprehensive literature review as our primary methodology.

2. LIABILITY QUESTIONS WITH THE USE OF AI

Artificial Intelligence can make decisions, sometimes autonomously, with severe implications for individuals, which poses the critical question of responsibility. When AI-driven decisions lead to adverse outcomes, the dilemma arises: who should be held accountable?

We can illustrate the issue with self-driving cars. Autonomous vehicle development traces back to the 1920s, with significant advancements like Japan's first semi-automatic vehicle in 1977 and DARPA's influential foundation in 1984 in the U.S. Nevada led state authorization in the U.S., followed by Columbia and California, which permitted autonomous vehicles on public roads by 2012, with evolving regulations to accommodate fully driverless technology. The classification of these vehicles ranges from Level 0 (no automation) to Level 5 (fully autonomous) according to the SAE J3016 standard. By 2020, the National Highway and Transportation Safety Administration (NHTSA) had issued guidelines focusing on higher automation levels to promote safety and innovation. The development of autonomous vehicles is also driven by major companies like Tesla and Mercedes, indicating a shift towards broader acceptance and integration of this technology in society.

In cases involving fully autonomous vehicles, determining who to hold accountable for accidents or crimes caused by the vehicle can pose a challenge:

- The first possible candidate is the manufacturer. The manufacturer isn't automatically responsible for production once the vehicle is approved; manufacturing isn't a crime without the proper permits. However, the manufacturer is liable if it can be proven that the vehicle was programmed to commit a deliberate crime, if they could have foreseen and prevented the accident, or if the accident can be traced back to a programming or manufacturing flaw.

- Another option might be the programmer**.** Programming errors also raise questions about the programmer's responsibility, whether the vehicle was programmed recklessly or deliberately in a way that directly causes an accident (e.g., misinterpreting right-of-way rules). However, modern autonomous vehicles are often programmed with "deep learning," continuously updating their decision-making in various situations based on new data, making it increasingly difficult to attribute poor decisions directly to the programmer.
- The third option can be the owner. The owner merely purchases the autonomous vehicle without influencing its autonomous driving system. In fully autonomous vehicles, the operator becomes merely a passenger, unable to affect the vehicle's operation (except possibly to stop it, which rarely helps in immediate situations). This does not preclude the commission of deliberate crimes using the vehicle (e.g., drug trafficking, terrorist attacks, human trafficking).
- Another candidate can be the user: Like the operator, in fully autonomous vehicles, the user is not a driver but a passenger. As automation increases (starting from Level 3), the "driver's" role becomes mere observation, without the need for active intervention over long periods (similar to autopilots used in airplanes and ocean liners). Since responsibility typically falls on those who can influence events, determining liability always requires considering the circumstances of each case.
- Lastly, we have the concept of the vehicle as a "digital person" (like the criminal liability of legal persons) that might arise in accidents involving fully autonomous vehicles. However, fully autonomous vehicles are unlikely to "understand" norms as commands for the foreseeable future since they operate solely based on pre-installed programming without independently interpreting or understanding legal norms and acting accordingly.

Determining who is liable for accidents caused by fully autonomous vehicles is not straightforward. The potential parties (the user, the manufacturer, the programmer, the owner/operator, and the digital person) can all be held accountable, individually or collectively, and responsibility must be determined based on the unique circumstances of each case.[2]

Csitei also acknowledges the complex issue of deciding who can be liable for accidents caused by self-driving cars. In his study, he emphasizes that as autonomous

[2] Herke, Cs., *A kiberbűnözés és a teljesen önvezető járművek*, in: Barabás, A. T.; Christián, L. (eds.), Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est, Ludovika Egyetemi Kiadó, Budapest, 2021, pp. 211-216.

vehicles transcend the traditional notion of a vehicle driver, the concept of culpability may lose meaning in many cases of traffic offenses, suggesting a shift in how liability is considered. He also points out that autonomous vehicles are not fully autonomous from human oversight, as humans define their development and operational parameters. Therefore, aspects of human conduct related to autonomous vehicles' design, development, and operational decisions could be considered for liability. He elaborates on holding legal entities accountable under certain conditions. For example, if it can be proven that the accident resulted from a defect in the vehicle's design or manufacturing process or if the software did not operate as intended, legal entities associated with these aspects might face liability.[3] However, we have to mention that legal persons under Hungarian criminal law cannot be held liable for crimes. They can be only sanctioned by measures and not punishments and only if the crime was committed by the entity's officials, employees, or agents within the entity's operational activities, with the intention or result of obtaining a benefit for the entity. In the case of self-driving cars, legal persons cannot be held liable for such accidents unless there is a statutory modification.[4]

