ENCUENTROS | Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico pp: 140-159

ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY: EXPLORING THE LEGAL IMPLICA-TIONS OF AI-ENABLED CRIMES

Inteligencia artificial y responsabilidad penal: exploración de las implicaciones legales de los delitos impulsados por la IA

Thamer Najm Abdullah Abbas
Al-Rafidain University College. Baghdad, Iraq.
thamer.najem71@ruc.edu.iq
https://orcid.org/0009-0008-0961-2085

Ali Akram Kadhim
Al-Mamoon University College. Baghdad, Iraq.
ali.a.kadhim@almamonuc.edu.iq
https://orcid.org/0009-0001-7767-8691

Raed Hameed
Al-Turath University, Baghdad, Iraq.
raed.hamid@turath.edu.iq
https://orcid.org/0000-0002-5008-4893

Nameer Hashim Qasim
Cihan University Sulaimaniya Research Center (CUSRC), Sulaymaniyah City 46001, Kurdistan/Iraq.
nameer.qasim@sulicihan.edu.krd
https://orcid.org/0000-0002-7283-0594

Este trabajo está depositado en Zenodo:
DOI: https://doi.org/10.5281/zenodo.13386675

ABSTRACT

Incorporating artificial intelligence (AI) has significantly influenced several facets of daily existence, notably revolutionizing crime prevention and investigation.The article aims to investigate the legal ramifications of criminal conduct enabled by AI, focusing on the intricate issues surrounding criminal liability in cases involving AI systems engaged in criminal activity. The study used a qualitative technique to investigate legal professionals' challenges in prosecuting these acts and the shortcomings in current legislative frameworks. The findings underscore the need to establish a robust legal framework especially tailored to address the complexities of illicit activities enabled by artificial intelligence. In order to successfully address the challenges presented by AI-enabled crimes and establish responsibility and openness in the era of digital technology, it is crucial to implement a multidisciplinary approach that integrates expertise from several domains like law, ethics, and technology.

Keywords: Artificial intelligence, criminal liability, legal implications, AI-enabled crimes.

RESUMEN

La incorporación de la inteligencia artificial (IA) ha influido significativamente en varias facetas de la existencia diaria, revolucionando notablemente la prevención e investigación del delito. El artículo tiene como objetivo investigar las ramificaciones legales de la conducta delictiva posibilitada por la IA, centrándose en las intrincadas cuestiones que rodean la responsabilidad penal en los casos que involucran sistemas de IA involucrados en actividades delictivas. El estudio utilizó una técnica cualitativa para investigar los desafíos de los profesionales del derecho en el enjuiciamiento de estos actos y las deficiencias de los marcos legislativos actuales. Los hallazgos subrayan la necesidad de establecer un marco legal sólido especialmente diseñado para abordar las complejidades de las actividades ilícitas posibilitadas por la inteligencia artificial. Para abordar con éxito los desafíos que presentan los delitos posibilitados por la IA y establecer la responsabilidad y la apertura en la era de la tecnología digital, es crucial implementar un enfoque multidisciplinario que integre la experiencia de varios dominios como el derecho, la ética y la tecnología.

Palabras claves: Inteligencia artificial, responsabilidad penal, implicaciones legales, delitos facilitados por IA.

RECIBIDO: 01/02/2024 ACEPTADO: 19/05/2024

INTRODUCTION

Artificial intelligence (AI) has brought about significant advancements in various industries, from healthcare to finance. However, the rapid development of AI has also raised concerns about its potential to be used for criminal purposes. As AI systems become more sophisticated, they also have the potential to be used in criminal activities, creating new challenges for the legal system [1].

The legal implications of AI-enabled crimes are complex, particularly with regard to criminal liability. Currently, there is no clear legal framework in place to address the issue of AI-assisted crimes. This creates a legal gray area, which makes it difficult to attribute blame and determine who should be held responsible for such crimes [2].

One of the key issues with AI-enabled crimes is the question of accountability. AI systems have the potential to operate autonomously and make decisions independently, which raises the question of who is responsible if an AI system is used to commit a crime. Should it be the person who created the AI system, the person who trained it, or the AI system itself? Moreover, if the AI system makes a mistake, which is held accountable for the consequences? [3]

Algorithmic transparency is another important issue that needs to be addressed when it comes to AI-enabled crimes. If AI systems are used to make decisions that impact people's lives, such as in the criminal justice system, there is a need for transparency in how these decisions are made. This is crucial for ensuring that the decisions made by AI systems are fair and unbiased [4].

The legal implications of AI-enabled crimes are complex and have raised concerns about its potential to be used for criminal purposes. There is currently no clear legal framework in place to address the issue of AI-assisted crimes, creating a legal gray area, which makes it difficult to attribute blame and determine who should be held responsible for such crimes. Several scholars have discussed the ethical implications of algorithms and AI in society, including the need for transparency and accountability. For instance, Mittelstadt et al. [5] mapped the debate on the ethics of algorithms, while Floridi and Cowls proposed a unified framework of principles for AI in society [6]. Moreover, Zeadally reviewed emerging threats and countermeasures of AI-enabled cybercrime [7], while Holm proposed a fiduciary duty for AI to address the AI-legal black box [8]. Hongjun et al. highlighted seven traps to avoid in AI ethics [9]. These works highlight the need for collaboration between legal and technical experts to develop a legal framework that takes into account the unique challenges posed by AI-enabled crimes, including determining criminal liability and ensuring algorithmic transparency. Moreover, ethical considerations and safeguards to protect vulnerable populations should be addressed to ensure the protection of human rights. As AI systems become more prevalent in society, it is crucial to explore the legal implications of AI-enabled crimes and develop a comprehensive approach to address these emerging legal challenges [10].

There are also ethical considerations that need to be taken into account when it comes to AI-enabled crimes. For example, there is a risk that AI systems could be used to target vulnerable populations or perpetuate existing biases and discrimination. This raises important questions about the role of AI in society and its impact on human rights [11].

According to a report by the World Economic Forum, the global market for AI is projected to reach $90 billion by 2025, demonstrating the significant growth of AI technology. However, a study by Europol found that AI is already being used by cybercriminals to develop more sophisticated attacks, highlighting the need for robust legal frameworks to address the issue of AI-enabled crimes. Furthermore, a

survey by PwC found that 63% of business leaders believe that AI will be a key driver of growth, but 76% also believe that the ethical risks associated with AI are a concern. These statistics highlight the need for a comprehensive approach to address the legal, ethical, and societal implications of AI-enabled crimes [12], [13].

This article aims to explore the legal implications of AI-enabled crimes, including criminal liability, algorithmic transparency, and ethical considerations. It examines the need for collaboration between legal and technical experts to develop a legal framework that takes into account the unique challenges posed by AI-enabled crimes. Furthermore, this article highlights the importance of understanding the risks and benefits of AI technology while ensuring the protection of human rights and safeguarding vulnerable populations. Overall, this article provides an overview of the legal landscape in AI-enabled crimes and the need for a comprehensive approach to address these emerging legal challenges.

