Macrothink Institute™

International Journal of Social Science Research
ISSN 2327-5510
2024, Vol. 12, No. 2

Legal Implications of Emerging Technologies in Criminal Investigations: Current Challenges and Catalysts for Change

Mohammed R. M. Elshobake (Corresponding Author)

Assistant Professor, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, 53100 Jalan Gombak, Kuala Lumpur Malaysia

E-mail: mshobake@iium.edu.my

Alaa Sakka

Ph.D. Candidate, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, 53100 Jalan Gombak, Kuala Lumpur, Malaysia

E-mail: alaa-sakka@outlook.com

Received: June 11, 2024 Accepted: August 26, 2024 Published: September 24, 2024

doi:10.5296/ijssr.v12i2.21965 URL: https://doi.org/10.5296/ijssr.v12i2.21965

Abstract

This paper focuses on the transformative impact of developing technology on criminal investigations, as well as the legal repercussions. The research reveals the multifaceted obstacles and opportunities that these innovations provide within the criminal justice framework, such as artificial intelligence. The research examines the developing balance between police enforcement activities and individual rights by examining some current cases and legal precedents, addressing problems of privacy, due process, and evidence standards. This research will employ the descriptive-analytical method and case study approach to conduct a comprehensive examination of the Legal Implications of Emerging Technologies in Criminal Investigations. The article suggests adaptive strategies to provide a nuanced approach that supports rapid technology innovation by identifying holes in existing legal systems. The research provides critical insights to policymakers, legal practitioners, and scholars navigating the dynamic convergence of law and technology, providing a complete grasp of the change agents in the ever-changing landscape of criminal investigations.

Keywords: Emerging Technologies, Artificial Intelligence, Criminal Investigations, Legal Implications

1. Introduction

Digital technology has completely taken over the world today, and people are dependent on it to always be connected. Following the world's recent exposure to the COVID epidemic, a new dimension in the everyday usage of digital technology and digitalization has evolved in all spheres of life, from the workplace to the home. One of the main causes of the societal shift has been technology. On the one hand, technology makes it easier for consumers to use, but on the other hand, it also gives antisocial elements and criminals a very comfortable platform on which to operate and commit frauds such as forging ATM cards or credit/debit cards (Gupta & Srivastava, 2023). Policing and security management are now heavily reliant on digital technologies, with drones, and body worn cameras and it has the potential to revolutionise the game (Laufs & Borrion, 2022).

Due to the widespread use of digital forms, computer and cell phone technologies have expanded data storage capacity and facilitated low-latency data sharing and communications both within and across organisations, agencies, states, and nations. The society is being significantly impacted by the constant advancements in technology. For example, when a new technology is introduced into society, people take some time to get used to it and it is not fully spread. Meanwhile, another novel technology is introduced, which primarily causes chaos when it comes to learning technology for the average person. However, criminal and antisocial elements are quick to upgrade themselves with the newest technology and misuse it for their own gain, which leaves people vulnerable to cybercrime and cyberfraud.

Evidence from the past few years indicates that identity crimes are growing dramatically and causing significant economic loss. In fact, cyber-deception and theft, or fraud, is one of the most often reported types of cybercrime (The National Fraud Center, 2010). As a culture, we now rely more and more on computers and the internet to handle almost every aspect of our financial lives. This has made it easier for us to keep tabs on our spending and purchases almost instantly.

Without the aid of contemporary information technologies, it is quite difficult to envision combating crime in the 21st century. This facilitates the ability to decrease the number of law enforcement personnel and the load on the legal system, as well as expedite the process of combating offences (Ivliev et al., 2023). The fight against organised crime is being extended to all areas of public life, including the information component, which will unavoidably rise in percentage as compared to other crimes. Using specialised software and technical gadgets is becoming more and more important as the number of cybercrimes and offences using digital information keeps rising. Furthermore, in order to combat crimes involving information, it is important to set up a variety of unique tools and techniques.

Existing and developing technologies have made a significant contribution to crime prevention, criminal identification, and criminal justice. When it comes to reducing and managing crime, the Internet, social media, digital cameras, licence plate readers, mobile and smart phones, and licence plate readers have all been effective. There is no longer any chance for criminals to commit heinous crimes in anonymity, there is a greater chance than ever that they will be apprehended (Breslin & Lowery, 2021).

In a time of lightning-fast technical development, criminal investigation practice is changing dramatically. This study explores the significant changes that modern technology have brought about as well as the legal implications for criminal investigations. This paper methodically reveals the various consequences that these advances have for the legal framework, ranging from artificial intelligence and machine learning algorithms.

Investigating privacy, due process, and evidentiary standards, the study critically looks at the potential and problems that come with integrating developing technologies into criminal investigations. The research evaluates the changing dynamics between law enforcement tactics and people's fundamental rights by looking at current case studies and court rulings.

The article also points out weaknesses in the current legal frameworks and suggests workable solutions to these problems. It highlights how important it is to have a legal framework that is both flexible and nuanced in order to keep up with the quick advancement of technology while maintaining the protection of civil liberties and the efficacy of law enforcement.

This research adds to a thorough grasp of the legal environment surrounding developing technologies in criminal investigations through an interdisciplinary analysis. Through shedding light on the forces driving change at this fast-moving nexus of law and technology, it provides important insights for academics, legal professionals, and policymakers debating how justice is changing in the digital era.

This research will employ the descriptive-analytical method and case study approach to conduct a comprehensive examination of the Legal Implications of Emerging Technologies in Criminal Investigations. The descriptive-analytical method involves systematically describing and analyzing the impact of emerging technologies, such as artificial intelligence on criminal investigations, and evaluating how current legal frameworks adapt to these advancements. This method provides a thorough understanding of the technological developments and their legal implications. Meanwhile, the case study approach focuses on specific instances and practical examples where these technologies have been applied in real-world criminal investigations. By analyzing these cases, the research can highlight practical challenges and gaps in the legal system, offering insights into the real-world impact of technological innovations and suggesting improvements for legal policies and practices.

Notably, the research will focus on the impact of technology in criminal investigation, especially artificial intelligence. It seeks to demonstrate the benefits of artificial intelligence, its potential drawbacks, and the ethical considerations for its use in criminal investigation. For the purposes of this research, artificial intelligence is defined as: “a field of science and technology that aims to make machines capable of human brainpower and intelligence, typically thinking and reasoning to solve problems, knowing communication by understanding language and speed, learning, and self-adaption” (Thao, 2023). AI can work on hardware devices, e.g., advanced robots, autonomous cars, drones. It also can work on software and the virtual world, e.g., voice assistants, image analysis software, search engines, speech, and face recognition systems (European Commission, 2018)

2. Innovative Technology and The Realm of Criminal Investigation: The Necessity for Adaptability

Crime investigation is a challenging and strenuous task, with potentially significant consequences for mistakes. In extensive investigations, detectives must navigate through a vast amount of disorganized evidence to make sense of it all (Bex et al., 2007). Since evidence is obtained by the judicial authorities to substantiate accusations and prove criminal activity and guilt, the investigative phase of the criminal process is crucial. It is a time-consuming, labour-intensive procedure that demands a great deal of care, persistence, and attention to detail. It also requires a large financial investment. However, because errors are difficult and expensive to remove and repair, human error occurs during this process, depending on the volume of work and data that needs to be analyzed (Stanila, 2020). Modern technology has made the investigation process easier and more complex, all at the same time. Because electronic data is so abundant, its extraction, analysis, and interpretation require certain techniques and knowledge. While making sure that the evidence they gather is admissible and lawful, investigators must also keep up with the rapid advancement of technology.