Joon differentiates the theoretical liability conditions according to the levels. For Level 4 autonomous vehicles, which need some driver input, Joon indicates that drivers are still responsible under traffic laws when using the autonomous feature. If an accident happens because they don't follow these laws, they could be held criminally accountable. However, if the car is usually in autonomous mode and only asks for driver help after giving an alert, drivers might not be blamed for accidents before the alert. If an accident occurs because they didn't take over manually after an alert, they could face charges for criminal negligence due to their failure to act. For Level 5 autonomous vehicles, which operate without any need for driver input, it is unreasonable to expect drivers to anticipate or prevent accidents, making it impractical to assign them criminal responsibility. In such cases, the liability for accidents shifts to the manufacturers, who are seen as the "drivers" of these fully autonomous vehicles. Although there is a notion of assigning criminal liability to the artificial intelligence or autonomous driving system, Joon's study ultimately points towards corporate manufacturers as the likely bearers of responsibility for any accidents involving fully autonomous vehicles.[5] Unfortunately, such a case has already occurred. In 2018, in the state of Arizona, an Uber

[3] Csitei, B., *Self-Driving Cars and Criminal Liability,* Debreceni Jogi Műhely, 17th Vol., No. 3-4, National University of Public Service, Faculty of Public Governance and International Studies, Department of Civilistics, 30 December 2020, pp. 34-38. [DOI 10.24169/DJM/2020/3-4/4.].

[4] Tóth, D., *The Theories and Regulation of Criminal Liability of Legal Persons in Hungary*, Journal of Eastern-European Criminal Law, Vol. 6, No. 1, 2019, pp. 178-189.

[5] Joon, K., *Criminal Liability of Traffic Accidents Involving Autonomous Vehicles*, Central Law Review, Vol. 19, No. 4, 2017, pp. 47-82. [https://doi.org/10.21759/caulaw.2017.19.4.47].

self-driving car hit a pedestrian, which resulted in her death due to the car's failure to identify and respond to her presence correctly. However, the car was not fully autonomous and had a safety driver who was charged with negligence. Uber faced no criminal liability because the company reached an undisclosed settlement with the victim's family.[6]

Some authors only mention civil law liability in these cases. Lohmann recommends a model where the vehicle holder remains strictly liable, ensuring the victim's compensation. Under strict liability, as vehicles advance towards full automation, the incidence of accidents attributed to human error is expected to decrease. At the same time, those caused by system malfunctions or software glitches may rise. In scenarios where such malfunctions lead to accidents, manufacturers might face liability for producing a defective product by product liability legislation. The advent of self-driving cars suggests a shift towards more accidents being linked to product defects rather than errors made by drivers, prompting a more thorough examination of the responsibilities borne by manufacturers.[7]

3. THE REGULATION OF AI IN THE EUROPEAN UNION

Manea and colleagues investigated which fundamental rights might be violated using AI. One primary concern is the right to non-discrimination. Suppose an AI system is trained on data that includes biased decisions from the past. In that case, it can perpetuate and even amplify these biases, undermining the principle of equality before the law. Another significant issue is the right to privacy and personal data protection. AI systems often collect and analyze large amounts of data, which can infringe on individuals' privacy rights. The right to freedom of expression is also at risk, as algorithms can affect how information is accessed and distributed. Finally, the right to a fair trial is a critical concern. If AI-based decision-making systems are used in judicial proceedings, they can distort judgments and introduce biases, potentially compromising the justice system's fairness.[8]

These types of concerns also appeared in the bodies of the European Union. Among the institutions of the EU, the European Parliament has dealt with the

[6] Neuman, S., *Uber Reaches Settlement With Family Of Arizona Woman Killed By Driverless Car*, THE TWO-WAY, [https://www.npr.org/sections/thetwo-way/2018/03/29/597850303/uber-reaches-settlement-with-family-of-arizona-woman-killed-by-driverless-car], Accessed 29 March 2024.

[7] Lohmann, M. F., *Liability Issues Concerning Self-Driving Vehicles*, European Journal of Risk Regulation, Vol. 7, No. 2, 2016, pp. 336-340, [doi: 10.1017/S1867299X00005754].

