Copyright © 2023 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2023. Vol. 17(2): 77–94. DOI: 10.5281/zenodo.4766706
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

# Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview

***Raed S. A. Faqir***[1,2*]
American University in the Emirates, UAE

## Abstract

*Artificial Intelligence (AI) has been integrated within digital criminal investigations comprehensively with the help of associated methodologies, legal ramifications, and its overarching impact on the justice system. This study adopted a multifaceted approach encompassing qualitative, descriptive, and analytical methods, drawing its data primarily from an array of legal documents and scholarly literature. Through its investigation, this study elucidated the pivotal role that AI plays within law enforcement, encompassing aspects such as arrest procedures, release decisions, sentencing processes, prediction of recidivism, identification of criminal activities and patterns, as well as the apprehension of suspects through advanced audio analysis techniques. The findings underscore the transformative potential of machine learning techniques in enhancing the analysis and organization of case data. The study provides a series of recommendations aimed at optimizing the utilization of AI in digital criminal investigations. These recommendations advocate for the prioritization of high-risk cases through the incorporation of diverse data sources to facilitate well-informed decision-making. Additionally, the study advocates for the deployment of AI in crime prediction, suspect identification, and the reinforcement of security measures. Furthermore, it underscores the importance of implementing AI-powered biometric identification (Bio-ID) systems to fortify identity verification processes. Lastly, the study advocates for the implementation of intelligent surveillance solutions to proactively prevent criminal activities, utilizing advanced visual analysis techniques. Concurrently, it emphasizes the role of machine learning in streamlining case management processes, thereby providing precise recommendations and enhancing overall efficiency within the criminal justice system.*

Keywords: Digital investigation, artificial intelligence, legal frameworks, digital evidence, law enforcement.

[1] Associate Professor in the programme of Master in Criminal Sciences, College of Law, American University in the Emirates, UAE. Email: raed.faqir@aue.ae
ORCID: https://orcid.org/0000-0002-6102-0983
[2] Associate Professor in Criminal Law, Faculty of Law, Balqa Applied University, Jordan. Email: r.faqir@bau.edu.jo
* Corresponding Author Email: raed.faqir@aue.ae

## Introduction

Digital criminal investigation is an advanced form of investigative procedures which involves several applications of computer science including validation with mathematical tools. Also known as digital forensics, it identifies and preserves digital evidence to facilitate investigation procedures (Dunsin, Ghanem, & Ouazzane, 2022). Evolved in mid-1980s, digitally equipped criminal investigation has unequivocally solidified its status as an indispensable method of law enforcement, national security, and the validation of legal processes. This specialized discipline is intricately entwined with the systematic collection, analysis, and extraction of digital evidence procured from electronic devices, with the primary objective of its judicious application in legal proceedings. Digital criminal investigation, in its multifaceted role, deftly navigates the realms of retrospection, encompassing the scrutiny of historical events, and proactivity, aimed at preempting potential threats, while simultaneously upholding the sanctity of digital environments and preserving individual privacy (Costantini, De Gasperis, & Olivieri, 2019).

In recent times, Artificial Intelligence (AI) has proved a highly effective mechanism in identifying risks by forecasting and preventing any kind of criminal activity. This is achieved through an algorithm customized to handle security breaches, cybercrimes and to analyze evidences (Mijwil, Mohammad, & ChatGpt, 2023). The AI mechanisms, assisted by its various forms like deep learning and machine learning algorithms, are also adopted for surveillance, to monitor anomalies in crowd or mob crimes through close-circuit cameras and video footages enabling facial recognition. These AI applications are in stark contrast to conventional criminal investigations as AI-enabled investigations stand out as a distinct domain of computer-generated data analysis and their admissibility in a judicial context. Furthermore, AI systems are shown to bolster real-time surveillance capabilities, potentially discerning intentions from subtle cues in facial expressions and body language. In conclusion,

There are several specialized software and methodologies strategically linked to AI enabled technology to extract pivotal digital artifacts as evidences, including but not limited to emails, chat logs, and metadata. These evidences are both reliable and legally admissible. Hence, the science of digital investigation assisted by AI applications thrives on diversity, leveraging cutting-edge tools to ensure precision, comprehensiveness in embracing a spectrum of digital evidence categories, and unwavering adherence to established legal frameworks. However, these advancements bring ethical and legal responsibilities as well. Upholding evidence integrity, respecting privacy, and ensuring fairness are paramount. Prioritizing data security, transparency, and meticulous documentation are essential steps in fostering just investigative procedures (Costantini et al., 2019; Hall, Sakzad, & Choo, 2021).