In order to combat the crime epidemic, law enforcement officials must identify strategies, resources, and instruments to make their jobs easier and provide the desired outcomes. Since these new methods could satisfy the requirements of speed, objectivity, and efficiency, they might be based on artificial intelligence (AI) and telematic tools (Stanila, 2020). The application of artificial intelligence (AI) in law enforcement provides a comprehensive strategy for tackling the complexity of contemporary crime. By analyzing large datasets at previously unheard-of speeds, machine learning algorithms help law enforcement organisations spot patterns, trends, and possible threats more quickly. In addition to accelerating investigations, this data-driven strategy improves objectivity by reducing human biases that could skew traditional investigative methods. Software could provide these capabilities by assisting criminal investigators in employing common knowledge to support their reasoning when presenting case-specific arguments regarding the evidence's relevance to different hypotheses. Software for organising and displaying evidence is already employed in crime investigation procedures and other related fact-finding procedures (Bex et al., 2007).

Many approaches to using AI as a resource for public safety are being investigated. Facial recognition is one AI application that is widely used in both the public and private sectors (Rigano, 2018). For example, intelligence analysts frequently use facial picture data to determine the identify and whereabouts of an individual. It takes a lot of time and effort to accurately and quickly review the vast amount of potentially relevant photos and videos, and there is a chance that human error will occur from weariness and other circumstances.

Since certain crimes, the number of which is rising, are closely associated with the internet and online resources used to perpetrate them, investigators should employ comparable resources to track down and apprehend the offenders. One such instance is child pornography, which has the potential to spread dangerously throughout the world (Stand for Girls, n.d.) In light of the large quantity of offenders, law enforcement officials are unable to depend

exclusively on the victims' reporting and the existing techniques of detection. Even if they were to resort to covert activities, it would be unrealistic to anticipate meaningful progress at this point in time given the scarcity of both financial and personnel resources and the critical need for prompt state response. State agents must be imaginative, inventive, and resourceful in the current turbulent times when combating criminal activity.

3. Use Of Emerging Technologies Ethically, Accountability and Responsibility

New tools and capacities are being made available to law enforcement through the growing usage of emerging technology in criminal investigations. However, there is a huge responsibility that goes along with authority. Incorporating these technologies into the criminal justice system requires careful consideration of ethics, accountability, and responsibility.

Law enforcement organisations have embraced a number of new technologies in the past ten years, including as drones, automated number plate readers, body cams, surveillance cameras, and now facial recognition technology (FRT). Because of the advantages that are clear and logical in this area, law enforcement organisations have been in the forefront of FRT implementation. But each of these technologies modifies the interactions between civilians and law enforcement officials, necessitating the negotiation of new parameters and updated accountability standards (Almeida et al., 2022). It is critical to strike a balance between the preservation of civil freedoms and the requirement for efficient law enforcement. Agencies are responsible for making sure that data is gathered and used in a way that is appropriate, lawful, and overseen. In this regard, COVID-19 has stretched privacy limits even beyond, prompting governments to enact new laws requiring them to monitor their citizens' whereabouts and interactions in an effort to stop the virus from spreading at that time (Sakka, 2023).

Integrating developing technologies into criminal investigations requires accountability, which calls for law enforcement agencies to be transparent about the technologies they use and how they use them. The communities that law enforcement serves benefit from this transparency. Setting up explicit policies and procedures for implementing these technologies is essential to complying with legal and ethical requirements. Regular audits and reviews should also be conducted to provide an extra degree of responsibility. Furthermore, considering the difficulties with storage, security, and access brought about by the massive volumes of data gathered via many technologies, proper data handling is essential. Implementing techniques like data anonymization and encryption is necessary to safeguard individuals' right to privacy and stop potential abuses while also preventing unauthorised access to and misuse of sensitive data.

Technology hides the identity of the violation, making it considerably more difficult to hold obligation bearers accountable. For instance, tasks completed by automation can seem inevitable, even when they are the result of choices that reflect and represent value judgements.Technology also normalises behaviour that could otherwise be seen as an affirmative damage by making breaches themselves more undetectable (Land & Aronson, 2020).

4. Evolving Technologies in Criminal Investigations

Significant technical developments in recent years have changed how the criminal justice system approaches crime prevention and detection. The adoption of data-driven strategies and predictive analytics by law enforcement organisations is one significant advancement. These methods help with proactive policing measures to avoid future crimes by predicting high-crime regions and identifying persons who are more likely to be involved in criminal activities (JWU, 2023). They do this by utilising massive databases. In addition to improving resource allocation efficiency, this data-centric strategy helps to make law enforcement more strategic and focused.

Voice command technology also improves the skills of officers in the field by allowing them to operate tools and functions without using their hands while on patrol. Even when not in use, cell phones can be used to track locations, intercept conversations, and access historical records, all of which are vital tools for investigators, given the ubiquity of tracking requests, police departments clearly think tracking is a useful law enforcement technique (Slobogin & Brayne, 2023). In order to provide law enforcement with even more cutting-edge tools to support criminal investigations, monitoring systems such as GPS, drones, licence plate scanning, gunshot detection, and surveillance cameras ensure a more efficient and technologically driven approach to preserving public safety (Jacobson, 2022).

The use of facial recognition and surveillance technologies is another important technical advancement. Video surveillance systems are being used by police departments more and more to keep an eye on public areas. Facial recognition technology assists in the identification of possible suspects by generating biometric profiles. This innovation saves law enforcement authorities a great deal of time and money by streamlining the processing of enormous volumes of video material in addition to speeding up the identification procedure. In addition, forensic science and DNA analysis have advanced tremendously, with methods such as polymerase chain reaction and DNA profiling being important in the resolution of cold cases. Since the discovery of the double-helix structure in the 1950s, forensic technology has advanced, giving law enforcement strong tools to unearth vital evidence and conclude protracted investigations (JWU, 2023).

5. Challenges for Human Rights

Human rights may be violated when technology is used to identify, investigate, and prosecute crimes as well as to enforce criminal penalties. For instance, the use of information technologies can result in egregious privacy violations. The possibility of violating someone's right to privacy, freedom of speech, a fair trial, and the assumption of innocence are only a few of the human rights issues that arise from the capacity to monitor computer usage.