[8] Manea, T.; Ivan, D. L., *AI Use in Criminal Matters as Permitted under EU Law and as Needed to Safeguard the Essence of Fundamental Right*s, International Journal of Law and Cyber Warfare, Vol. 1, No. 1, 2022, pp. 18-32.

regulation of the use of artificial intelligence in criminal law cases. Several factors prompted the Parliament to investigate this area. Similarly to the findings above, the European Parliament found that AI systems used in law enforcement can perpetuate and amplify biases and discrimination, mainly based on race or ethnicity. Concerns were also raised about the use of AI in mass surveillance and predictive policing, as these technologies are considered unreliable in accurately predicting individual actions, potentially leading to unjust police actions. Due to these issues, the European Parliament adopted a resolution[9] with the following key points:

- The resolution opposes mass surveillance, explicitly calling for a ban on the processing of biometric data, such as facial images, for law enforcement purposes that lead to mass surveillance. It also recommends halting funding for research and development programs that could further this technology.
- It opposes the use of AI in predictive policing due to its potential for discriminatory applications.
- Human oversight is necessary for decisions with legal implications to ensure accountability and fairness. The resolution states that AI-generated results should not be used to propose judicial decisions.
- Transparency is emphasized regarding which bodies use AI, how, and for what purposes.
- The guidelines aim to ensure that AI use in criminal matters respects fundamental human rights, promotes transparency, and prevents discriminatory practices.

However, this resolution is not legally binding and does not impose obligations on member states. Despite this, the adoption of the resolution is positive, as the applications above could violate people's fundamental rights in criminal proceedings, such as the presumption of innocence. On the other hand, we disagree with the stance on halting research and development, as ethically conducted research could advance law enforcement in the future. Additionally, the transparency criteria are too general in their current form.

Future legislation will be required to address liability questions with legal certainty. The European Union actively explores new AI liability frameworks that could serve as models for global standards. All member states have ratified the so-called AI Act draft[10], confirming political consensus. This draft, first presented by the

[9] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

[10] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

European Commission on April 21, 2021, as the Artificial Intelligence (AI) Act, aims to regulate AI use across the European Union comprehensively. The Council of the EU further solidified its stance by adopting a common position known as the 'general approach' on December 6, 2022.[11] The AI Act emphasizes the critical need for ex-ante testing, risk management, and human oversight to prevent violations of fundamental rights, particularly in crucial areas like law enforcement and the judiciary. The Act recognizes both the potential benefits and significant risks of AI in law enforcement, underscoring the EU's cautious approach toward its usage to safeguard fundamental rights.[12]

The draft does not explicitly detail liability provisions related to AI; the regulatory framework emphasizes accountability for providers and deployers of AI systems, especially those classified as high-risk. For example, they are obliged to undergo rigorous assessment and continuous monitoring to prevent or mitigate potential harm associated with their use. The proposal includes a principle called responsibility for harm or damage. The idea behind this principle is that if harm or damage occurs due to a provider's or deployers' failure to comply with regulatory standards for AI systems, they may be held legally liable. Damage can manifest in many ways, like personal injury, financial loss, and breach of privacy rights, and the draft acknowledges these outcomes and seeks to hold providers and deployers accountable for both anticipated and unforeseen consequences. The proposal has a holistic approach, stating that harm or damage is shared across the entire lifecycle of an AI system, from design and development to deployment and end-of-life. This ensures that liability considerations are included at every stage.[13]

Should the proposed regulation be accepted and implemented, it might result in a scenario where liability is distributed among multiple parties if self-driving vehicles are involved in accidents. Suppose an investigation determines that the cause of the accident is linked to fundamental defects in the AI system's design, development, or deployment phases. In that case, the AI system's provider might face legal liability. This encompasses situations where the AI was insufficiently trained to navigate road conditions or did not meet established safety and performance

[https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf], Accessed 29 March 2024.

[11] [https://artificialintelligenceact.eu/developments/], Accessed 29 March 2024.

[12] Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: Where Do We Stand?* in: „45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)", 2022, p. 1229.

[13] *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* [https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf], Accessed 29 March 2024.

norms. Moreover, if the deployer (which could be the vehicle owner or a company providing autonomous vehicle services) failed to perform regular maintenance, update the software, or operate the vehicle under conditions for which it was not intended (for example, driving in extreme weather conditions that exceeded the AI's capabilities), the deployer could also bear responsibility. But this remains in the field of civil law liability.

4. THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON CRIME

Artificial intelligence can transform forms of crime as well. Like all new technological solutions, artificial intelligence also provides opportunities for criminals. In this section, we will review what potential forms of crime could become prevalent in the near future.