Within the United Arab Emirates (UAE), IT infrastructure has made a colossal growth and the country is expected to become a leading tech giant by 2025 (Abdo & Yusof, 2023; Dahabreh, 2023). Only in 2019, the revenue of the IT companies based in UAE, and mainly in Dubai were estimated at around $6 bn, which is a growth of 12.5% compared to 2018. Threse IT Companies in the United Arab Emirates need specialized support from digital forensics &auditing service providers, which have also grown tremendously in both public and private sectors. For instance, *Eshield IT Services* is a Dubai based cybersecurity company which is a leading provider of cybersecurity solutions. It assists clients in implementing robust security measures to protect their businesses and organizations from cyberattacks. *EXEO* is another multi-faceted cloud and cybersecurity provider agency, which helps its clients to identify risks, and to protect and monitor their assets through business process automation and smart services. The practice of digital investigation is also governed by a well-defined legal framework, in which the UAE police play a pivotal role in orchestrating and overseeing this intricate process. It is ensured that forensics and other services are designed to give end-to-end capabilities and complete forensic and security solutions, to businesses. The UAE government ensures that these forensic services establish a framework distinguished by its unwavering commitment to maintaining a robust legal foundation, preserving data confidentiality, upholding professional ethical standards, and rigorously verifying the integrity of evidence. As a result, the UAE government facilitates effective execution of digital investigation procedures within this jurisdiction (Dahabreh, 2023).

Although the AI assisted digital applications encompass a wide array of data spanning electronic devices, network records, mobile data, and content sourced from social media platforms, necessitates the harnessing of an array of technologies, including artificial intelligence, text recognition, and statistical analysis, to extract and present digital evidence in the context of legal proceedings. This serves as the rationale of this study as it is necessary to investigate and scrutinize the intricate legal dimensions and the consequential impact of AI deployment within the sphere of digital investigations.

The current research study therefore focuses on the following research objectives:

- To discern the gamut of artificial intelligence methodologies employed by law enforcement agencies in the context of digital investigations pertaining to cybercrimes.
- To rigorously ascertain the legal status of criminal evidence procured through the utilization of artificial intelligence methodologies and its admissibility in the context of criminal adjudication proceedings.
- To meticulously ensure that the integration of artificial intelligence methodologies into the sphere of criminal investigations remains in strict compliance with established legal frameworks, thereby safeguarding the individual rights and liberties enshrined within the purview of prevailing statutory enactments.
- To gain comprehensive insight into the prospective advancements and potential applications of artificial intelligence within the domain of digital criminal investigations, thereby discerning the trajectory of future developments in this critical field.

To achieve these objectives, this research embarked on an exploration of the integration of artificial intelligence (AI) with digital criminal investigations, a domain intrinsically tied to the acquisition and analysis of electronic evidence, with AI tools occupying central positions. These objectives are multifold, encompassing a comprehensive understanding of AI methodologies however, it is an urgent need to critically evaluate the legal implications associated with AI-facilitated evidence. This study attempts an in-depth analysis of the alignment of AI tools with established legal frameworks, and how this alignment impacts the pursuit of justice, and whether such AI advancements would help in the criminal investigations of cybercrimes. This study further seeks to expound upon the advantages and associated risks that AI applications pose to the fundamental rights and liberties of individuals.

## Research Methodology

The present research employs a qualitative research methodology to investigate the potential integration of artificial intelligence within the sphere of criminal digital investigation. This qualitative research endeavor is dedicated to the development of a theoretical framework for the application of AI techniques in the context of criminal investigation, in alignment with the technological facets inherent to digital and criminal investigative research methodologies. Consequently, the research strategies employed in this study encompass qualitative research, descriptive analysis, and analytical research.

In the pursuit of data acquisition, this research adopted the "normative juridical research method" and the "scientific research method," both firmly established techniques in the domain of legal studies. Data collection involved both primary and secondary sources. Primary data comprised a variety of primary legal documents, including foundational legal codes, legislative opinions, and a spectrum of technical and scientific resources pertinent to criminal procedural laws, regulations, rules, and associated documentation. The secondary data included a comprehensive analysis of existing literature pertaining to forensic investigation and criminal procedural laws, with a specific focus on the integration of artificial intelligence. An extensive literature review was conducted through database sources, which comprised reputable law journals, online legal databases accessible through institutions such as the American University in the Emirates and Balqa Applied University (including Mandumah, Springer, West Law, J.S.T.O.R., Bloomberg Law, Emerald, and Hein Online, among others), as well as a diverse array of publications in the fields of cyber and criminal investigation. To analyze the data collected from this diverse array of sources, the "content analysis method" served as the chosen analytical framework within the current research study.