To address these challenges, there is a need for collaboration between legal and technical experts to develop a legal framework that takes into account the unique challenges posed by AI-enabled crimes. This framework should include clear guidelines for determining criminal liability and ensuring algorithmic transparency. It should also address the ethical implications of AI-enabled crimes and provide safeguards to protect vulnerable populations.

In conclusion, as AI systems become more prevalent in society, it is essential to explore the legal implications of AI-enabled crimes. Criminal liability, algorithmic transparency, and ethical considerations are all crucial aspects that need to be taken into account when developing a legal framework. By working together, legal and technical experts can ensure that the benefits of AI technology are realized while minimizing the risks posed by AI-enabled crimes.

1.1. The study objective

This article discusses the difficulties of assigning criminal responsibility to AI systems and the legal ramifications of AI-enabled crimes. The paper will look at concerns including algorithmic transparency, accountability, ethical considerations, and the necessity for successful cooperation between legal and technological specialists. The article will also cover the difficulties in prosecuting crimes facilitated by artificial intelligence and the need for a legislative framework to deal with this newly emergent criminal behavior. The article aims to raise awareness of the legal ramifications of AI-enabled crimes and the need for a holistic strategy to address these issues.

1.2. Problem statement

The likelihood of AI systems being utilized for illegal activity increases as they advance. When an AI system is utilized to commit a crime, this raises serious concerns regarding criminal responsibility. The legal ramifications of AI-enabled crimes are intricate and multidimensional, incorporating concerns like algorithmic transparency, responsibility, and ethical considerations. Prosecutors also need help with cases involving crimes aided by artificial intelligence since the underlying technology is frequently complex and challenging to grasp. The legal ramifications of AI-enabled crimes must thus be investigated, along with the possibilities and threats in this new field of criminal behavior. The ultimate aim is to create a complete legal framework that meets the issues provided by AI-enabled crimes and guarantees that people and institutions are held responsible for their acts.

LITERATURE REVIEW

The article on artificial intelligence and its effects on criminal responsibility and ethics thoroughly analyzes the advantages and challenges of integrating AI technology into legal and ethical frameworks. This research

synthesizes significant data from notable publications in the field, highlighting the interdependent connection between the advancement of artificial intelligence and the evolving dimensions of criminal justice, ethical considerations, and cybersecurity.

In Spesivov's study, the author examines the possible ramifications of artificial intelligence (AI) and predictive technologies within criminal justice. The study suggests that using AI significantly enhances decision-making processes in this sector. Nevertheless, discussions are taking place to recognize the need for robust legal and ethical frameworks for governing the use of new technologies [1]. Klemenc and Trittenbach emphasize the importance of model selection criteria that favor reducing possible damage as they examine the concerns associated with adversarial assaults on AI models [2]. This issue directly impacts the reliability and credibility of AI systems in sensitive fields like criminal justice.

Hayward and Maas provide an extensive manual for criminologists on the convergence of AI and crime. The authors analyze the advantages and disadvantages of AI technology in the context of criminal activities and their subsequent investigation [3]. Mittelstadt et al. enhance the ethical discourse by studying the ethical implications of algorithms. The authors highlight the challenges of ensuring justice, accountability, and transparency in algorithmic decision-making [5].

Floridi et al. propose an ethical paradigm aimed at fostering a society that harnesses the advantages of AI while successfully mitigating its potential risks. The framework comprises concepts and recommendations to achieve a harmonious equilibrium between the opportunities and obstacles posed by AI [6]. Zeadally et al. bolster this claim by examining how artificial intelligence (AI) may be used to augment cybersecurity, a vital element in protecting digital infrastructures from AI-enabled crimes [7]. On the other hand, Holm supports the idea that AI algorithms should not be transparent and argues that there are situations when 'black box' AI systems are necessary [8]. This perspective creates apprehensions about the clarity and accountability of AI's use in legal settings.

Hongjun et al. conducted a thorough analysis of the ethical hazards associated with AI decision-making, emphasizing the need for ethical governance in the implementation of AI [9]. Naik et al. examine the legal and ethical consequences of artificial intelligence (AI) in the healthcare field, with a particular emphasis on the allocation of accountability [10]. Zhou and Nabus go further into the ethical implications of AI by examining the capabilities of DALL-E and the possible challenges it poses [11].

Nightingale and Farid highlight the challenge of distinguishing between AI-generated faces and authentic ones, leading to concerns over trust and authenticity in digital representations [14]. Altayari et al. investigate the role of artificial intelligence (AI) in the delivery of forensic evidence, emphasizing its potential to revolutionize forensic methodologies [15]. Vojtuš et al. examine the complex issue of AI and criminal responsibility, outlining the challenges and proposing solutions for attributing guilt in crimes enabled by AI [16]. Sivaram et al. investigate the rise of illegal behaviors facilitated by artificial intelligence, emphasizing evading spam filters. They emphasize adversarial machine learning as a significant risk [17].

The article highlights the need to build comprehensive legal, ethical, and technical frameworks to tackle the challenges posed by AI in many domains, particularly in ensuring equity, security, and ethical standards in the age of artificial intelligence.

AI-ENABLED CRIMES AND AUTONOMOUS SYSTEMS

The preliminary examination collected examples of actual or possible interactions between AI and crime. Both terms were mainly used. The examples come from academic literature, media, and popular culture, which may be a barometer of contemporary anxieties.

The provided instances were classified into one of three major groups according to the nature of the link between criminal behavior and AI:

• An error in artificial intelligence, such as being unable to unlock a device that relies on facial recognition.

• The use of AI in law enforcement tasks, such as identifying illicit financial market activities. Committing a crime using artificial intelligence; one example is blackmailing victims with "deep fake" videos [17].

Table 1 compiles a variety of AI-facilitated illegal activities and classifies them into major categories. Some categories overlap, but this chart should help you consider how artificial intelligence may be used unethically. In addition, it might provide a basis for developing regulatory and technical responses to these crimes.

Legal liability and accountability for AI-enabled crimes involving autonomous systems present unique challenges. Autonomous systems are those that operate independently of human oversight and can make decisions on their own. Such systems include autonomous vehicles, crewless aircraft, and robotic systems[18].

One crime that may be committed with the help of AI is the employment of drones for nefarious activities like drug or weapon smuggling. Criminal organizations may use drones to carry narcotics over borders or into prisons, making it more difficult for authorities to detect and disrupt criminal activity.