First, we could mention identity theft and DeepFake technology. The latter utilizes AI, specifically deep learning algorithms, to alter videos or create audio recordings that convincingly mimic a person's appearance or voice. This technology can fabricate scenarios or statements, creating the illusion of never-occurring events. By training on extensive datasets of an individual's visual and auditory information, deepfake generates highly realistic but entirely fictitious content. This capability introduces unprecedented risks in identity theft, as evidenced by a notable incident in 2019. A UK-based company was defrauded $243,000 through a scam involving an AI-generated voice impersonating the CEO, showcasing the potent combination of deepfake technology and social engineering tactics.[14]

Morphing represents another facet of AI-enabled crime, involving the fusion of multiple images to create a composite that retains characteristics of the original inputs. This process, comprising warping and cross-dissolving phases, manipulates digital identities by blending faces into a singular, indistinguishable image. Such techniques can be exploited to bypass security measures or create fraudulent identification documents, further complicating the challenges of digital identity verification.[15] In Hungary, identity theft is not a separate crime, but the lawmaker should consider an independent statutory provision for this delict.[16]

[14] *Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company*, Trend Micro, [https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company], Accessed 5 September 2023.

[15] Agarwala, A. Nalini R. Manipulating, *Faces for Identity Theft via Morphing and Deepfake: Digital Privacy,* in: "Deep Learning", 2023, Vol. 48, p. 223.

[16] Tóth, D., *The Criminal Law Protection of Personal Data in Hungary,* in: Ćeranić, D.; Ivanović, S.; Lale, R.; Aličić, S. (eds.), Collection of Papers "Law Between Creation and Interpretation", Vol. 3, Faculty

Using artificial intelligence, cybercriminals can more easily and quickly analyze illegally stolen personal data, causing more significant harm in the process. Artificial intelligence software can be utilized for malicious purposes, including creating malware.[17] One example is WormGPT, a generative AI tool based on the GPTJ language model developed for malicious purposes, including phishing and Business Email Compromise (BEC) attacks. It is designed to generate highly persuasive and strategically cunning emails for cybercrime, explicitly trained on malware-related data. WormGPT represents an advanced capability for cybercriminals, lowering the barrier to executing sophisticated attacks even for those with limited technical skills. Consequently, users become even more vulnerable to the dangers of cybercrime.[18]

Sibai created a classification of AI crimes primarily based on whether they involve human intervention (intentional or unintentional acts) or crimes committed autonomously by AI without human involvement. According to the study, we can differentiate between the following delicts:

- crimes involving human participation, which are further divisible into additional subcategories:
    - purposeful actions, wherein the actor possesses both the objective and the determination to commit an offense. This encompasses scenarios where the offender deliberately formulates and executes the criminal act.
    - Inadvertent actions, representing offenses arising from carelessness or the involvement of a third entity. This includes instances of oversight, like inadequate system design or examination, and situations where an external party manipulates the AI, leading to criminal activity.
- Crimes executed solely through machine intervention, where AI autonomously perpetrates an offense without human involvement. Here, we can see scenarios where artificial intelligence evolves to a level capable of autonomously committing crimes, absent of human intention.[19]

of Law, University of East Sarajevo, East Sarajevo, Bosnia-Herzegovina, 2023, pp. 233-246.

[17] Allan, K., *Cybercriminals are creating a darker side to AI*, Cyber Magazine, [https://cybermagazine.com/articles/cybercriminals-are-creating-a-darker-side-to-ai], Accessed 24 January 2024.

[18] Kelley, D., *WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks*, SlashNext, [https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/], Accessed 13 January 2024.

[19] Sibai, F. N., *AI Crimes: A Classification*, 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 2020. pp. 5-8.

Caldwell and others differentiate based on the security risk level.

- The first category for AI-enabled crime is when the threat level is high. This includes the previously mentioned crimes related to Deepfakes. Disrupting AI-controlled systems represents another high-level threat, targeting critical infrastructures such as power grids and transportation networks, posing risks to societal stability. AI-authored Fake News also falls into this category, using AI to fabricate news content that can manipulate public opinion and cause social unrest.
- The second is the medium threat level. This features threats like autonomous attack drones, which could shift warfare and security dynamics, and learning-based cyber-attacks, where AI algorithms adapt to bypass security measures.
- Lastly, the third category is the low threat level. Here, they mention, for example, bias exploitation, manipulating AI's decision-making process, and AI-assisted stalking, enhancing the capabilities of stalkers through data aggregation and analysis.[20]

Overall, artificial intelligence significantly transforms the crime landscape, enabling new methods for committing identity theft and fraud and creating sophisticated cyber-attacks through technologies like Deepfake and AI morphing.