## Literature Review

- *Artificial Intelligence for digital investigation*

Artificial Intelligence (AI) techniques have several applications to assist the legal agencies in combating cybercrimes. AI tools such as computational intelligence, neural networks, artificial immune systems, machine learning, data mining, pattern recognition, fuzzy logic, and heuristics have been very helpful in cybercrime detection and prevention (Dilek, Çakır, & Aydın, 2015; Sadiku, Fagbohungbe, & Musa, 2020; Verma & Gupta, 2020).The legal agencies and crime prevention units have been benefited by AI integrated tools; for instance, neural networks help detect Denial of Service (DoS) detection, computer worm detection, spam detection, malware classification and forensic investigations (Ahmed Alaa El-Din, 2022; Brown, 2015). AI techniques such as Heuristics, Data Mining, and AISs and some IDSs assist the intelligence agencies to investigate suspicious cyber activity. Cybersecurity agencies make use of AI algorithms to explore various disciplines in forensic science, including DNA analysis (Gless, 2019; Mohsin, 2020).

Gunawan Widjaja et al. (2023) in a recent study, brings into notice the use of AI tools in law enforcement and resolving various electronic crimes, such as virus attacks, phishing scams, fraudulent transactions, and identity theft. The criminal investigation takes a good shape in identifying user activity patterns, spotting anomalies or discrepancies, and raising the red flag on suspicious transactions, Intelligence agencies are able to detect and prevent crimes, identify and stop malware assaults, such as ransom ware which can potentially harm computer networks. AI algorithms are also being used in medicine to interpret radiological images, which assist greatly in investigating crimes. Likewise, Al-Amiriyeen (2022) also asserted that, given the complexity of cybercrime data, artificial intelligence-driven methods are essential for ensuring reliable digital evidence for legal proceedings. Digital criminology has been recognized as a modern field, which enhances investigations through advanced techniques by addressing criminal justice needs (Rigano, 2019; Wexler, 2018). Investigative authorities employ it to gather and analyze cybercrime data, requiring expertise in computing and specialized tools, including processing electronic crime data such as server logs, emails, social media, videos, and encrypted content (AL-Salahin & Rahman, 2017). The integration of artificial intelligence, machine learning, and big data into law enforcement has revolutionized evidence extraction, suspect identification, and digital crime detection. AI programs have revolutionized digital investigations, enhancing the collection, identification, processing, and analysis of electronic data for court-admissible digital evidence. Interpretable Artificial Intelligence (XAI) plays a pivotal role in this transformation, enabling transparent and understandable decision-making (Arshey & Viji, 2021; Heaton, 2013). It is also emphasized the importance of AI's transparency in legal proceedings, ensuring the credibility of evidence presented in court (Ahmed & Rahman, 2021). AI programs significantly contribute to improving the accuracy and transparency of digital investigations by clarifying the decision-making process. This, in turn, results in the presentation of reliable and admissible digital evidence in court, bolstering public trust in criminal justice agencies and the outcomes of digital investigations.

- *Pattern Recognition Technology*

Pattern identification, a traditional research technique, has gained prominence in criminal investigation through AI integration (Ghassouna, 2019). It utilizes methods such as image recognition to uncover concealed details, extending its application to email content categorization, including spam, images, and audio. Successful pattern recognition relies on data utilization, statistics, and inference (Babylon, 2019). The software's efficacy depends on proficiently managing extensive data through statistical analysis and probability (Rosario, Romano, & Borel-Donohue, 2011), posing challenges for investigators, especially when dealing with large datasets. Criminal investigators employ deep learning techniques such as syntax analysis for handwritten text understanding and face recognition for individual identification (Mohammed & Ameerah, 2022). These methods involve the analysis of grammatical structures and facial patterns. Neural networks, particularly deep neural networks, are employed for tasks like computer vision, natural language processing, and data recognition, including facial recognition and fingerprint analysis (Mohammed &

Ameerah, 2022). These networks extract insights from data to infer patterns and perform various tasks, including image analysis, language interpretation, and identity verification.