They were additionally labeled with one or more rough taxonomic classifications describing the technologies or vulnerabilities involved:

Table 1. AI-Enabled crimes: examples across taxonomic classes

Taxonomic class	Example of al-enabled Crime
Adversarial perturbations	Adversarial attacks on facial recognition systems to bypass security
Autonomous vehicles	Using autonomous vehicles for terrorist attacks or as a getaway vehicle for theft
Fake content	Spreading fake news or propaganda using AI-generated content
Automated snooping	Using AI-enabled surveillance to spy on individuals or organizations
Robotics	Using AI-powered robots for criminal activities such as theft or vandalism
Biometrics	Using stolen biometric data for identity theft or unauthorized access
Precognition	Using AI systems to predict criminal activity or exploit vulnerabilities in security systems
Anomaly detection	Using AI to detect unusual patterns of behavior to identify potential targets for theft or other crimes
Computer Science, not AI	Exploiting vulnerabilities in computer systems using traditional hacking techniques
Automated software	Using AI-enabled malware to infect and control computer systems
Cryptography	Using AI to crack encryption codes to access sensitive data
AI blowback	Unintended consequences of AI systems leading to security breaches or other crimes

The March 2020 Cam4 data leak was the most significant data breach up to that point in time (August 2022). As a result of this hack, almost 10 billion documents were made accessible online. In 2013, a cyberattack against Yahoo caused the second-greatest data breach in history. During an investigation, the business changed its original estimate and said three billion user accounts had been hacked, rather than the initial one billion. Next, in March of 2018, over 1.1 billion records were exposed due to a breach in the security of India's id Card database, Aadhaar. Biometric data like fingerprint scans and identification numbers were among these. They may be used for various governmental tasks, from applying for benefits to establishing a bank account (Fig.1).

The prospect that exists, for instance, that criminals would use autonomous vehicles in the case of a robbery or terrorist attack as getaway automobiles is still another example. Self-driving cars powered by artificial intelligence (AI) might make it easier for criminals to depart the scene of an incident and evade arrest by following a predetermined course.

Using autonomous systems for criminal purposes presents severe legal responsibility and liability issues. Who should be held accountable if an autonomous system is used to commit a crime? Who should be responsible for fixing the system, its trainers or the system itself? Who is responsible if an autonomous system makes a mistake or causes harm?

A North Dakota man was jailed this year after he shot at a police robot that was stationed on his property. This incident shows how AI-enabled surveillance equipment might face resistance and violence from the general people.

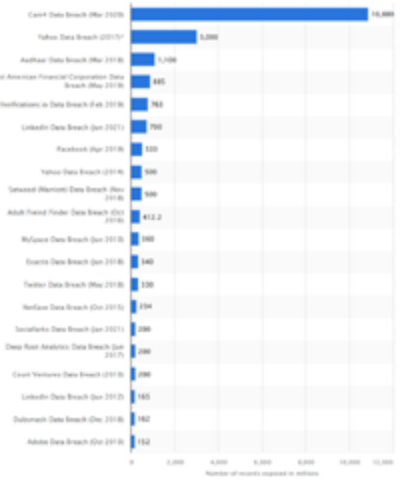
In 2018, Chinese police used facial recognition technology to apprehend a criminal in the audience of a play. In a country like China, where the authorities have been criticized for limiting individual freedom, this incident raises concerns regarding implementing AI-enabled surveillance tools.

In 2018, a man in Japan was arrested for allegedly using a drone to drop leaflets on a nuclear power plant. This incident highlights the risk of drones equipped with artificial intelligence being used for criminal activities like espionage and sabotage.

These incidents highlight the need for international cooperation in the fight against AI-enabled crimes using autonomous systems. Legal frameworks that address the unique challenges posed by AI technology are required to deter and punish such offenses and provide accountability and redress for victims [19].

Legislative frameworks that address using autonomous systems for illicit purposes are needed to ensure accountability and end AI-enabled crimes. These models should account for the unique challenges posed by autonomous systems and provide criteria for assigning blame in cases involving the use of AI.

The illicit use of autonomous systems creates significant challenges for the justice system. By establishing legal frameworks that deal with these concerns, we can guarantee that AI technology is utilized safely and responsibly and lessen the likelihood of damage from AI-enabled crimes [20].



Machine Learning, Cybersecurity and Data Privacy

All three issues—machine learning, cyber security, and data privacy—are intertwined and fundamental to the reliable and secure implementation of AI systems.

Machine learning uses algorithms and statistical models to let AI systems learn from data, spot patterns, and make decisions without being explicitly programmed. However, the quantity and quality of data used to train machine learning models significantly impact the models' quality and accuracy. It undermines confidence in machine learning algorithms, particularly problematic in politically charged areas like criminal justice [21].

Cybersecurity keeps digital infrastructure from threats, including hacking, theft, and destruction. Cybersecurity has gained prominence recently due to the increasing prevalence of artificial intelligence (AI) systems in critical infrastructures like the nation's power grids and financial networks. Threats like AI-based malware and the potential for AI systems to be hacked arise due to AI's application in cybersecurity [7].

Phishing continues to pose a significant risk to businesses across sectors, as shown by the fact that financial institutions were the target of more than 25% of all phishing schemes [22] in the first quarter of 2022 (Fig. 2). Such attacks may do severe damage to a company's reputation and bottom line. It is interesting to see that webmail and browser-based phishing assaults predominated. This highlights the need for a skilled workforce who can see and respond to phishing attempts and secure software and webmail services.

Due to the widespread nature of phishing attacks, businesses must prioritize cybersecurity and implement proactive measures to protect themselves. A possible answer is implementing two-factor authentication and other types of advanced security, conducting regular security audits, and teaching employees to spot and avoid phishing scams.

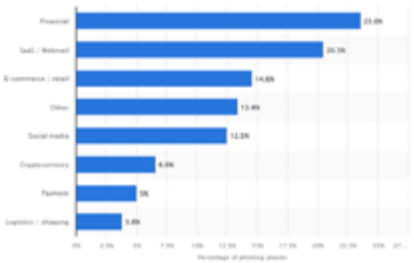


Figure 2. Phishing attack vectors as of the first quarter of 2022

The protection of private and confidential data against unauthorized access, usage, and disclosure is known as data privacy. Access to massive amounts of data, including often sensitive personal information, is required to use AI systems. This causes privacy concerns, particularly in areas like healthcare and finance, where the adoption of AI might have unintended repercussions like bias and loss of control [10].

The fields of machine learning, cybersecurity, and data privacy are all subject to a wide range of rules and regulations.

Privacy and Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) is a piece of EU law that will take effect in 2018. It lays forth rules for how companies based in the EU may and must collect, use, and store customers' private information [23].

The CCPA (California Consumer Privacy Act) was enacted as a statute in the state in 2020. It protects California citizens from having their data sold and allows them to request that their data be deleted [24].

The federal government has passed the Computer Fraud and Abuse Act (CFAA), making committing fraud or hacking a computer system illegal. It lays forth criminal and civil penalties for anyone who break the law and gain unauthorized access to computers and networks [25].