5. ARTIFICIAL INTELLIGENCE AND DIGITAL EVIDENCE

In recent decades, digital evidence has been increasingly used as proof in criminal proceedings. In this context, artificial intelligence also creates new challenges and opportunities during the criminal process. On the one hand, artificial intelligence can assist in the identification, for example, through biometric data or by converting audio material into written form. From this perspective, artificial intelligence can speed up and make the operation of judicial organs more efficient. On the other hand, using digital evidence generated by artificial intelligence can pose difficulties. The emergence of Deepfake videos or audio materials and their evaluation may necessitate the involvement of forensic experts. However, involving experts will not replace the legal assessment of cases and, therefore, may require ongoing training for judges, prosecutors, and the police to understand the admissibility of digital evidence.

The research shows that the correlation between Artificial Intelligence and digital evidence manifests in several transformative ways, enhancing cybersecurity

[20] Caldwell, M.; Andrews, J. T.; Tanay, T.; Griffin, L. D., *AI-Enabled Future Crime*, Crime Science, Vol. 9, No. 1, 2020, pp. 6-12.

threats' identification, analysis, and management. Firstly, the ability of AI to rapidly analyze extensive datasets is fundamental in identifying cybersecurity threats such as malware, cyber-attacks, and phishing attempts, thereby facilitating the collection of digital evidence. This swift examination is critical for detecting threats that may produce digital proof. Furthermore, AI-driven systems excel in continuous learning, analyzing past incidents to refine protective strategies. This ongoing adaptation is crucial for collecting precise and efficient digital evidence against evolving cybersecurity threats. For example, in the event of a phishing attack, AI capabilities can quickly recognize and neutralize the threat while simultaneously collecting detailed evidence about its origin and methodology. In addition, the complex data analysis afforded by AI surpasses human analytical capabilities, particularly in identifying subtle anomalies and patterns that may indicate security breaches. This enhanced detection capability is critical for uncovering digital evidence in scenarios where it may be obscured or sophisticatedly disguised. Finally, AI significantly contributes to monitoring network security and analyzing traffic to detect potential threats. By scrutinizing network behavior, AI technologies are adept at identifying unusual activities and compiling digital evidence, elucidating the attack's nature, source, and intentions.[21] The synergy between AI and digital evidence lies in AI's superior analytical and reactive strengths. Through its ability to detect threats, automate incident response, learn from past incidents, and assist in evidence collection and analysis, AI significantly bolsters cybersecurity defenses and the efficacy of digital evidence in safeguarding against cyber threats.[22]

A study from Blount examines the application of artificial intelligence in predictive policing and its effect on the justice system. She emphasizes the critical role that artificial intelligence algorithms can play in these activities while acknowledging the challenges they introduce, especially regarding transparency and fairness in proceedings. Blount also draws attention to the reliability and objectivity of digital evidence generated by artificial intelligence, noting that these qualities significantly depend on the quality and integrity of the data used. A problem arises because artificial intelligence relies on historical data, which can lead to substantial distortions and biases in predictive policing operations. This may misdirect the operations of judicial bodies and infringe upon the principles of fair procedure. Concerns about the presumption of innocence are also raised, as individuals or locations deemed high risk based on digital evidence might be subjected to intensified surveillance, potentially leading to biases against them. In summary, although the use of artificial intelligence in crime prevention offers potential benefits, the

[21] Bagó, P., *Cyber Security and Artificial Intelligence*, Economy and Finance, Vol. 10, Iss. 2, June 2023, pp. 195-211. [doi: 10.33908/EF.2023.2.5.]

[22] *Ibid.*

implications of its use in the production and utilization of digital evidence require a thorough examination of ethical, legal, and procedural safeguards to ensure the fairness and integrity of the criminal justice system. The relationship between artificial intelligence and digital evidence underscores the need for transparency, accountability, and fair access to evidence to uphold the norms of fair procedure.[23]

In their research, Constantini and colleagues explore using artificial intelligence to enhance the management and analysis of digital evidence in criminal investigations and forensic science. They argue that AI can significantly streamline examining digital evidence, which is traditionally labor-intensive and intricate. AI, through tools like Answer Set Programming (ASP), can take the massive amounts of data involved in digital evidence and process it quickly and efficiently. This means investigators can form hypotheses or theories about a case faster and more accurately. In simpler terms, AI can help sift through digital clues much faster than humans, helping speed up investigations and make them more effective.[24]