Several regional and international measures are enacted to guarantee the protection of human rights when investigating cybercrime. In order to protect human rights norms and privileges in the context of cybercrime investigations, the Council of Europe's Convention on Cybercrime (2001) includes a number of provisions. These include proportionality requirements, judicial or other independent supervision requirements, and provisions that

require respect for and consideration of third parties' rights. However, some privacy advocates have criticised these as being insufficient given the severity of the laws permitting search, seizure, and monitoring.

Two important pieces of legislation within the Council of Europe are the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Ethical Charter on the use of artificial intelligence in judicial systems, both of which have been adopted by the European Commission for the Efficiency of Justice (CEPEJ) (Council of Europe, 2018). Regarding the protection of private life, liberty, and security as well as the provision of strong legal recourse in the event of invasions of privacy and to shield people from illegal surveillance, including that which is carried out via the use of modern technology, the case law of the European Court of Human Rights is especially vital.

5.1 Discrimination

Artificial intelligence is being used by police to help them find potential crime scenes and assess the risk that an individual in custody poses to society. This is done while maintaining the objectivity and impartiality of the decisions made by the police and basing them on factual information (Miller, 2018). On the other hand, detractors of artificial intelligence and prediction models have shown that these impartial systems either encode specific ways of thinking into code or reproduce biases present in the data they are trained on. A system will unavoidably become biassed if it is fed human biases, even unconscious ones, which will serve to reinforce prejudice and discrimination (Boskovic, 2020).

Criminal justice systems in the United States have long employed instruments to evaluate criminal behaviour. However, recent research from the criminal justice system regarding parole, policing, bail, and sentencing has shown that racial and ethnic profiling results in harsher criminal punishments for particular groups. Evaluation of COMPAS, a criminal recidivism prediction model that was, until recently, employed by certain US courts to assist judges in making parole request decisions, revealed a significant racial bias in the model (Larson et al., 2016). In comparison to white people under the identical circumstances, the model allocated a double risk to backs who will not really commit a crime (Pedreschi & Miliou, 2020) The overrepresentation of Black inmates in American jails has an impact on the model, which most likely acquired the bias inherent in the past sentencing (Boskovic, 2020).

The European Union Fundamental Right Agency cautions that additional protections in this area need to be developed, as decision-making based on predictive models and related techniques is still relatively new. In an effort to increase the effectiveness of their criminal justice systems, European nations are also exploring predictive models as a potential answer to their limited budgetary resources and growing caseload. Nonetheless, European policy makers have exercised caution and implemented a number of measures to reduce potential hazards. Additionally, the European Parliament issued a warning, stressing that extreme caution is necessary to stop illegal discrimination and the targeting of specific people or groups based on their race, colour, ethnicity, social background, or any other attribute (Monteleone, 2017).

Big data is used by law enforcement for a variety of tasks, including risk management, crime analysis, and patrol as well as investigation and dragnet and guided surveillance. The main difference between dragnet and directed surveillance is that the latter is universal and collects data on everyone, while the former is concentrated on certain people and locations that are suspicious (Brayne, 2018).

5.2 Right to Privacy

While the use of new technologies in police investigation procedures guarantees increased efficiency in the investigation and prosecution of criminal cases, their high level of intrusiveness compromises individuals' right to privacy. Certain modern technologies allow policy to get over physical obstacles. Examples of this include quiet video surveillance of the interior of homes and communication eavesdropping. In order to effectively address emerging offences pertaining to technology use, European authorities have implemented regulations on the use of undercover agents in online communications, electronic communication interception, remote computer system searches, and the preservation of stored computer data, among other topics (Ortiz-Pradillo, 2017). These particular rules should only be used in accordance with the safety measures put in place for the application of special investigation techniques, and the regulations controlling their collection should be followed.

The European Court of Human Rights has determined in multiple cases that the use of special investigation techniques is in violation of the European Convention on Human Rights' article 8, which deals with the right to privacy. The European Court of Human Rights ruled in the Klass v. Germany judgement that any surveillance system must include sufficient and reliable safeguards against misuse (European Court of Human Rights, 1978).

The right to privacy may be violated by the use of modern technologies for monitoring. The European Court of Human Rights ruled in the Shimovolos v Russia case that there had been a breach of article 8 of the Convention. The case pertained to the registration of a human rights activist in the monitoring database, which gathered data on the movements of activists (European Court of Human Rights, 2011). The ministerial decree that oversaw the database's establishment, upkeep, and operational processes was never made public, and it contained no mention of the minimal security measures meant to prevent database misuse. The Court's stance on secret monitoring for national security reasons was similar in the Szabo and Vissy v Hungary decision because there were insufficient safeguards to prevent abuse (European Court of Human Rights, 2016).

Emerging technologies in criminal investigations, such as facial recognition, biometric tools, and big data analytics, bring significant advancements but also raise serious data privacy and security concerns. These technologies enable extensive data collection and real-time surveillance, potentially infringing on personal privacy and leading to risks related to data breaches. The increased volume and sensitivity of data collected heighten concerns over its storage, security, and potential misuse, challenging the adequacy of current data protection measures (Rowena, 2020).

The rapid evolution of technology often outpaces existing data protection laws, creating gaps

in how privacy rights are safeguarded. For instance, regulations like the GDPR may not fully address the complexities of new technologies, leading to conflicts between technological capabilities and privacy protections. To address these issues, there is a need for updated legal frameworks that can adapt to technological advancements while ensuring robust privacy safeguards. Ongoing collaboration between technology developers, legal experts, and privacy advocates is essential to strike a balance between enhancing investigative capabilities and protecting individual privacy rights (Lindsey, 2018; Leite et al., 2023).

6. Using Artificial Intelligence (AI) in Criminal Investigation

In criminal investigations, time is of the essence. The sooner law enforcement can gather evidence and information, the more effectively they can solve crimes, prevent escapes, and protect potential victims. Investigators and murder experts consistently emphasize that if evidence isn't found within the first 48 hours, the chances of solving the case significantly decrease (Lunter, 2023). Integrating artificial intelligence (AI) into criminal investigations can expedite the process, generate high-quality evidence, and enhance law enforcement efforts. However, like any technological advancement, it raises significant ethical questions and potential for misuse (Lunter, 2023).

In this discussion, we will explore the potential benefits and drawbacks of using AI in criminal investigations, considering whether this development could be a double-edged sword. We will also present case studies and practical examples of AI applications in the field of criminal investigation.

6.1 Benefits of Using Artificial Intelligence (AI) in Criminal Investigation

Artificial intelligence could become a permanent fixture in the criminal justice system, offering valuable investigative support and helping law enforcement professionals enhance public safety (Rigano, 2018).