Organization of the National Standards and Technologies (NIST) Guidelines for enhancing cybersecurity in organizations of all sizes and kinds may be found in the NIST Cybersecurity Framework. It provides a means of discovering, assessing, and managing online threats [26].

The Algorithmic Accountability Act is a piece of legislation presented in the United States Congress to control how algorithms are used in policymaking. It requires organizations to investigate and remedy the potential for discriminatory or biased outcomes from using algorithms [27].

Protecting the privacy of individuals' medical records is a top priority for the United States federal government, which is why it enacted the Health Insurance Portability and Accountability Act. Care providers should have secure, convenient access to confidential medical records. Medical records should be kept private, stored safely, and easy for everyone involved in the care continuum to get to [28].

The top credit card companies made the Payment Card Industry Data Security Standard to protect their customers' credit card information. To protect customers' credit card data, stores, and other organizations must take and maintain up-to-date security procedures.

The Cybersecurity Information Sharing Act is a federal law in the United States that encourages businesses and government agencies to share cybersecurity information to strengthen their defenses against cyberattacks. It provides protections, such as immunity from liability, for private companies that provide information to the government.

Electronic communications surveillance and disclosure in the United States are governed under the Electronic Communications Privacy Act (ECPA). Law enforcement agencies will need a warrant to intercept electronic communications, including email and text messages, and the legislation sets standards for the disclosure of such information by service providers [29].

The FCRA regulates the collection, dissemination, and use of consumers' personal credit information in the United States. Credit reporting agencies are required to safeguard their customers' personal information, and consumers can dispute inaccurate information that may appear on their credit reports [30].

In general, the development and deployment of AI systems must account for the significant difficulties posed by machine learning, cybersecurity, and data privacy to ensure these technologies' safe and effective use.

ROBOTIC PROCESS AUTOMATION, DIGITAL FORENSICS AND HUMAN-MACHINE COLLABORATION

Automation and robotics automation (RPA), digital forensics, and human-machine cooperation are three significant areas where AI and cybersecurity merge. These innovations are crucial for enhancing the effec-

tiveness of information security and lowering risks to individuals and organizations. This article will discuss these technological advancements in detail and provide concrete examples of how they might be used in cybersecurity.

In robotic process automation (RPA), software robots perform regular operations automatically. Using RPA, businesses can boost output, reduce error rates, and free up workers to focus on more complex tasks. Robotic process automation (RPA) might be used in the cybersecurity industry to streamline tasks like data entry, system backups, and software updates. According to recent research by Grand View Research, the global market for RPA is expected to reach $25.56 billion by 2027, expanding at a CAGR of 33.6% over that time. The increasing need for automation across various industries, including cybersecurity, is fueling this growth [31].

Collecting, evaluating, and archiving forensic evidence in court is known as "digital forensics." Regarding cybersecurity, digital forensics is essential for tracking down the origin of an attack, determining who is responsible for it, and ultimately prosecuting the perpetrators. Digital forensics allows for the recovery of deleted data, the examination of network traffic, and the detection of malware. MarketsandMarkets projects that the global digital forensics market will increase from $9.9 billion at the end of 2023 to $18.2 billion by 2028, representing a CAGR of 12.9% [32].

"Human-machine collaboration" refers to using AI tools to assist people in strenuous activities. The cybersecurity industry may benefit from human-machine collaboration to improve threat detection and response, enhance the speed and precision of decision-making, and augment the expertise of security analysts. Machine learning methods may be used on large data sets to spot patterns or outliers that indicate an impending cyberattack. With this information in hand, the operator may take appropriate measures. By 2025, Gartner predicts that half of all SOCs will use machine learning or some AI to supplement the work of human analysts [33].

The use of RPA, digital forensics, and human-machine interaction in cybersecurity has the potential to improve efficiency, accuracy, and effectiveness. Nonetheless, the use of this technology has its related dangers and difficulties.

The potential for malfunctions and security holes in RPA is a significant reason for concern. For instance, an incorrectly built RPA system might inadvertently compromise system security. The malicious use of a hacked RPA system is another concern. If a business is serious about avoiding these dangers, it must first guarantee that its RPA systems are correctly configured and protected [34].

Digital forensics also raises questions about data privacy and security. It is essential to ensure that people's privacy rights are respected and that personal data is safeguarded when collecting and analyzing digital evidence. Large volumes of data generated during digital forensics investigations may require more work to process and assess. In order to address these challenges, firms should implement robust policies and procedures for maintaining digital evidence and acquire the necessary tools and expertise.

Human-machine interaction raises concerns about AI systems taking over human jobs. Although artificial intelligence (AI) systems may improve human performance in certain areas, they cannot replace people in fields like cybersecurity, where creative problem-solving, empathy, and analytical thinking are essential. Organizational efforts to foster inte-

raction between humans and machines should complement rather than replace existing human capabilities. To achieve this, it is crucial to have employees participate in developing and implementing RPA and AI systems, provide training and education to ensure familiarity with their usage and build processes that combine the best of automation with human involvement [35].

One example of successful human-machine collaboration in cybersecurity is using AI-powered threat detection systems. These systems can sift through mountains of data from many sources to find vulnerabilities in your network's defenses. Nevertheless, they could be better, overlook important details, or provide false positives. Human connection is crucial for validating the threat and selecting the appropriate response. Using AI's speed and efficiency with human decision-making and critical thinking may help businesses improve their cybersecurity posture and reduce their exposure to cyber-attacks.

The legal industry may use robotic process automation to boost productivity and save expenses. Robotic process automation can streamline labor-intensive tasks, including the review process and contract analysis (RPA). By automating these mundane tasks, law firms may save time and money while allowing their lawyers to focus on more strategic and client-facing activities.

In digital forensics, robotic process automation, often known as RPA, is being used to assist investigators in analyzing massive data sets in a much shorter amount of time. Experts in digital forensics collect and analyze digital evidence to help investigate computer and network crimes. Since the amount of data collected by individuals and organizations continues to grow, RPA might aid investigators in processing and analyzing it more quickly and efficiently. Data extraction from large datasets, social media research, and identifying patterns and anomalies are all areas where robotic process automation (RPA) might be helpful in forensics. Because of the time and money RPA saves investigators, they can put their attention where it is most needed: on the most complex tasks [36].

Human-machine collaboration is also an essential part of RPA. Although robotic process automation (RPA) has the potential to streamline many mundane tasks, it is important to remember that specific roles will always need human input due to the complexity of tasks like decision-making, analysis, and innovation. RPA can only be successful if it strikes a balance between automated processes and human oversight. Incorporating RPA into processes while retaining human involvement at decision points might help achieve this.

The healthcare industry is an excellent place to see successful human-machine collaboration. By employing robotic process automation (RPA), medical professionals may free up time formerly spent on mundane tasks like patient scheduling and billing. Human expertise is still essential in medical diagnosis and treatment. Here, RPA's data analysis and decision-support features might be used to aid medical staff. For instance, RPA might be used to analyze patient data and suggest therapy courses. The doctor may use the RPA system's findings to arrive at a definitive diagnosis and course of therapy [37].