6. CRIME PREVENTION

We see numerous opportunities and challenges when examining the interplay between artificial intelligence and crime prevention. AI-based technologies can enhance societal surveillance by filtering out criminals and assisting in the reintegration of convicted individuals after their release, further reducing the rate of recidivism. In the future, AI-based probation officers could aid convicts in reintegration, offering more extensive monitoring and providing constant advice after release. The National Institute of Justice in the United States has already funded projects exploring AI's potential benefits in these areas to introduce reforms in the future.[25]

Delving deeper into the practical applications of AI, Raaijmakers' research highlights[26] its transformative potential concerning crime prevention. The author discusses how AI technology can be broadly applied in various areas, including creat-

[23] Blount, K., *Seeking Compatibility in Preventing Crime with Artificial Intelligence and Ensuring a Fair Trial*, Masaryk University Journal of Law and Technology, Vol. 15, No. 1, 2021, pp. 25-51, [https://doi.org/10.5817/MUJLT2021-1-2].

[24] Costantini, S.; De Gasperis, G.; Olivieri, R., *Digital Forensics and Investigations Meet Artificial Intelligence*, Annals of Mathematics and Artificial Intelligence, Vol. 86, 2019, pp. 193-229, [https://doi.org/10.1007/s10472-019-09632-y].

[25] Martin, E.; Moore, A., *Tapping Into Artificial Intelligence: Advanced Technology to Prevent Crime and Support Reentry*, in: Corrections Today, May/June 2020, pp. 28-32, National Institute of Justice, US Department of Justice, Office of Justice Programs, United States of America.

[26] Raaijmakers, S., *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*, IEEE Security & Privacy, Vol. 17, No. 5, 2019, pp. 74-77, [https://doi.org/10.1109/MSEC.2019.2925649].

ing suspicious profiles, traffic pattern analysis, investigation of financial flows on the dark web, detection of child pornography, and identification of anomalies in surveillance recordings. Within this context, AI can provide substantial assistance to law enforcement agencies in their investigative activities and in enhancing the efficiency of digital evidence management, ultimately contributing to the success of investigations.

Additionally, we can highlight the capabilities of artificial intelligence in recognition technologies, which can also assist authorities. For instance, ShotSpotter uses AI to detect gunfire in real time through sound data recognition. This technology is already operational in over 90 cities, significantly enhancing the police's response time to gun-related crimes. Furthermore, AI can be used to improve security camera systems. These cameras do not merely record video but can be enhanced with various techniques for facial recognition and license plate reading. By applying AI, identifying suspects becomes more accessible, which in turn can increase public safety. AI also offers support to authorities in making placement decisions. In this context, tools like Hart (Harm Assessment Risk Tool) assess the risks associated with suspects and those on probation. With risk assessment software, decisions regarding arrests and conditional releases can be made more efficiently.[27]

Roksandic and colleagues also explored the role of artificial intelligence in law enforcement and criminal identification. They noted AI's capability to process large databases more efficiently, assisting in various law enforcement activities such as penalty enforcement, assessing prisoner escape risks, or preventing terrorist attacks. However, they also highlighted concerns about AI's use potentially infringing fundamental human rights. AI systems can create the illusion of absolute precision in predicting events, potentially leading to discriminatory decisions based on gender or age in investigations and detentions. The study mentions the development of algorithms by the University of Houston, which are used to predict suspicious and criminal behavior through camera networks. These algorithms analyze clothing, movement, and skeletal structure to identify persons of interest, helping prevent security threats more effectively. The collaboration between the Cologne Prosecutor's Office and Microsoft is another honorable example. Together with the Ministry of Justice of North Rhine-Westphalia and Microsoft Germany, they developed a hybrid cloud-based system that utilizes AI algorithms to detect and categorize online child pornography while anonymizing the image files. This collaboration led to faster interventions and significantly reduced the psychological stress on the

[27] Faggella, D., *AI for Crime Prevention and Detection – 5 Current Applications*, Emerj, [https://emerj.com/ai-sector-overviews/ai-crime-prevention-5-current-applications/], Accessed 2 February 2024.

personnel involved, demonstrating a practical application of AI in safeguarding public security while managing sensitive data.[28]

The integration of artificial intelligence into crime prevention efforts brings its own set of challenges alongside its benefits. A primary concern is the potential for AI systems to perpetuate biases, mainly if they depend heavily on historical data. Such biases could lead to unfair profiling of individuals as potential offenders based on superficial characteristics, undermining the presumption of innocence—a cornerstone of the criminal justice system.