AI applications in criminal investigations offer several promising advancements:

a) AI-Driven Fingerprint Analysis: AI can rapidly identify latent fingerprints, significantly reducing the time compared to manual forensic methods. However, the accuracy of these identifications still needs to be verified by trained forensic experts, ensuring that AI serves as a supportive tool rather than a decision-maker (Lunter, 2023).

b) Facial Recognition Technology: This technology can aid in identifying individuals from photos or security footage, speeding up the process of apprehension or interrogation. Additionally, advancements such as forensic cameras for non-destructive fingerprint collection can make on-site investigations more efficient (National Science and Technology Council, 2016; IARPA, n.d.)

c) Video Analysis: AI can analyze video footage to help law enforcement identify potential suspects and gather crucial evidence for court. In Malaysia, researchers are developing AI software for CCTV cameras to reduce street crime. This software can detect whether individuals are carrying weapons, recognize aggressive behaviors, and

alert authorities if suspicious activities are detected (Monash University, 2021).

d) AI Contact Analysis and Graph Databases: These tools help uncover hidden connections between suspects, crime scenes, and victims, providing valuable insights for investigations (Lunter, 2023). In addition, AI can integrate and manage case information from various sources, helping investigators keep track of leads, evidence, and suspect information in a more organized manner. This streamlined approach improves workflow efficiency and ensures that critical information is readily accessible (Rigano, 2018).

e) DNA Analysia: AI algorithms have been investigated across different areas of forensic science, including DNA analysis (Brynjolfsson & McAfee, 2017). AI has the potential to significantly enhance forensic DNA analysis by tackling complex challenges in evidence processing. Traditional DNA testing has become increasingly sensitive, allowing the detection of trace amounts of DNA from various sources, including old or degraded samples. This sensitivity can lead to detecting DNA from multiple contributors, which complicates the interpretation of results. AI can address this issue by analyzing large, intricate datasets generated during DNA testing, identifying patterns that might be missed by human analysts. Researchers, such as those from Syracuse University, are exploring machine learning methods to improve the deconvolution of DNA mixtures, combining AI algorithms with traditional approaches to accurately separate and identify individual DNA profiles. This hybrid method aims to minimize the limitations of each approach and enhance the reliability of forensic analyses (National Institute of Justice, 2014).

f) Gunshot detection: It represents another promising application of AI algorithms. In one initiative funded by NIJ, Cadre Research Labs, LLC is developing algorithms to analyze gunshot audio recordings from smartphones and other smart devices. Their approach is based on the understanding that the content and quality of gunshot recordings are affected by factors such as the type of firearm and ammunition, the scene's geometry, and the recording device. Using a precise mathematical model, Cadre scientists aim to create algorithms capable of detecting gunshots, distinguishing between muzzle blasts and shock waves, determining shot-to-shot intervals, identifying the number of firearms used, linking specific shots to particular firearms, and estimating the class and caliber of the firearms. These advancements could significantly aid law enforcement in their investigations (Rigano, 2018).

g) Criminal and Victim Data Analysis :AI is revolutionizing the analysis of criminal justice data by predicting recidivism and improving warrant management. Researchers at the Research Triangle Institute, with support from NIJ, are developing a triage tool for North Carolina's Statewide Warrant Repository. By analyzing over 340,000 warrant records, their algorithms can forecast when a warrant might remain unserved, assess the risk of re-offending, and optimize resource allocation by targeting high-risk areas (Taniguchi *et al.*, 2019).

In addition, AI is advancing the detection of elder abuse and predicting potential violent crime

victims. Researchers at the University of Texas Health Science Center are using AI to differentiate between financial exploitation and other types of elder abuse, aiming to create tools for timely intervention (Burnett et al., 2017). Meanwhile, the Chicago Police Department, in collaboration with the Illinois Institute of Technology, is applying AI to identify high-risk individuals through social network analysis, enhancing their Violence Reduction Strategy (Chicago Police Department, 2011).

Despite these advancements, it is essential to remember that AI technology does not replace human expertise. Errors, such as false accusations, highlight that the fault often lies in the investigative process, not the technology itself (Lunter, 2023). AI serves as a valuable assistant, but final decisions must be made by human specialists.

6.2 Potential Drawbacks of Using Artificial Intelligence in Criminal Investigation

Despite the many benefits of using AI in forensic investigation, there are several potential drawbacks and risks. AI systems are not infallible and can produce false positives, where innocent individuals are incorrectly identified as suspects, or false negatives, where actual suspects are overlooked. Such errors can undermine investigations, lead to wrongful accusations, and compromise the integrity of the justice process. Instances of false arrests have occurred due to errors made by AI systems. For example, Randal Quran Reid (a 29-year-old Atlanta man) was wrongfully arrested and held for about a week in jail due to the misuse of facial recognition technology (Marcus, 2023).

Nathan Freed Wessler, deputy director of the American Civil Liberties Union's Speech, Privacy, and Technology Project, argues that stricter regulations are needed for law enforcement's use of AI. He points out that the data used in these systems often reflects over-policing in minority communities, which could lead to negative consequences for these groups. Wessler expressed concern that AI technology could cause significant issues for police departments, potentially resulting in harm. He noted that similar problems have occurred with other technologies like facial recognition, which have disproportionately affected people of color. He believes that AI carries the same risks and could lead to wrongful arrests and other adverse outcomes (Hunter, 2024).

There is growing public concern about the possibility of innocent people being detained due to errors in technology. This underscores the need for AI to be used as a preliminary tool in investigations rather than a definitive solution. AI results should initiate an investigation, not conclude it, with law enforcement relying on additional evidence and factors to accurately identify suspects rather than making hasty decisions based solely on AI outputs (Lunter, 2023).

Furthermore, AI's effectiveness relies heavily on the quality of the data it processes. Incomplete, outdated, or inaccurate data can lead to misleading results and undermine the reliability of AI tools. Ensuring high-quality, comprehensive datasets is essential but can be challenging and resource intensive (Luz & Olaoye, 2024).

In addition, modern AI systems that can be used in criminal investigations are systematically vulnerable to a new type of cybersecurity attack called "AI attack." Using this attack, accused

persons, or criminals can manipulate these systems to escape criminal liability. As AI systems become increasingly integrated into the field of criminal investigation, these AI attacks represent an emerging and systematic vulnerability with the potential to have negative effects on the course of criminal investigations (Comiter, 2019).

Moreover, there is a risk that law enforcement agencies may become over-reliant on AI tools, potentially leading police to ignore contradictory evidence as well as a reduction in critical thinking and investigative skills among police officers (Hunter, 2024; Fan, 2024). While AI can assist in investigations, it should complement, not replace, human judgment and expertise.