U.S. companies were surveyed on customer experience (CX) in 2019 and asked how the integration of AI into CX will impact cybersecurity. Most responders (53%) say the reduced need for human interaction in processes and activities is the most critical impact (Fig. 3).

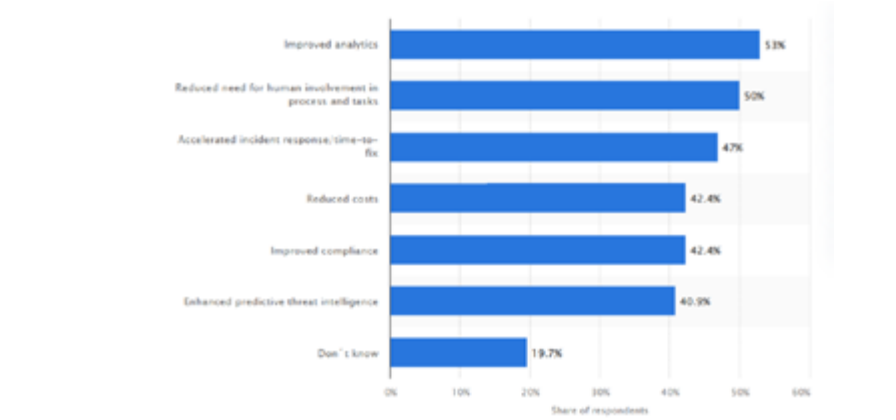


Figure 3. Cybersecurity is affected by AI and robots that improve the consumer experience (CX)

The fields of robotic process automation, digital forensics, and human-machine collaboration are rapidly developing fields that can potentially transform various industries. RPA may improve efficiency, reduce expenditures, and increase accuracy in everyday tasks. Digital forensics may help investigators handle vast volumes of data more rapidly and efficiently. Nevertheless, RPA can improve efficiency, cut expenses, and raise accuracy. Cooperation between humans and machines is essential to successfully implementing RPA and can improve decision-making and work performance. RPA is a technology not intended to replace human expertise but to supplement and augment human abilities. It will be essential to address these technologies' ethical, legal, and social repercussions as they continue to grow to ensure that they are employed responsibly and beneficially as they progress.

LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY

The application of artificial intelligence (AI) has the potential to dramatically increase the efficacy, accuracy, and fairness of the criminal justice system. The rise in the popularity of AI, on the other hand, has given rise to several significant ethical and legal challenges that need to be addressed to ensure that the technology is used ethically and responsibly. The use of AI within the framework of the legal system has some significant implications, including the following:

Responsibility for Crimes Committed Using AI: Concerns have been expressed about the potential for abuse of artificial intelligence as its usage in illicit acts grows more widespread, as well as wondering who should be held responsible for its misuse. Who should be liable when artificial intelligence is used for unethical or unlawful purposes? The inventors of the AI systems, the humans who utilize them, or both? There will be substantial repercussions for determining criminal culpability and who is to blame in cases of AI-enabled criminality.

Concerns have been raised about the potential for artificial intelligence technology to be used in a manner that would serve to exacerbate pre-existing biases and inequity within the criminal justice system. Particular groups might be subjected to discrimination due to the use of partial data or algorithms in decision-making processes inside AI systems. Fairness, due process, and the principle of equal treatment under the law are all at stake here.

Accountability and openness to the public: issues about ai's lack of human supervision in the criminal justice system have been expressed. it may be difficult for people to appreciate how artificial intelligence systems arrive at conclusions. it may also be difficult for them to dispute those judgments if they feel those decisions are unjust or biased. as a result, it is of the utmost importance to make ai systems accessible and accountable, as well as to provide humans with the tools they need to grasp and debate the conclusions reached by ai.

Protection of personal information and privacy: the application of artificial intelligence in the criminal justice system requires collecting, storing, and examining enormous amounts of data. this discovery raises several questions and concerns about the privacy and security of data, including who may see the data, how it will be used, and how it will be protected. throughout the process of developing and deploying ai systems, it is essential to consider people's constitutional rights to privacy and the protection of their data.

Respect for human rights and due process: the use of artificial intelligence (ai) within the framework of the justice system for crime raises substantial problems about the concepts of judicial oversight and the guarantee of human rights. it may be difficult for humans to argue the decisions made by an ai system, such as their bail, sentencing, or parole, or to grasp how those decisions were made. the ramifications of this finding concerning fundamental human rights, such as due process and the right to a fair trial, are significant.

Implications of artificial intelligence on the law and the criminal justice system:

- Risk Assessment Tools: Many jurisdictions are turning to risk assessment systems powered by artificial intelligence to determine whether or not a probationer will violate the conditions of their release. However, there are worries that such services may be biased and help to maintain racial and socioeconomic inequities in the criminal justice system. Concerned individuals have voiced these worries. According to a report by ProPublica, a commonly used risk assessment tool, for example, was shown to incorrectly identify black defendants as having a high risk of committing future crimes compared to white defendants by a factor of two. It was the case when comparing black defendants to white defendants.
- Facial Recognition: Several law enforcement agencies have begun using artificial intelligence software to recognize people's faces to apprehend offenders and bring them to justice. It is thought that these methods may be biased and erroneous, in particular when used to identify persons who belong to disadvantaged groups. Complaints have also been voiced over law enforcement's absence of control and regulation around using facial recognition technology.
- Sentencing Algorithms: Algorithms powered by artificial intelligence are utilized in certain nations to dole down sentences for criminal offenders. This practice is known as the "sentencing algorithm." Nevertheless, there are worries that such systems may be biased and therefore contribute to the continued existence of racial and socioeconomic disparities in sentencing. For instance, the Brennan Center for Justice found that a sentencing algorithm in Florida was biased against black defendants, predicting harsher sentences for

black criminals than white offenders. This discovery was made in Florida.

- Predictive Policing: Several law enforcement agencies are enhancing their predictive policing systems using AI to create profiles of high-risk neighborhoods and individuals. Concerns have been made, however, that these systems may be biased and contribute to the continuation of racial and economic disparities in the administration of justice. The adoption of artificial intelligence within the criminal justice system context presents significant concerns about the ideas of judicial supervision and the protection of human rights.
- Autonomous Weapons: Some countries are now working on developing autonomous weapons that are controlled by artificial intelligence and can locate and eliminate targets without the assistance of humans. Concerns about ethics and the law are raised when such weapons are used, particularly in light of issues of accountability and responsibility, as well as the likelihood of unintended consequences.

These are just a few examples of situations in which the usage of AI might potentially have significant repercussions in the courts. Politicians and legal experts should work to build laws and oversight procedures to ensure that AI is employed in a method that respects human rights and ethical standards.