- *The use of Neural Network Technology*

Synthetic neural networks, inspired by human cognitive processes, are employed in law enforcement to analyze various online data sources, including servers, digital communication, websites, and social media (Ali & Al-Junaid, 2009). They excel at detecting patterns, aiding in suspect identification and evidence collection in cybercrime cases (Taqiya & Al-Wasifi, 2012). These networks learn from extensive criminal data to recognize illicit patterns, even in new information, facilitating proactive law enforcement efforts (Ibrahim, 2021). Their capabilities extend to scrutinizing large datasets, revealing anomalies like data breaches and financial crimes. They also uncover the hidden actions of suspicious users and detect potential money laundering through financial transactions. In criminal investigations, synthetic neural networks are widely used for monitoring suspicious phone conversations (Talbani & Fadi, 2014). They analyze call recordings to identify relevant keywords, leveraging machine learning's understanding of natural language and crime-related terms (Ibrahim, 2021). These models utilize call records and locations to reveal unusual behavioral patterns. They can identify individuals despite changing numbers or aliases and recognize discussions with known criminals. Furthermore, the technology effectively tracks online offender activities, monitors criminal communications, and monitors access to illicit websites (Talbani & Fadi, 2014).

- *Medical Applications (Clinical)*

Bioprinting plays a crucial role in criminal investigations by aiding suspect identification and connecting individuals to crimes through biometric data such as fingerprints, DNA, behavior, voice, and gait. Various techniques like fingerprint and DNA analysis, facial recognition, and iris identification are employed for crime investigation (Abdelfattah, 2014; Ahmed & Osman, 2016). In the realm of cybercrime, computers and information technology are essential for evidence collection, perpetrator identification, and tracking crime trails. Artificial intelligence, particularly deep learning methods, is integral to cybersecurity efforts (Jaballah, 2022). Criminal investigators utilize deep learning algorithms for cybercrime detection, including identifying online fraud, uncovering hacks, and detecting malware, viruses, hacking incidents, and cyber harassment (Jaballah, 2022).

- *Psychological Techniques*

Neurological prediction, which utilizes neuroimaging to anticipate behavior, raises legal and theoretical debates regarding its legitimacy and reliability. Despite concerns, it proves valuable in criminal investigations, especially for assessing recidivism risk (Melby, 2021). AI-supported neuroimaging, employing machine learning, uncovers behavioral patterns, notably among previous offenders (Melby, 2021). Techniques encompass MRI and PET scans, studying brain interactions in addiction, Alzheimer's, autism, and psychopathy (Fowler et al., 2007). While achieving remarkable precision, ethical and legal concerns necessitate regulatory frameworks to ensure responsible use in criminal investigations. The 'truth serum' method involves administering substances like sodium pentothal or sodium amytal to induce a semi-conscious state, aiming to extract information and confessions from suspects (Khalifa, 2008). Despite potential effectiveness, ethical and legal concerns persist, including unreliable results and false confessions (Khalifa & Mehira, 2021). Some legal systems permit its use with strict controls, yet it raises issues like self-incrimination protection (Kamil, 2002). In India, it is admissible but faces criticism for infringing on personal freedoms and the presumption of innocence (Bharadwaj & Suresh, 2008). UAE law explicitly rejects this technique, deeming its evidence illegal due to rights and dignity violations vide Article 48 of the UAE Federal Code of Criminal Procedure No. 38, 2022.

## Results and Discussion

- *AI and its integration with cybercrime and cyberlaws*

The current study made evident several unexplored facts about AI and its integration with cybercrime and cyberlaws. In recent years, cyberattacks have significantly impacted businesses, governments, and individuals due to technological advancements and increased digital platform usage (Diogenes & Ozkaya, 2019). Cybercriminals exploit software, network, and device vulnerabilities for ransom attacks, hacks, and denial-of-service attacks. In response, governments are prioritizing cybersecurity to protect society (Wairimu, 2023). Digital investigation plays a crucial role, facilitating various tasks, including cybersecurity and fraud detection, by examining financial records, email, and digital communication (Jones, 2018; Smith, 2020). Despite all advancements, investigative authorities grapple with a daunting challenge posed by the sheer volume of data, leading to associated difficulties (Casey, 2000; Daniel & Daniel, 2012). They encounter issues related to the capture, identification, and storage of criminal records, hindering efficient acquisition, storage, and processing of vast amounts of information, particularly in the management, processing, and control of digital evidence. This challenge primarily stems from the surge in big digital data, encompassing millions of records, documents, digital messages, audio files, and videos from various sources, such as transaction data, automated data, and human-generated data (Taylor, 2023), spanning computers, emails, cloud files, tablets, and social networks (Mayer-Schönberger & Cukier, 2013).