6.3 Ethical Considerations for Using Artificial Intelligence in Criminal Investigation

In addition to the human rights challenges such as bias, discrimination and privacy which were illustrated in Section 5 of this paper, there are several ethical considerations surrounding the use of artificial intelligence (AI) in criminal investigations. Here are some important key ethical concerns:

a) Accountability and Transparency: The use of AI in criminal investigations can obscure decision-making processes, making it challenging to understand how conclusions are reached. This lack of transparency can impede accountability, as it may be unclear who is responsible for errors or wrongful decisions made by AI systems. Many AI algorithms function as “black boxes”, where their decision-making processes are not easily comprehensible or accessible to users. This opacity can hinder trust and scrutiny from investigators, legal professionals, and the public, potentially complicating legal proceedings and accountability (Brożek et al., 2024). Ensuring transparency in AI systems and establishing clear lines of accountability are essential for maintaining trust in the justice system.

b) Misuse and Abuse: The potential for misuse of AI technologies in criminal investigations is a significant ethical concern. AI systems could be employed for purposes beyond their intended use, such as unauthorized surveillance or evidence manipulation (Lunter, 2023). To prevent such misuse and ensure responsible use of AI tools, it is crucial to establish strict regulations and ethical guidelines.

c) Informed Consent: The use of AI technologies often involves collecting and analyzing personal data. It is vital to ensure that individuals are fully informed about how their data will be used and that they provide consent for its collection and analysis (Rhem, 2023). This is especially important in criminal investigations, where the data can be particularly sensitive and personal. It is worth mentioning that the accused should be informed when information related to them is obtained through technological means during a criminal investigation, based on both ethical and legal considerations. Ethically, transparency about how personal data is collected and used respects the individual’s right to privacy and promotes trust in the justice system. Legally, jurisdictions require that evidence, including that obtained through technology, be disclosed to the defense to ensure the accused can challenge it and maintain their right to a fair trial. This disclosure helps

ensure that evidence is collected lawfully and meets procedural standards, which is crucial for its admissibility in court (Simonato, 2014).

Addressing the ethical concerns surrounding AI in criminal investigations demands a balanced approach that integrates robust safeguards, transparency, and ongoing oversight. The deployment of AI raises complex ethical and legal questions, including issues related to data collection consent, the scope of surveillance, and the potential misuse of technology (Olaoye & Potter, 2024). To ensure that AI technologies respect privacy, fairness, and justice while enhancing investigative capabilities, it is crucial to engage with diverse stakeholders, such as legislatures, legal experts, and community representatives. This collaborative effort helps to develop and implement statues and regulations that protect civil liberties and rights while advancing the use of AI in criminal investigations.

6.4 Case Studies on the Use of Artificial Intelligence in Criminal Investigation

The use of artificial intelligence (AI) in criminal investigations varies significantly across different countries and legal frameworks, reflecting diverse approaches to leveraging technology while navigating associated ethical and legal challenges. Here are some case studies illustrating how AI has been utilized in criminal investigations globally:

a) United States: Predictive Policing and Facial Recognition

In the United States, AI technologies are extensively employed in predictive policing and facial recognition. One notable example is the use of predictive policing tools such as PredPol, which analyzes historical crime data to anticipate potential future crime hotspots. Specific examples include (Lau, 2020; Epstein & Emerson, 2024):

- Chicago Police Department (CPD): CPD has experimented with predictive policing technologies, which may involve AI for analyzing various data sources, including social media.
- Los Angeles Police Department (LAPD): LAPD has explored predictive policing technology, incorporating elements of AI and social media analysis for intelligence gathering.
- Baltimore Police Department: Reports suggest that the Baltimore Police Department has utilized social media monitoring tools for intelligence gathering, though the extent of AI use is less clear.

Additionally, facial recognition technology has been employed by law enforcement agencies such as the FBI to identify suspects from surveillance footage. However, this technology has sparked significant debate over its accuracy and potential for misuse. For example, higher error rates in identifying individuals from minority groups have raised concerns about privacy and civil rights violations. In response, some cities, such as San Francisco, have enacted bans on the use of facial recognition by city agencies. In 2019, San Francisco's Board of Supervisors voted to prohibit city agencies, including the police department, from using facial recognition technology, and about two dozen other U.S. cities have since implemented similar bans (Conger et al., 2019; Joh, 2022).

b) United Kingdom: Use of AI in Crime Analysis and Policing

In the United Kingdom, AI technologies have been employed for crime analysis, crime prediction and investigative purposes. For example, several police forces across the UK including the Metropolitan Police Service in London have used AI to analyze large volumes of data to predict and prevent crime. One notable project is the use of AI to identify patterns in criminal behavior and optimize police resource deployment. In the UK, Predictive policing uses algorithms to forecast where crimes tend to occur, founded on historical data, providing appropriate measures (Christie, 2021; Mahalias, 2024).

In February 2024, the UK has established guidelines for the ethical use of AI in policing, focusing on five core principles: (Wong, 2024; Gallo & Nair, 2024)

- Safety, security, and robustness
- Appropriate transparency and explainability
- Fairness
- Accountability and governance
- Contestability and redress transparency and public accountability.

The Information Commissioner's Office (ICO) provides oversight on data protection, ensuring that AI applications comply with legal standards for data privacy and protection. However, concerns remain about the potential for AI systems to inadvertently reinforce existing biases and the need for ongoing scrutiny to ensure equitable use (ICO, 2023).

c) Canada: AI in Forensic Analysis

In Canada, probabilistic genotyping (PG) technology employs artificial intelligence algorithms to analyze DNA samples obtained during police investigations or criminal prosecutions. However, like many AI and algorithmic tools used in the justice system, PG tools have implications for human rights, equity, due process, and access to justice (Presser & Robertson, 2021).

Moreover, AI is also advancing forensic analysis by enhancing the examination of digital evidence and improving investigative techniques. For instance, the Royal Canadian Mounted Police (RCMP) has leveraged AI tools to analyze large datasets and refine evidence collection processes (Hill et al., 2022).

Canada's approach includes rigorous data protection measures under the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs the collection, use, and disclosure of personal information. These regulations help ensure that AI technologies used in criminal investigations comply with privacy standards and safeguard individuals' data from misuse (Office of the Privacy Commissioner of Canada, 2020).

d) Australia: AI in Crime Prevention and Investigation

Australia has also investigated the application of AI for crime prevention and investigation.

AI tools are employed for various functions, including analyzing criminal networks and predicting potential crime patterns. For example, the Australian Federal Police (AFP) utilizes AI for cybersecurity investigations and improving the analysis of digital evidence. The AFP has stated that it uses AI to examine data collected through telecommunications and surveillance warrants, with a commitment to maintaining full transparency regarding the technology's use (Taylor, 2023).

The Australian government develops regulatory frameworks to govern the use of AI in law enforcement, aiming to balance technological progress with privacy rights. The Office of the Australian Information Commissioner (OAIC) manages data protection, ensuring that AI applications comply with privacy regulations and ethical standards (Australian Government, 2023).

Notably, these case studies highlight the various ways AI is incorporated into criminal investigations. Although AI offers significant potential for improving investigative processes, it also presents challenges related to privacy, bias, and ethical considerations. Different countries tackle these issues in their own ways, reflecting their unique legal, cultural, and ethical priorities. Continued international dialogue and collaboration will be crucial for establishing best practices and ensuring the responsible use of AI technologies in the criminal justice system.