Raaijmakers raises essential considerations about the transparency and accountability of AI technologies in legal settings. He argues that for AI-generated evidence to be deemed valid in court, there must be clear documentation and comprehension of the processes, models, and algorithms that underpin these technologies. This transparency is crucial for establishing a legal framework that ensures these innovations do not infringe upon the principles of justice. Furthermore, Raaijmakers emphasizes the importance of continuous professional development for those in law enforcement. Adequate training and the necessary technological infrastructure are essential for law enforcement personnel to effectively utilize AI tools, ensuring they are both efficient and ethically deployed.[29]

7. SUMMARY AND CONCLUSIONS

To encapsulate, AI represents a dual-faced phenomenon within the modern digital landscape, marked by its potential to enrich and complicate public safety and cybersecurity aspects. Our comprehensive review sheds light on this intricate interplay, drawing attention to AI's multifaceted implications for societal frameworks.

The evolution of autonomous vehicles is a prime example of the legal and ethical dilemmas accompanying AI's integration into everyday life. The question of accountability — whether it should be attributed to manufacturers, programmers, or the AI systems themselves — highlights the need for dynamic legal frameworks capable of navigating the complexities introduced by technological progress.

Moreover, AI's role in generating and analyzing digital evidence shows a significant shift in the landscape of criminal investigations. While AI promises to enhance the efficiency and precision of such inquiries, AI-generated evidence's integrity and legal validity demand thorough examination to uphold justice.

[28] Roksandić, S. *et. al. op. cit.*, note 12, p. 1227.

[29] Raaijmakers, S. *op. cit.*, note 26, pp. 74-77.

In the realm of crime prevention, from predictive policing to the deployment of advanced public safety solutions like gunfire detection systems, AI's potential is profoundly evident. However, this potential is moderated by the ethical issues it raises, particularly regarding the risk of perpetuating biases and violating privacy rights. These concerns highlight the necessity of maintaining a reasonable balance between innovation and ethical responsibility.

From our analysis, several key conclusions emerge: Firstly, the advent of AI requires ongoing adaptation within legal and regulatory frameworks to adequately address the new dimensions of accountability and evidence it introduces. Secondly, applying AI in crime prevention and law enforcement demands a thoughtful approach, ensuring that technological advancements do not overshadow fundamental ethical standards and human rights. Hence, a comprehensive legal framework is essential to avoid loopholes in the legal system. The European Union has already set a precedent with the General Data Protection Regulation. The future implementation of the AI Act will mark a significant regional step forward. While the EU AI Act is a commendable example of regulating AI within a regional framework, it's also crucial to highlight the need for a coordinated global effort. For instance, the United Nations could establish comprehensive guidelines that address critical issues such as liability questions related to AI and the use of AI in surveillance for crime prevention while protecting human rights. These guidelines could then be adopted as part of an international convention, ensuring a worldwide standardized approach to AI governance. This would help harmonize regulations, promote ethical AI use, and protect fundamental rights globally. Additionally, the effective integration of AI in surveillance and crime prevention should include extensive training programs for judicial personnel. Such training would ensure that law enforcement and judicial officers are well-prepared to engage with AI-driven tools and data, enabling them to make informed decisions and uphold justice while respecting human rights. This comprehensive approach would bolster the capacity of judicial systems to utilize AI ethically and efficiently.

In conclusion, the future of AI in societal security and justice relies on cooperation among technologists, legal experts, and policymakers. They need to develop a regulatory framework that maximizes AI's benefits for public safety while addressing potential issues. Working together, they can enhance public safety and the legal system while carefully managing ethical challenges.