Two distinct sets of problems emerge related to operational and technical. The operational problems emerge when vast data volume prolongs investigation timeframes, causing delays in case resolution. Moreover, the data's sheer size can compromise its quality, leading to inaccuracies and incomplete information, ultimately undermining reliable conclusions. Dealing with such extensive information demands substantial resources, including computational power and storage capacity, resulting in significant state expenses for data management, preservation, and storage. Regarding technical problems, the substantial data volume complicates digital investigations as investigators contend with diverse data types and sources. This complexity intensifies with the rapid evolution of digital technologies, necessitating continuous adaptation to modern tools and techniques for data collection and analysis. Failure to keep pace can hamper investigations' efficiency and effectiveness. Overcoming these challenges requires the adoption of advanced algorithms, statistical methods, data exploration techniques, innovative data management approaches, data analysis tools, data visualization, scalable and distributed computing systems, and effective data storage and retrieval methods (Hey, Tansley, & Tolle, 2011; Leskovec, Rajaraman, & Ullman, 2020; Lin & Dyer, 2010; Mayer-Schönberger & Cukier, 2013; Ohlhorst, 2012).

- *Problems of Digital Evidence's Legitimacy*

AI applications ensure the authenticity of digital evidence is critical in criminal cases, requiring adherence to specific criteria such as data accuracy, integrity, documentation of sources and methods, and consistency with witness statements (Al-Awaram, 2014). The admissibility of digital evidence varies across various legal systems globally. For instance, Anglo-Saxon Legal System, which is adopted in countries like the United Kingdom, the United States, and Canada, there are specific legislative conditions that must be met for digital evidence to be admissible (Hilali, 2014). Judges do not have discretion in admitting evidence; rather, they assess compliance with legislated conditions. The admissibility criteria include credibility, relevance, source safety, legitimacy, and reliability of the technology used (Barbara, 2015; Casey, 2011; Cicchini, 2016; Schmidt, 2016; Scroggins, 2019). The 'Dobert' and 'Fry' standards help determine the authenticity and scientific validity of digital evidence (United States v. Simpson, 741 F.3d 539, 542, 7th Cir. 2013). Similarly, Latino Legal System requires judges to possess broad discretion to accept or reject digital evidence, even without explicit legal provisions. The evidentiary value of digital evidence is generally accepted without significant issues, and various means of proof can establish criminal proceedings. In France and the UAE, the authenticity of digital evidence has been recognized in their legal systems. The Paris Criminal Court and the Supreme Federal Court of the UAE have upheld cases based on digital evidence, emphasizing legality, reliability, safety precautions, and protection against manipulation (Société de Distribution de Films de France (SDFF) v. Google France, Paris Criminal Court, December 20, 2019; Cassation, Criminal Ruling No. 1 of 2018, The UAE Federal Supreme Court, 2018).

Regardless of the legal system, safeguarding the legality of digital investigations is essential. Judicial and law enforcement officers must respect individuals' privacy rights, ensuring that data is not searched, seized, or accessed without the appropriate judicial authorization. Reducing the volume of targeted data and implementing secure collection methods are essential to preventing privacy violations. Legislation and regulations governing digital evidence examination, collection, preservation, analysis, and submission to the court should also be considered.

- *Challenges for digital investigation*

The digital investigation phase poses several challenges, including data volume, fragmentation, compression, encryption, cybersecurity threats, and legal and privacy issues (Daudi, 2022). Investigators, prosecutors, and police officers must analyze substantial data sets, often requiring artificial intelligence techniques and tools for data decoding and encryption key retrieval (Al-Radvani, 2014). Digital investigators face the complexity of gathering evidence distributed across physical and virtual environments. Data and digital evidence can be found on various electronic media, such as hard drives, CDs, DVDs, USB drives, memory cards, information systems, internet servers, and social media platforms (Casey, 2000, 2011). Notably, social media platforms like Instagram, Twitter, Facebook, OneDrive, Digital Cash Exchange Networks, Google Drive, and

Microsoft have become hubs for distributing digital evidence, often containing videos, conversations, photos, and documents. The widespread distribution of digital evidence on internet platforms poses challenges for collection and analysis. Retrieving this evidence, accessing digital sources, and processing it demand significant effort, time, expertise, resources, and digital intelligence. Therefore, effective digital investigative units should collaborate with experts to recover and analyze data stored on physical media like hard drives, CDs, DVDs, USB drives, memory cards, and information systems.