The implications of artificial intelligence (AI) on the field of law enforcement as a whole are multifaceted and far-reaching. Politicians, legal experts, and other stakeholders need to work together to develop appropriate legal frameworks and standards to ensure that AI is used in a way that respects human rights and values. That will guarantee that AI is utilized in a manner that is ethical and responsible.

AI-ENABLED CRIME DETECTION AND PREVENTION

AI-enabled crime detection and prevention" means using artificial intelligence tools. Algorithms powered by AI might scan through data reams in search of anomalies and suspicious patterns. It might include monitoring security footage for suspicious activity, analyzing financial transactions for signs of fraud, or perusing social media data in search of signs of impending danger. Artificial intelligence (AI) may examine data from sensors and IoT devices to identify vulnerabilities [3].

One way that AI is being put to use in the fight against crime is via the practice of predictive policing. Predictive police algorithms use historical crime data to establish a time and place for potentially criminal behavior. The data might help authorities use their resources more wisely and stop crimes before they happen. However, if these algorithms are trained on just a subset of the available data, they might perpetuate bias and discrimination. These issues have been expressed [38].

Another technology that has found use in the law enforcement sector is facial recognition software. By comparing footage from surveillance cameras to databases of previously captured faces of known criminals, law enforcement may be able to apprehend those responsible for crimes and bring them to justice. Concerns have been raised about the accuracy and fairness of facial recognition systems and their potential for extensive surveillance [39].

Ethical concerns also arise from using AI for crime prevention and detection. One area that raises concerns is the possibility that AI systems would violate the rights of humans to free speech and privacy. It is of the

utmost importance to ensure that crime prevention and detection systems that depend on AI are open, responsible, and by the standards of society and ethics.

Figure 4. Data breaches and affected Americans, annually, in the United States, 2005–2022

In 2022, the total number of data breaches in the United States reached 1802. In the same year, about 422 million individuals were damaged due to data breaches, including data spills, leakage, and exposure. There is a link that can be drawn between each of these three separate instances. An unauthorized third party accessed sensitive information without proper authority in each of the three instances [40].

A further illustration of how artificial intelligence may be used to detect and prevent crime is using algorithms based on machine learning to identify cases of financial fraud. These algorithms can look through mounds of financial data in search of warning signs, such as unusual activity on an account or questionable transactions. This may help financial institutions prevent illicit behavior before it ever happens. Also, it may provide law enforcement with helpful information that can be used to track down and prosecute people guilty of committing financial crimes.

It is also possible to utilize artificial intelligence to search through social media for indications of potentially dangerous or unlawful behavior. For instance, police enforcement agencies may use AI to monitor social media posts to detect individuals planning to commit crimes or engage in terrorist activities. This could improve public safety by preventing similar actions from occurring before they occur [36].

Risk assessment is an essential component in the context of detecting and preventing crimes facilitated by AI. It is necessary to consider both the positive and negative aspects of using AI technology to detect and prevent crime. In order to ensure that AI systems are used responsibly and ethically, risk assessment can aid in identifying potential sources of bias, discrimination, and inaccurate information.

Using artificial intelligence to identify criminal activities and take preventative measures can significantly boost public safety and law enforcement's efficiency. Nonetheless, it is of the utmost importance to put in place the appropriate levels of monitoring and accountability to guarantee that these systems are developed and employed responsibly and ethically.

Figure 5. Challenges in prosecuting ai-enabled crimes

RESULTS

Although the fast progress of artificial intelligence (AI) has improved many facets of contemporary life, others worry that criminals may use its power. The justice system must adapt to this new frontier as more complex AI systems may be exploited to commit crimes. This article addresses the legal consequences of AI-enabled crimes and the issues that emerge when prosecuting such crimes.

The question of who is legally responsible for crimes made possible by AI is a significant problem. There is currently no established legal framework for dealing with the problem of AI-assisted crimes, making it hard to assign responsibility and identify perpetrators. The paper argues that a thorough legal framework is required, one that specifies how criminal culpability should be established and how algorithmic openness should be guaranteed.

Regarding crimes assisted by artificial intelligence, algorithmic transparency is a crucial concern. If AI systems are used to consider making choices that affect someone's life, there must be transparency regarding how these decisions are made. It is vital to ensure that the judgments made by AI systems are impartial and equitable.

Additionally, the study stresses the ethical aspects of AI-enabled crimes that need to be considered. Artificial intelligence systems may be misused to prey on or further marginalize already marginalized groups. The ethical ramifications of crimes facilitated by artificial intelligence should be addressed in the legal system, and vulnerable people should be protected.

To solve these issues, legal and technological professionals must work together to create a legal framework that accounts for the particular difficulties presented by AI-enabled crimes. This article analyzes the need for partnership between technical and legal professionals and summarizes the legal environment in AI-enabled crimes.

The article also addresses the difficulties in prosecuting AI-enabled offenses and the need for current legislation to address this group undergoing criminal activity. Legal and technological professionals may collaborate to guarantee that AI's advantages are achieved while the dangers of AI-enabled crime are minimal.

Algorithmic transparency guarantees that AI systems are responsible and that their decision-making processes can be evaluated. In the context of AI-enabled crimes, algorithmic transparency is essential for ensuring that AI systems make choices that are equitable, objective, and in line with legal and ethical norms. However, the complexity of AI algorithms might make it challenging to comprehend how judgments are made, raising questions about AI systems' responsibility.

One possible answer to this challenge is the development of explainable AI (XAI) systems. XAI systems aim to improve human comprehension of AI decision-making by providing visibility into the reasoning behind AI judgments. XAI systems are beneficial in the case of AI-enabled crimes since they enable legal professionals to establish if AI systems have been used to commit a crime and who is to blame.

The legal frameworks for AI-enabled crimes are still in their infancy. A clear legal framework must be clarified, making it difficult to identify who is accountable for AI-enabled crimes. The legal environment around crimes facilitated by artificial intelligence is complicated, posing difficulties for law enforcement and lawyers.

One possible answer is the establishment of international legal frameworks to handle the issues faced by AI-enabled crimes. Ethical issues, algorithmic transparency, and criminal culpability are some areas that such systems may cover. The creation of international legal frameworks, however, is a complex procedure that calls for the participation of several parties.

The proliferation of AI-enabled criminal activity raises serious moral questions. Artificial intelligence systems may be misused to prey on or further marginalize already marginalized groups. It raises problems regarding the role of AI in society and its influence on human rights.

To solve this issue, it is crucial to establish moral principles for creating and using AI systems. These rules should cover concerns such as prejudice, fairness, and privacy. They should also create safeguards to protect vulnerable groups and guarantee that the advantages of AI technology are achieved while limiting the dangers presented by AI-enabled crimes.