REFERENCES

BOOKS AND ARTICLES

1. Agarwala, A. N.; R. Nalini, *Manipulating Faces for Identity Theft via Morphing and Deepfake: Digital Privacy*, in: „Deep Learning," 2023, Vol. 48, pp. 223-241
2. Andrea, K.; László, K.; Dávid, T., *Digital Dangers of Smartphones*, Journal of Eastern-European Criminal Law, Vol. 7, No. 1, 2020, pp. 36-49
3. Bagó, P., *Cyber Security and Artificial Intelligence*, Economy and Finance, Vol. 10, Iss. 2, June 2023, pp. 189-212, [https://doi: 10.33908/EF.2023.2.5.]
4. Blount, K., *Seeking Compatibility in Preventing Crime with Artificial Intelligence and Ensuring a Fair Trial*, Masaryk University Journal of Law and Technology, Vol. 15, No. 1, 2021, pp. 25-51, [https://doi.org/10.5817/MUJLT2021-1-2].
5. Caldwell, M.; Andrews, J. T.; Tanay, T.; Griffin, L. D., *AI-Enabled Future Crime*, Crime Science, Vol. 9, No. 1, 2020, pp. 1-13
6. Costantini, S.; De Gasperis, G.; Olivieri, R., *Digital Forensics and Investigations Meet Artificial Intelligence*, Annals of Mathematics and Artificial Intelligence, Vol. 86, 2019, pp. 193-229, [https://doi.org/10.1007/s10472-019-09632-y]
7. Csitei, B., *Self-Driving Cars and Criminal Liability*, Debreceni Jogi Műhely, 17th vol., No. 3-4, National University of Public Service, Faculty of Public Governance and International Studies, Department of Civilistics, 30 December 2020, pp. 34-46, [DOI 10.24169/DJM/2020/3-4/4]
8. Faggella, D., *AI for Crime Prevention and Detection – 5 Current Applications*, Emerj, [https://emerj.com/ai-sector-overviews/ai-crime-prevention-5-current-applications/], Accessed 2 February 2024
9. Herke, Cs., *A kiberbűnözés és a teljesen önvezető járművek*, in: Barabás, A. T.; Christián, L. (eds.), Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est, Ludovika Egyetemi Kiadó, Budapest, 2021, pp. 211-221
10. Joon, K., *Criminal Liability of Traffic Accidents Involving Autonomous Vehicles*, Central Law Review, Vol. 19, No. 4, 2017, pp. 47-82, [https://doi.org/10.21759/caulaw.2017.19.4.47]
11. Lohmann, M. F., *Liability Issues Concerning Self-Driving Vehicles*, European Journal of Risk Regulation, Vol. 7, No. 2, 2016, pp. 335-340, [doi: 10.1017/S1867299X00005754]
12. Martin, E.; Moore, A., *Tapping Into Artificial Intelligence: Advanced Technology to Prevent Crime and Support Reentry*, in Corrections Today, May/June 2020, pp. 28-32, National Institute of Justice, US Department of Justice, Office of Justice Programs, United States of America
13. Manea, T.; Ivan, D. L., *AI Use in Criminal Matters as Permitted under EU Law and as Needed to Safeguard the Essence of Fundamental Rights*, International Journal of Law and Cyber Warfare, Vol. 1, No. 1, 2022, pp. 18-32.
14. Raaijmakers, S., *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*, IEEE Security & Privacy, Vol. 17, No. 5, 2019, pp. 74-77, [https://doi.org/10.1109/MSEC.2019.2925649]
15. Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: Where Do We Stand?,* in: "45th Jubilee International Conven-

tion on Information, Communication and Electronic Technology (MIPRO)", 2022, pp. 1225-1232

16. Sibai, F. N., *AI Crimes: A Classification*, 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 2020. pp. 1-8
17. Tóth, D., *The Criminal Law Protection of Personal Data in Hungary*, in Ćeranić, D.; Ivanović, S.; Lale, R.; Aličić, S. (eds.), Collection of Papers „Law Between Creation and Interpretation," Vol. 3, Faculty of Law, University of East Sarajevo, East Sarajevo, Bosnia-Herzegovina, 2023, pp. 233-246
18. Tóth, D., *The Theories and Regulation of Criminal Liability of Legal Persons in Hungary*, Journal of Eastern-European Criminal Law, Vol. 6, No. 1, 2019, pp. 178-189

WEBSITE REFERENCES

1. Allan, K., *Cybercriminals are creating a darker side to AI*, Cyber Magazine, [https://cybermagazine.com/articles/cybercriminals-are-creating-a-darker-side-to-ai], Accessed 24 January 2024
2. Faggella, D., *AI for Crime Prevention and Detection – 5 Current Applications*, Emerj, [https://emerj.com/ai-sector-overviews/ai-crime-prevention-5-current-applications/], Accessed 2 February 2024
3. Kelley, D., *WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks*, SlashNext, [https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/], Accessed 13 January 2024
4. Neuman, S., *Uber Reaches Settlement With Family Of Arizona Woman Killed By Driverless Car*, THE TWO-WAY, NPR, [https://www.npr.org/sections/thetwo-way/2018/03/29/597850303/uber-reaches-settlement-with-family-of-arizona-woman-killed-by-driverless-car], Accessed 29 March 2024
5. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,* [https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf], Accessed 29 March 2024
6. *Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company*, Trend Micro, [https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company], Accessed 5 September 2023