Another challenge faced in criminal investigation is respecting individual privacy and protection of individual privacy rights (Hess, Orthmann, & Cho, 2016; Silva et al., 2021). A digital criminal investigation hinges on respecting constitutional, legal, and moral principles related to individual privacy rights. Cybercrime investigators must be mindful of the potential privacy violations that may occur when collecting and storing large amounts of data on suspects (Casey, 2000). Privacy concerns in digital investigations pose significant challenges for law enforcement and prosecutors as they seek to balance the need for criminal evidence with individual privacy rights. Unlike traditional investigations, digital investigations involve the collection, analysis, and preservation of extensive personal data and information about potential perpetrators (Verma & Ramanathan, 2022). Addressing this challenge requires investigators to ensure that their methods align with constitutional, legal, and ethical standards. To mitigate privacy violations during digital investigations, we propose a set of procedural and substantive measures. Firstly, investigators should refrain from conducting searches or seizures of electronic devices and their data without obtaining a warrant from legally authorized authorities. This ensures that investigators have the necessary legal authority to access individuals' personal information. Secondly, investigators should focus on the quality rather than the quantity of data by employing targeted research and filtering methods. Finally, data security should be ensured through encryption, password protection, and other security measures to prevent unauthorized access to collected information (Verma & Ramanathan, 2022).

- *Role of international organizations*

Several international organizations have taken the initiative to combat AI crimes with respect to the application of legal principles through cybercrime frameworks. For instance, International Telecommunication Union (ITU), an agency of the United Nations, devised a toolkit for Cybercrime Legislation and shared it with all member nations to plan strategies for developing cybercrime legislation in respective countries. The ITU's toolkit acts as a model law for countries, because of its global application owing to its universality of legislative measures. The ITU cybersecurity framework covered a very wide scope cybercrimes such as unauthorized access or disruption to computers or computer networks; digital forgery; digital fraud; and extortion. The ITU cybersecurity framework also laid down certain legislations including fixing the liability of leadership in case of cybercrimes committed by employees in an organization (Brundage et al., 2020; Mohsin, 2020).

Another framework that can be mentioned here is the framework of Council of Europe Convention on Cybercrime, also known as the Budapest Convention, which proclaimed to establish a common criminal code globally to combat cybercrimes.

Some of the cyber offences identified in the Convention included illegal access and interception in computer systems and networks; data interference and misuse of devices; computer related forgery and fraud, copyright infringements, and like. The convention also emphasized upon determining the liability, especially when there exists regional and national cybercrime framework across nations. The Convention felt the need to devise new codifications which are equipped with latest devices to identify latest offences like cyber espionage and cyber weapons (Sadiku et al., 2020).

- *Transparent& Interactive AI models*

The study witnessed the presence of several AI models in the extant literature that help in digital criminal investigations, aiding investigators in taking decisions during data collection, processing, and analysis. Investigative authorities commonly use two types of models: Transparent AI models and Interactive AI models (Mohammed, 2023). Transparent AI models provide reliable and valid results, allowing investigators to understand and clarify decision-making processes (how and why). Interactive AI models enable investigators to interact with machine learning and deep learning models, enhancing their understanding of these algorithms' decision-making mechanisms (Mohammed, 2023). The Interpretable AI models encompass both transparency and interactivity, enhances investigators' abilities to grasp automated and complex deep learning decision processes. These tools offer insights into the analysis and processing mechanisms employed by these intricate models. A few of these models are worth mention in the context of the current study.

—*Machine Learning and Deep Learning Models*

Artificial intelligence and machine learning models, including deep learning integral to automated decision-making processes that learn from specific data and patterns, reducing human intervention. Deep learning, an advancement in artificial intelligence, performs complex functions such as sound recognition, facial feature analysis, and pattern recognition in digital data (Hamzawi, 2021). Both machine learning and deep learning are computer-based approaches to skill and concept learning, differing in complexity and performance. Machine learning involves automating analytical model creation, while deep learning trains computers independently by recognizing patterns through various processing layers (Hamzawi, 2021). Criminal investigation authorities utilize machine learning in digital investigations to expedite digital evidence searches and analysis, providing reliable court-admissible evidence (Tahfah, 2020). These models identify intricate digital data patterns and assist investigators in analyzing data relationships (Al-Ghafri, 2007, 2009). In digital investigations requiring accurate and complex results, deep learning models analyze features of various data types, such as images, sounds, texts, videos, audio files, and online interactions. This analysis relies on synthetic neural networks and complex algorithms (Hamzawi, 2021). These models also aid in analyzing digital data, evidence, incidents, and suspect behaviors across various crimes, helping investigators predict future events, identify perpetrators, determine sources of communication, verify and manipulate media, and detect cybercrimes like fraud, espionage, and cyberterrorism (Iqbal, Debbabi, & Fung, 2020).