As AI systems grow more commonplace in society, it is crucial to comprehend the legal ramifications of crimes facilitated by AI. Criminal culpability, algorithmic openness, and ethical issues are essential to consider when crafting a legal framework. Experts in law and technology must work together to adapt the legal system to the novel dangers presented by crimes facilitated by artificial intelligence.

Although AI technology can potentially transform many facets of contemporary life, it also presents novel problems to the legal system. The legal ramifications of AI-enabled crimes are intricate, necessitating an all-encompassing strategy to meet the problems presented by AI.

Legal frameworks that address criminal culpability, algorithmic transparency, and ethical considerations are necessary to guarantee that the advantages of AI technology are achieved while limiting the dangers presented by AI-enabled crimes. Together, legal and technological professionals can create a legal framework that protects human rights while also addressing the unique issues provided by crimes facilitated by artificial intelligence.

DISCUSSION

The intersection of artificial intelligence and criminal justice involves new opportunities and complex challenges, necessitating a detailed discussion on the role of AI in presenting forensic evidence, determining criminal responsibility, the emergence of AI-assisted crimes, and the broader legal responsibilities associated with AI technologies. This discussion is based on recent scholarly contributions to understanding the complex consequences of integrating AI into the criminal justice system.

Altayari et al. argue that AI may significantly transform how forensic evidence is presented by streamlining the analysis and presenting procedures. Consequently, this might enhance precision and effectiveness in criminal inquiries [15]. AI implementation in this domain accelerates the processing of digital forensic data and introduces advanced capabilities for pattern recognition and anomaly detection, which are crucial in complex criminal inquiries.

However, integrating AI into the criminal justice system raises significant concerns about criminal responsibility, mainly when AI systems contribute to illegal actions. Vojtuš, Kordík, and Dražová investigate the challenges described earlier, focusing on the legal and ethical barriers related to determining responsibility in situations when AI systems are implicated in or entirely accountable for criminal acts [16]. Their study emphasizes the need for legal structures to adjust to tackle the complexities arising from AI, ensuring the implementation of accountability mechanisms for AI-assisted crimes.

The rise of illegal actions assisted by artificial intelligence, namely those using adversarial machine learning, adds more intricacy to the scenario. Sivaram, Narrain, Honnavalli, and Eswaran examine using adversarial strategies to bypass spam filters in their research. The statement emphasizes the sophisticated tactics criminals use to misuse artificial intelligence for unlawful purposes [17]. The advancement of cybercrime necessitates a corresponding improvement in AI-driven cybersecurity solutions, highlighting a continual rivalry between cybercriminals and cybersecurity professionals.

The issue of legal liability for AI is a topic of interest, as emphasized by Kingston , who examines the challenges in assigning blame for any harm caused by AI systems [18]. The issue lies in applying traditional legal concepts to scenarios where autonomous systems may provide judgments that lead to unexpected consequences, thereby blurring the lines of accountability and necessitating a reevaluation of legal conceptions about culpability.

The discussion also includes the impact of AI on privacy and data protection, specifically examining the General Data Protection Regulation (GDPR) as a critical reference point for evaluating the development of legal standards to protect individuals' rights in the era of AI [23]. The GDPR prioritizes the rights of persons whose data is being processed and the accountability of those handling the data, setting a benchmark for protecting privacy. This standard profoundly influences global standards and protocols for managing data generated by artificial intelligence.

When contemplating the future of AI in criminal justice, it is evident that the benefits of using AI to enhance forensic analysis, predict crimes, and aid law enforcement must be carefully evaluated in light of the ethical, legal, and societal risks connected with AI's capabilities. Collaboration among legal experts, technologists, and politicians is essential to tackle the evolving nature of AI-enabled crimes properly. This collaboration should be proactive and adaptable. Collaboration is essential to guarantee that the incorporation of AI into the criminal justice system not only enhances the administration of justice but also maintains ethical norms and safeguards individual rights.

Furthermore, the analysis of AI and criminal justice is enriched by investigating the utilization of AI in cybersecurity [19], the philosophical and legal dimensions of AI in criminal law [20], and the broader societal implications of AI's advancement [21], [22]. These comments emphasize the significance of using a diverse range of fields to tackle the issues and prospects of artificial intelligence in criminal justice. They stress the need for continuous dialogues, inventive strategies, and moral consciousness as we progress toward a future shaped by artificial intelligence.

CONCLUSIONS

The intersection of artificial intelligence and criminal responsibility raises challenging challenges for lawmakers, law enforcement, and the legal system. Digital crimes and autonomous systems raise questions about who ought to be held accountable for acts committed by AI systems and how to ensure these systems are utilized morally and ethically. These questions center on how to ensure that these systems are used correctly. To ensure that artificial intelligence (AI) devices are created and deployed to respect the safety and privacy of individuals and organizations, constant attention must be paid to algorithmic, cyber, and data privacy concerns. It is vital for there to be algorithmic transparency and accountability if artificial intelligence systems are to be fair, transparent, and accountable. Fears regarding the potential for AI systems to replace human workers are balanced out by opportunities for the automation of robotic operations, the advancement of computer forensics, and the collaboration of humans and machines to increase the abilities of cybersecurity professionals. Ethical considerations and risk assessments are essential to guarantee that AI systems will be developed and used in a manner that is both ethical and responsible. Research, collaboration, and creative thinking are three essential ingredients required to develop effective strategies for preventing and prosecuting crimes made feasible by artificial intelligence. In conclusion, to effectively address the challenges of

detecting and preventing AI-enabled crimes and the difficulties in prosecuting AI-enabled crimes, a multi-disciplinary approach incorporates technical expertise, regulatory and legal structures, and cooperation across stakeholders is necessary. This is the only way to address these challenges effectively.

The challenges posed by artificial intelligence and criminal responsibility intersection highlight the need for ongoing article, collaborative efforts, and innovation in this field. Legislators, law enforcement, and the legal system must continue to develop to ensure that AI technologies are used ethically and responsibly. This includes providing training and help for those working in this industry and creating appropriate regulatory norms and frameworks to ensure the openness and accountability of AI systems.

Also, there is a pressing need to educate the general people more thoroughly on both AI technology's positive and negative aspects. This requires educating individuals and businesses on maintaining their private information and the danger that AI algorithms may be abused for malicious ends.

When it comes down to it, the intersection of AI and criminal culpability is fraught with both benefits and drawbacks. The development of effective ways of avoiding and convicting crimes committed with the aid of artificial intelligence and ensuring that such techniques are developed and utilized responsibly and ethically could result from collaborative efforts between various fields of study and interested parties. This could lead to the creation of effective methods.

REFERENCES

A. Lohmann: 'Strafrecht im Zeitalter von Künstlicher Intelligenz', in Editor (Ed.)^(Eds.): 'Book Strafrecht im Zeitalter von Künstlicher Intelligenz' (2021, edn.), pp.