7. International Criminal Law: The Principles of Evidence

The legal field that deals with prosecuting and punishing individuals for crimes committed abroad is known as international criminal law, or ICL. War crimes, crimes against humanity, aggression, and genocide are some of these offences. In the quest for justice for such serious crimes, the norms of evidence are essential to guaranteeing an impartial and efficient judicial procedure. The credibility of the evidence put up before the international tribunals is crucial in determining the guilt or innocence of those involved in criminal proceedings conducted on a global scale.

The regulations and legal precepts governing the establishment of facts in court cases are collectively referred to as the law of evidence. The diverse legal traditions' differing approaches to fact-finding and evidence further complicate the already complex international laws of evidence (Hazard & Dondi, 2006). To differing degrees, all international and internationalised criminal tribunals have combined elements of the common and civil law systems in their institutional design as well as their rules of evidence and procedure (Picker, 2021). Determining the applicable law might be challenging because relevant regulations are dispersed across several sources. Notably, the foundational documents of international courts frequently do not specify the norms of evidence, giving judges a great deal of latitude. Due to the absence of juries, evidence requirements in international criminal law are typically more permissive than in common law regimes (Brady, 1999). Furthermore, it is challenging to forecast the outcomes made by international criminal courts and tribunals due to their mixed benches, which include judges from both legal traditions.

Three steps are involved in the evaluation of evidence in proceedings before the International

Criminal Court: Submission or identification; Admission; And weight assessment. Unless they are prima facie (demonstrably untrustworthy), all evidence will be submitted, that is, noted on the record before being formally acknowledged (ICC, 2011). The Chambers may opt to rule on the admissibility of the evidence at any time throughout the trial when the parties submit evidence, or they may decide to hold off until after they have rendered a decision. Evidence exclusion is rare since international judges have demonstrated a tendency to accept evidence, even when they are free to assign it little or no weight. A few Chambers have allowed exceptions for specific pieces of evidence, but the majority of Chambers decide to rule on admissibility in the final judgement. When digital evidence is involved and crucial to the prosecution's case, such exceptions have happened. For instance, the Trial Chamber in Bemba et al. made an exception for evidence such as call data records, telephone intercepts by Dutch authorities, and financial records originating from Western Union, even though it decided to rule on admissibility only after the final judgement was rendered. This was because these more recent forms of evidence were unheard of at the ICC (2016).

The admissibility of evidence under International Criminal Law (ICL) is dependent upon a number of fundamental concepts. First and foremost, in order to keep the focus on proving guilt or innocence, all evidence must be pertinent and directly related to the allegations at hand. Any irrelevant material must be removed. Second, the legitimacy and dependability of the evidence are critical; international tribunals have strict guidelines to follow, examining details like the evidence's source, acquisition technique, and consistency. Last but not least, justice requires that evidence that is acceptable be gathered in accordance with international human rights standards. This means that evidence gathered by coercion, torture, or any other violation of fundamental rights is not admissible and should not be used (Freeman, 2018).

Evidence of many kinds is essential to International Criminal Law (ICL) proceedings. Documentary evidence is a fundamental component that includes official documents, reports, and communications obtained from government agencies, international organisations, or non-governmental organisations (Freeman, 2018). Witnesses, especially victims and specialists, offer testimonial evidence, which provides firsthand recollections and expert judgements that are essential for establishing case facts. To establish a factual basis for the charges, forensic evidence, which includes DNA analysis, forensic pathology, and ballistics, is frequently presented in support of or opposition to witness testimony. Furthermore, in the contemporary period, electronic evidence -which includes emails, phone conversations, and digital documents- bears greater weight, necessitating strict protocols to guarantee authenticity and integrity during international criminal prosecutions.

8. Conclusion

It is evident that technological advancements have a major impact on how every system functions, including the criminal justice system. Any new technology should be adapted, but society must also embrace it and provide the necessary ethical justification. People are adopting new technology tools without realising the effects it will have on society at large and on themselves.

International investigators and prosecutors must continuously modify their procedures and

rules to handle new legal challenges concerning digital evidence since technology is always changing. In order to stay abreast of advancements in the usage and use of current technologies, international criminal investigators, attorneys, and judges must continuously acquire new skills. The integration of portable gadgets and growing connection will cause an exponential growth in the amount of data that is available. But the sheer volume might tax investigation resources to the breaking point and result in an untenable backlog of digital evidence. There have been significant advancements in the field of information technology, which have increased the importance of digital evidence analysis and collection as a tool for criminal investigation and court case preparation.

In conclusion, the pervasiveness of digital technology in modern society has changed not only how we interact and live but also spawned a complicated web of interactions between criminal activity and technological breakthroughs. The COVID-19 pandemic's aftermath has sparked an unparalleled increase in the use of digital tools in many facets of daily life. Technology gives people more power and convenience, but it can also be a powerful instrument that thieves can use to their advantage, especially when it comes to fraud and cybercrimes. With a greater reliance on digital tools like drones and body-worn cameras, policing and security management have experienced a paradigm shift that presents opportunities as well as problems for law enforcement.

Identity theft has become more common over the last few years, which emphasises how urgent it is to fix the weaknesses in our digital infrastructure. As society relies more on computers and the internet for financial transactions, the convenience of monitoring our financial activity is paired by the rising risk of cyber-deception and theft. The study highlights the necessity of integrating modern information technology in the fight against crimes committed in the twenty-first century. Technological devices and specialised software are turning into essential tools in the fight against the growing wave of cybercrimes, which highlights the significance of a complex legal system. The study emphasises how new and developing technologies are revolutionising criminal justice and crime prevention, underscoring the necessity for flexible legal frameworks that strike a balance between the growth of technology and the defence of civil liberties and the effectiveness of law enforcement. This research offers insightful information to scholars, legal experts, and legislators who are attempting to understand how law and technology are interacting in the digital age.

The integration of emerging technologies into criminal investigations presents both opportunities and challenges. Policymakers should develop comprehensive regulations that address data privacy, ethical use, and transparency, including stringent protections for personal data and ethical guidelines for technology deployment. To ensure accountability, law enforcement, and legal practitioners should adopt practices that include mandatory disclosure of AI algorithms and independent oversight audits. Additionally, interdisciplinary collaboration is crucial for addressing the complexities of new technologies through research, training, and development of adaptive legal standards.

To navigate these challenges effectively, it is essential to update legal frameworks to account

for technological advancements, focusing on privacy laws and bias mitigation. International cooperation should also be encouraged to harmonize regulations and share knowledge across jurisdictions. By implementing these strategies, stakeholders can enhance investigative capabilities while safeguarding individual rights and promoting fairness in the criminal justice system.