—*Natural Language Processing Models (NLP)*

NLP model specializes in natural language processing, analyzing text data from various sources, including chat records, emails, and social media posts (Adamson, 2023). It processes extensive natural language text data from the internet to extract relevant information. Digital criminal investigation agencies prioritize AI-driven NLP models due to the surge in digital text data and information technology. These models assist investigators in monitoring digital data related to criminal activities and collecting data from diverse sources for crime detection and prediction. Much of this data is unstructured and unclassified, necessitating intelligent models for organization and categorization as manual verification is impractical (Dogra et al., 2022) practice, digital investigation authorities employ NLP techniques and models like the Automated Response Model (ARA), Text Linguistic Analysis Model (NLA), Bing Model, Stanford Model, and Emotion Analysis Model (Sentiment Analysis). These models classify digital text data by emotions, topics, and language and identify individuals, facts, dates, institutions, messages, documents, emotions, connections, relationships, and crime-related information. They also analyze text sentiments in individuals' communications on social media and electronic platforms.

—*Image and Video Analysis Models*

AI technologies, including machine learning and deep learning algorithms like convolutional neural networks, play a crucial role in image and video analysis during digital investigations (Vamathevan et al., 2019). These algorithms help identify objects, classify images, recognize faces, and interpret contexts and scenes from visual data in photos, videos, and audio files. They are essential tools for acquiring visual evidence, such as surveillance footage or images, during digital investigations. However, analyzing video and photo data can be challenging and resource-intensive. It requires expertise in the field, and there is a risk of human error due to the vast volume of data and constant changes in smartphone generations and operating systems (Babylon, 2019). In practice, law enforcement agencies can train AI algorithms to identify specific objects, tools, or content categories within videos and images, including people, objects, animals, tools, and vehicles. These algorithms can also recognize facial features or interpret specific contexts and scenes in photographs or videos. In conclusion, AI techniques, including machine learning and deep learning, excel in analyzing visual data, classifying objects, and identifying features like shape, texture, and color in images and videos. These capabilities greatly assist investigators in detecting and interpreting visual content, including images, videos, and social media posts.

—*Expert Systems Models*

Expert systems are essential AI tools that encode human expertise and knowledge into software formats (Al-Hassan, 2010). These systems use intelligent human knowledge to solve complex problems, collaborating with human experts in the field. Investigators employ expert systems during digital investigations to address digital evidence-related challenges. Expert systems possess unique attributes, including speed, efficiency, logical reasoning, depth of analysis, and self-awareness, setting them apart from traditional software (Al-Hassan, 2010). They can interpret, diagnose, design, plan, monitor, predict, learn, and perform tasks at the level of human experts quickly and professionally. In digital investigations, expert system models analyze intricate digital data and provide recommendations based on their analysis. The effectiveness, accuracy, and efficiency of these systems depend on their ability to absorb specialized knowledge in the field of data and digital evidence. By assimilating this expertise, these systems can analyze patterns and electronic data to offer pertinent recommendations regarding critical digital evidence in financial, criminal, and electronic investigations.

—*Automated Robot Models*

Robotic automation models play a crucial role in digital criminal investigations, streamlining various tasks. These models aid investigators in collecting digital data from diverse sources such as public records, social media, and other digital platforms, analyzing reports, memos, and emails (Azhari, 2020), examining financial records and digital financial data to detect fraud, embezzlement, and money laundering, and managing large volumes of investigation data and documents. Automation of these processes allows investigators to focus on the legal and technical aspects of data analysis, pattern identification, and trends related to digital investigations. It eliminates the need for manual data entry and document organization. Additionally, it assists investigators in identifying suspicious patterns, potential suspects, motives, and details surrounding the commission of the crime. Legal systems are increasingly embracing the use of robots in various aspects of digital investigations (Badawi, 2022). These robots are programmed for tasks such as collecting digital forensics related to fingerprints, genetic evidence at crime scenes, and data recovery from inaccessible locations (Kerli Marlin & McMahon, 2021). They also analyze large volumes of digital data, aiding investigators in uncovering criminal links and patterns across social media, financial records, electronic data, phone conversations, and emails. Furthermore, robots equipped with sensors, cameras, and other tools can conduct surveillance, monitor individuals suspected of criminal activities, and track network traffic for security violations and unauthorized access attempts (Andrejevic, 2019; Saqr, 2021).