A. Mukherjee, and A. Ghosh: 'Heterogeneous Decomposition of Predictive Modeling Approach on Crime Dataset Using Machine Learning', in Editor (Ed.)^(Eds.): 'Book Heterogeneous Decomposition of Predictive Modeling Approach on Crime Dataset Using Machine Learning' (2019, edn.), pp.

A. P. E. Sickler: "The (Un)Fair Credit Reporting Act", LSN: Consumer Credit & Payment Issues (Topic), 2016

B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi: "The ethics of algorithms: Mapping the debate", Big Data & Society, 3, 2016

C. Scoccia, M. Ciccarelli, G. Palmieri, and M. Callegari: "Design of a Human-Robot Collaborative System: Methodology and Case Study", Volume 7: 17th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA), 2021

C.-K. Wang: "Security and privacy of personal health record, electronic medical record and health information", Problems and Perspectives in Management, 13, 2017

D. Fernandez, and A. Aman: 'Impacts of Robotic Process Automation on Global Accounting Services', in Editor (Ed.)^(Eds.): 'Book Impacts of Robotic Process Automation on Global Accounting Services' (2018, edn.), pp.

E. A. Holm: "In defense of the black box", Science, 364, 2019, pp. 26 - 27

F. Vojtuš, M. Kordík, and P. Dražová: "Artificial Intelligence and the criminal responsibility - challenges, obstacles and possible solutions", 2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2022, pp. 660-72

H. Arshad, S. Abdullah, M. Alawida, A. Alabdulatif, O. I. Abiodun, and O. Riaz: "A Multi-Layer Semantic Approach for Digital Forensics Automation for Online Social Networ-

ks", Sensors (Basel, Switzerland), 22, 2022

H. Guan, L. Dong, and A. Zhao: "Ethical Risk Factors and Mechanisms in Artificial Intelligence Decision Making", Behavioral Sciences, 12, 2022

ITRC: "Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises", Electronic resource, 2023

J. K. C. Kingston: 'Artificial Intelligence and Legal Liability', in Editor (Ed.)^(Eds.): 'Book Artificial Intelligence and Legal Liability' (2016, edn.), pp.

J. Klemenc, and H. Trittenbach: "Selecting Models based on the Risk of Damage Caused by Adversarial Attacks", ArXiv, abs/2301.12151, 2023

J. Sivaram, J. M Narrain, P. B. Honnavalli, and S. Eswaran: "Adversarial Machine Learning: The Rise in AI-Enabled Crime and its Role in Spam Filter Evasion", SSRN Electronic Journal, 2022

K. J. Hayward, and M. M. Maas: "Artificial intelligence and crime: A primer for criminologists", Crime, Media, Culture: An International Journal, 17, 2020, pp. 209 - 33

K. Zhou, and H. Nabus: "The Ethical Implications of DALL-E: Opportunities and Challenges", Mesopotamian Journal of Computer Science, 2023

L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, and E. Vayena: "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations", Minds and Machines, 28, 2018, pp. 689 - 707

L. McGregor, D. Murray, and V. Ng: "INTERNATIONAL HUMAN RIGHTS LAW AS A FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY", International and Comparative Law Quarterly, 68, 2019, pp. 309 - 43

M. A. Barrett, J. Marron, V. Pillitteri, J. M. Boyens, S. R. Quinn, G. A. Witte, and L. Feldman: 'Approaches for federal agencies to use the cybersecurity framework', in Editor (Ed.)^(Eds.): 'Book Approaches for federal agencies to use the cybersecurity framework' (2020, edn.), pp.

M. R. R. Ghodekar, and P. S. Roy: "Phishing: A Way of Attacking the Privacy", International Journal of Advanced Research in Science, Communication and Technology, 2022

M. Rimol: "Gartner Predicts Half of Cloud Data Centers Will Deploy Robots with AI Capabilities by 2025", Gartner Press Release, 2021 D. Fernandez, and A. Aman: "The Challenges of Implementing Robotic Process Automation in Global Business Services", International Journal of Business and Society, 2021

MarketsandMarkets: "Digital Forensics Market by Component (Software, Hardware, and Services), Type (Network Forensics, Mobile Device Forensics, Cloud Forensics), Deployment Mode (Cloud and On-Premise), Vertical and Region - Global Forecast to 2028", Electronic resource, 2023

N. Naik, B. M. Z. Hameed, D. K. Shetty, D. Swain, M. J. Shah, R. Paul, K. Aggarwal, S. Ibrahim, V. Patil, K. Smriti, S. Shetty, B. P. Rai, P. Chłosta, and B. K. Somani: "Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?", Frontiers in Surgery, 9, 2022

N. V. Spesivov: "From Fantastic Theories to Objective Reality: Is there Future for Artificial Intelligence and Predictive Technologies in Administration of Criminal Justice?", Lex Russica, 2023

O. S. Kerr: "The Next Generation Communications Privacy Act", University of Pennsylvania Law Review, 162, 2013, pp. 373

P. Bukaty: 'The California Consumer Privacy Act (CCPA)', in Edi-

tor (Ed.)^(Eds.): 'Book The California Consumer Privacy Act (CCPA)' (2019, edn.), pp.

P. Hofmann, C. Samp, and N. Urbach: "Robotic process automation", Electronic Markets, 30, 2019, pp. 99 - 106

S. J. Nightingale, and H. Farid: "AI-synthesized faces are indistinguishable from real faces and more trustworthy", Proceedings of the National Academy of Sciences of the United States of America, 119, 2022

S. Kane: "Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act", University of Chicago Law Review, 87, 2020, pp. 5

S. Khan, M. H. Javed, E. Ahmed, S. A. A. Shah, and S. U. Ali: "Facial Recognition using Convolutional Neural Networks and Implementation on Smart Glasses", 2019 International Conference on Information Science and Communication Technology (ICISCT), 2019, pp. 1-6

S. Likens: "PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution", PwC 2023

S. Lo Piano: "Ethical principles in machine learning and artificial intelligence: cases from the field and possible ways forward", Humanities and Social Sciences Communications, 7, 2020

S. Mishra, M. A. Alowaidi, and S. K. Sharma: "Impact of security standards and policies on the credibility of e-government", Journal of Ambient Intelligence and Humanized Computing, 2021, pp. 1-12

S. Zeadally, E. Adi, Z. A. Baig, and I. A. Khan: "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity", IEEE Access, 8, 2020, pp. 23817-37

T. C. King, N. Aggarwal, M. Taddeo, and L. Floridi: "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", Science and Engineering Ethics, 26, 2019, pp. 89 - 120

V. Chico: "The impact of the General Data Protection Regulation on health research", British Medical Bulletin, 128, 2018, pp. 109–18

W. Altayari, M. Kamalrudin, and M. M. Jaber: "role of artificial intelligence in forensic evidence presentation", International journal of health sciences, 2022

W. E. Forum: "Davos 2024: 5 business leaders on adopting AI and managing associated risks", Electronic resource, 2024