The limitations of this research include its scope and applicability. This study does not cover every emerging technology or the full range of criminal investigation laws across different jurisdictions. Instead, it focuses on providing a broad overview of general principles and ideas related to the legal implications of emerging technologies in criminal investigations. Consequently, the research highlights overarching trends and challenges without delving into the specifics of individual technologies or national legal frameworks. Future studies could explore more detailed aspects of this topic, such as examining the impact of emerging technologies within specific countries or analyzing particular legal systems. This would allow researchers to address gaps and develop a more nuanced understanding of how various jurisdictions adapt to technological advancements in criminal investigations.

Acknowledgments

The authors have no relevant financial or non-financial interests to disclose.

References

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Australian Government. (2023). *Safe and responsible AI in Australia*. Retrived from https://cdn.ymaws.com/iot.org.au/resource/resmgr/resources/advocacy/ttd/safe-and-responsible-ai-in-a.pdf

Brożek, B., Furman, M., Jakubiec, M., & Kucharzyk, B. (2024). The black box problem revisited. Real and imaginary challenges for automated legal decision making. *Artificial Intelligence and Law*, *32*, 427–440. https://doi.org/10.1007/s10506-023-09356-9

Bex, F., van den Braak, S., van Oostendorp, H., Prakken, H., Verheij, B., & Vreeswijk, G. (2007). Sense-making software for crime investigation: How to combine stories and arguments? *Law, Probability and Risk*, *6*(1–4), 145–168. https://doi.org/10.1093/lpr/mgm007

Boskovic, M. M. (2020). Implications of new technologies on criminal justice system. *Journal of Eastern-European Criminal Law*, *2*, 137–148.

Brady, H. (1999). The system of evidence in the statute of the International Criminal Court. *Essays on the Rome Statute of the International Criminal Court*, *1*, 279–302.

Brayne, S. (2018). The criminal law and law enforcement implications of big data. Annual *Review of Law and Social Science*, *14*, 293–308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839

Breslin, M., & Lowery, R. G. (2021). Technology: Opportunities and challenges for criminal investigations. *American Intelligence Journal*, *38*(1), 57–65.

Brynjolfsson, E., & Mcafee, A. (2017) The Business of Artificial Intelligence. *Harvard Business Review*, *7*, 3–11. Retrieved from: https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf

Burnett, J., Xia, R., Suchting, R., & Dyer, C. (2017). *Exploring Elder Financial Exploitation Victimization*. Project of the University of Texas Health Science Center at Houston, National Criminal Justice Reference Service. Retrieved from https://www.ojp.gov/pdffiles1/nij/grants/250756.pdf

Chicago Police Department. (2011). *Chicago Police Predictive Policing Demonstration and Evaluation Project: Phase 2*. NIJ award number 2011-IJ-CX-K014. Retrieved from https://nij.ojp.gov/funding/awards/2011-ij-cx-k014

Christie, L. (2021). *AI in policing and security*. UK Parliament. Retrieved from https://post.parliament.uk/ai-in-policing-and-security/

Comiter, M. (2019). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. Belfer Center Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf

Conger, K., Fausset, R., & Kovaleski, S. (2019). *San Francisco Bans Facial Recognition Technology*. The New York Times. Retrieved from https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Council of Europe. (2001). *Convention on cybercrime*. Retrieved from https://www.refworld.org/docid/47fdfb202.html

Council of Europe. (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. Adopted by the European Commission for the Efficiency of Justice (CEPEJ).

Epstein, B., & Emerson, J. (2024). *Navigating the Future of Policing: Artificial Intelligence (AI) Use, Pitfalls, and Considerations for Executives*. Police Chief Online. Retrieved from https://www.policechiefmagazine.org/navigating-future-ai-chatgpt/

European Commission. (2018). *Artificial Intelligence for Europe*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

European Court of Human Rights. (1978). *Case: Klass v. Germany, Application No. 5029/71*. Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57510%22]}

European Court of Human Rights. (2011). *Case: Shimovolos v Russia, Application No. 30194/09*. Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-105217%22]}

European Court of Human Rights. (2016). *Case Szabo and Vissy v Hungary, Application No. 37138/14*. Retrieved from https://hudoc.echr.coe.int/fre/#{%22itemid%22:[%22001-160020%22]}

Fan, L (2024). *AI reduces critical thinking*. The Nexus. Retrieved from https://wvnexus.org/opinions/ai-reduces-critical-thinking/

Freeman, L. (2018). *Digital evidence and war crimes prosecutions: The impact of digital technologies on international criminal investigations and trials*. Fordham International Law Journal, 41. Retrieved from https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1

Gallo, V., & Nair, S. (2024). *The UK's framework for AI regulation*. Retrived from https://www2.deloitte.com/uk/en/blog/emea-centre-for-regulatory-strategy/2024/the-uks-framework-for-ai-regulation.html

Gupta, R. R., & Srivastava, A. (2023). Impact of emerging technology on recent criminal scenario. *IP International Journal of Forensic Medicine and Toxicological Sciences*, *8*(2), 65–68. https://doi.org/10.18231/j.ijfmts.2023.013

Hazard, G. C., Jr., & Dondi, A. (2006). Responsibilities of judges and advocates in civil and common law: Some lingering misconceptions concerning civil lawsuits. *Cornell International Law Journal*, *39*, 59–70.

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Hunter, J. (2024). *Do Public Safety Benefits Outweigh Risks of Police AI. Government technology*. Retrieved from https://www.govtech.com/public-safety/do-public-safety-benefits-outweigh-risks-of-police-a

Information Commissioner's Office (ICO). (2023). *Guidance on AI and data protection*. Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

International Criminal Court (ICC). (2011). *Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08-1386*. Judgment on the appeals of Mr Jean-Pierre Bemba Gombo and the Prosecutor against the decision of Trial Chamber III entitled "Decision on The Admission into Evidence Of Materials Contained In The Prosecution's List Of Evidence". Retrieved from https://www.icc-cpi.int/court-record/icc-01/05-01/08-1386

International Criminal Court (ICC). (2016). Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/13-1854. In *Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69* (p. 7)". Retrieved from https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2016_03125.PDF

Ivliev, P., Ananyeva, E., Prys, I., & Burbina, Y. (2023). The use of IT technologies in the

prevention of crimes. *BIO Web of Conferences*, *65*(35), 9. https://doi.org/10.1051/bioconf/20236508007

Jacobson, N. (2022). *How technology is used for criminal investigations*. Open Fox. Retrieved from https://www.openfox.com/how-technology-is-used-for-criminal-investigations/

Joh, E. (2022). Ethical AI in American Policing. *Notre Dame Journal on Emerging Technologies*, *3*(2), 261–287.

JWU. (2023). *Empowering justice: Exploring the impact of criminal justice technology in the modern era*. Retrieved from https://online.jwu.edu/blog/empowering-justice-exploring-impact-of-criminal-justice-technology-modern-era/#:~:text=From%20technological%20advancements%20like%20surveillance,parole%2C%20and%20even%20courtroom%20appearances

Land, M. K., & Aronson, J. D. (2020). Human rights and technology: New challenges for justice and accountability. *Annual Review of Law and Social Science*, *16*, 223–240. https://doi.org/10.1146/annurev-lawsocsci-060220-081955

Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016). *How we analyzed the COMPAS recidivism algorithm*. ProPublica. Retrieved from https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Lau, T. (2020). *Predictive Policing Explained*. Brennan Center for Justice. Retrieved from https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

Laufs, J., & Borrion, H. (2022). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management*, *24*(2), 190–209. https://doi.org/10.1177/14613557211064053

Leite, E., Leite, M. & Leite, A. (2023). AI's impact on human rights: the need for legal evolution. *Journal of Entrepreneurial Researchers*, *1*(2), 81–86. https://doi.org/10.29073/jer.v1i2.16

Lindsey, N. (2018). *Artificial intelligence: privacy and legal issues*. CPO Magazine. Retrieved from https://www.cpomagazine.com/data-privacy/artificial-intelligence-privacy-and-legal-issues/

Lunter, J. (2023). *Can criminal investigations rely on AI*? Retrieved from https://www.biometricupdate.com/202311/can-criminal-investigations-rely-on-ai

Luz, A., & Olaoye, G. (2024). *Data quality and data privacy challenges in AI applications*. Retrieved from https://www.researchgate.net/publication/378904709_Data_quality_and_data_privacy_challenges_in_AI_applications

Mahalias, I. (2024). *AI adoption in criminal justice – How can industry support the justice system in implementing Artificial Intelligence*. Retrieved from

https://www.techuk.org/resource/ai-adoption-in-criminal-justice-how-can-industry-support-the-justice-system-in-implementing-artificial-intelligence.html#:~:text=In%20the%20UK%2C%20AI%20tools,historical%20data%2C%20providing%20appropriate%20measures

Marcus, J. (2023). *Louisiana police sued for wrongly arresting Black man using AI face recognition program*. Retrieved from https://www.independent.co.uk/news/world/americas/crime/louisiana-police-facial-recognition-lawsuit-b2419085.html

Miller, A. P. (2018). Want less-biased decisions? Use algorithms. *Harvard Business Review*. Retrieved from https://hbr.org/2018/07

Monash University. (2021). *Using AI to combat street crimes*. Retrieved from https://hbr.org/2018/07

Monteleone, S. (2017). *Fundamental Rights Implications of Big Data*. France: European Parliament.

National Institute of Justice. (2014). *A Hybrid Machine Learning Approach for DNA Mixture Interpretation*. Syracuse University Project. Retrieved from https://nij.ojp.gov/funding/awards/2014-dn-bx-k029

National Science and Technology Council and the Networking and Information Technology Research and Development Subcommittee. (2016). *The National Artificial Intelligence Research and Development Strategic Plan*. Washington, DC: Office of Science and Technology Policy.

Office of the Privacy Commissioner of Canada. (2020). *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*. Retrieved from https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/

Olaoye, F., & Potter, K. (2024). *Ethical Considerations in Artificial Intelligence*. Retrieved from: https://www.researchgate.net/publication/379033670_Ethical_Considerations_in_Artificial_Intelligence

Ortiz-Pradillo, J. C. (2017). The New Regulation of Technology-Related Investigative Measures in Spain. *ERA Forum*, *18*(3), 425–435. https://doi.org/10.1007/s12027-017-0484-1

Pedreschi, D., & Miliou, I. (2020). *Artificial intelligence (AI): New developments and innovations applied to e-commerce*. France: European Parliament.

Picker, C. B. (2021). International law's mixed heritage: A common/civil law jurisdiction. *Vanderbilt Law Review*, *41*(4), 1083–1140.

Presser, J., & Robertson, K. (2021). *AI Case Study: Probabilistic Genotyping DNA Tools Used in Canadian Courts*. Law Commission of Ontario. Retrieved from https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/ai-case-study-

pg/

Rhem, A. J. (2023). Ethical use of data in AI Applications. In R. Miroslav (Ed.), *Ethics - Scientific Research, Ethical Issues, Artificial Intelligence and Education*. IntechOpen. https://doi.org/10.5772/intechopen.1001597

Rigano, C. (2018). *Using artificial intelligence to address criminal justice needs*. National Institute of Justice. Retrieved from https://www.nij.gov/journals/280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.aspx

Rowena, R. (2020). Legal and human rights issues of AI: Gaps, challenges, and vulnerabilities. *Journal of Responsible Technology*, *4*. https://doi.org/10.1016/j.jrt.2020.100005

Sakka, A. (2023). *COVID-19 pandemic policies in Malaysia and the issues of privacy and data protection*. Master's dissertation. International Islamic University Malaysia.

Simonato, M. (2014). Defence rights and the use of information technology in criminal procedure. *Revue internationale de droit pénal*, *85*, 261–310. https://doi.org/10.3917/ridp.851.0261

Slobogin, C., & Brayne, S. (2023). Surveillance technologies and constitutional law. *Annual Review of Criminology*, *6*, 219–240. https://doi.org/10.1146/annurev-criminol-030421-035102

Stand For Girls. (n.d.). *Raising awareness campaigns in the United States*. Retrieved from https://standforgirls.org/where-we-work/united-states/

Stanila, L. (2020). Memories of the future - Sweetie and the impact of the new technologies on the criminal justice system. *EU and Comparative Law Issues and Challenges Series* (ECLIC), *4*, 557–575. https://doi.org/10.25234/eclic/11916

Taniguchi, T., Aagaard, B., Baumgartner, P., Young, A., & Wenger, M. (2019). *Applying Data Science to Justice Systems: The North Carolina Statewide Warrant Repository* (NCAWARE). RTI International, National Criminal Justice Reference Service. Retrieved from: https://www.ojp.gov/pdffiles1/nij/grants/303964.pdf

Taylor, J. (2023). *Australian federal police using AI to analyse data obtained under surveillance warrants*. The Guardian. Retrived from https://www.theguardian.com/australia-news/2023/sep/22/australian-federal-police-afp-using-ai-analyse-surveillance-warrants-data

Thao, N. (2023). The Use of Artificial Intelligence in Criminal Investigation and Trials in Europe and Some Countries: Experience for Vietnam. *Vietnamese Journal of Legal Sciences*, *8*(1), 55–77. https://doi.org/10.2478/vjls-2023-0003

The Intelligence Advanced Research Projects Activity (IARPA). (n.d.). *Janus*. Washington, DC: Office of the Director of National Intelligence. Retrieved from

https://www.iarpa.gov/research-programs/janus

The National Fraud Center. (2020). *The Growing Global Threat of Economic and Cyber Crime*. New York: LexisNexis.

Wong, D. (2024). *How UK Police Agencies Can Use AI in 2024*. Retrieved from https://www.veritone.com/blog/how-uk-police-agencies-can-use-ai-in-2024/

Copyrights