## Conclusion

This study highlights the widespread adoption of artificial intelligence (AI) techniques in law enforcement for addressing cybercrime, particularly in facial and vocal analysis to recognize criminal patterns. AI's role in the criminal justice system is expanding, especially in risk assessment, pretrial detention decisions, and judicial determinations based on suspect data. This process involves comprehensive data collection, followed by statistical and AI-driven analysis, risk factor identification, prioritization of high-risk suspects, and measures to maintain public order while safeguarding individual rights.AI techniques assist law enforcement agencies in various legal determinations, including arrest, release, and sentencing, by analyzing criminal histories and predicting future recidivism using machine learning. They also analyze data related to prospective defendants, aiding in recommendations for sentencing and parole. AI plays a crucial role in identifying potential criminal activities and their locations, analyzing past incidents to anticipate future patterns, analyzing visual data for suspect identification, and examining recorded audio data to detect manipulated vocal elements and predict future criminal involvement.

In addition, AI enhances criminal justice surveillance by analyzing real-time surveillance footage to identify potential criminal actions and anomalies. Future developments may enable AI to recognize subtle indicators like facial expressions and body language to deduce individuals' intentions for criminal activities. In summary, machine learning advances case data analysis, modeling, and organization, resulting in informed decisions regarding case management and recommendations for various legal issues. The study advocates that like criminal courts in both Anglo-Saxon and Latino legal systems, the courts in UAE should also prioritize the reliability and credibility of digital evidence as a condition for admissibility. Evidence obtained unlawfully or subject to misinformation or falsification should be excluded from criminal proceedings. Courts typically assess the legal basis for evidence collection and the chain of custody to ensure the evidence's validity.

The study also formulates a series of recommendations pertaining to the prospective utilization of artificial intelligence models in the domain of digital forensic inquiries. The ensuing recommendations are delineated as follows:

- Prioritize high-risk cases by leveraging diverse data sources, thereby promoting fairness and informed outcomes.
- Utilize AI to forecast crime patterns, identify potential suspects, and bolster security through advanced analysis of images, videos, and voice data. This can significantly contribute to crime prevention and the gathering of evidentiary material.
- Assess the effectiveness of AI-driven biometric identification verification techniques, such as facial recognition and voice analysis, in criminal investigations. These technologies can expedite case resolution and advance digital inquiries by enhancing identity verification.
- Incorporate AI-powered smart surveillance systems to proactively mitigate crime. Real-time analysis can be employed to identify patterns, predict potential criminal activities, and facilitate timely intervention. Emphasis should be placed on advanced visual analysis for the detection of subtle behavioral indicators.
- Enhance case management processes with machine learning capabilities. Utilize data analysis, decision optimization, and precise recommendations generated by deep neural networks to increase accuracy and operational efficiency.

## References

Abdelfattah, M. L. (2014). Genetic footprint A branch of biotechnology and its role in criminal evidence: A legal scientific study. *Journal of Ibn Youssef University, 14*(15), 107-130.

Abdo, A., & Yusof, S. M. (2023). Exploring the impacts of using the artificial intelligence voice-enabled chatbots on customers interactions in the United Arab Emirates. *IAES International Journal of Artificial Intelligence, 12*(4), 1920. http://dx.doi.org/10.11591/ijai.v12.i4.pp1920-1927

Adamson, D. (2023, Feb 27). *Understanding Text Classification In Natural Language Processing—A Beginners' Guide*. https://www.linkedin.com/pulse/understanding-text-classification-natural-language-david-adamson-mbcs

Ahmed Alaa El-Din, E. (2022). Artificial Intelligence in Forensic Science: Invasion or Revolution? *Egyptian Society of Clinical Toxicology Journal, 10*(2), 20-32. https://esctj.journals.ekb.eg/article_272046.html

Ahmed, N. H. A., & Osman, S. F. (2016). *Fingerprint Matching* (Doctoral Thesis, Nilin Khartoum University).

Ahmed, T. Z., & Rahman, M. S. (2021). Artificial Intelligence and Forensic Science: A Review. *International Journal of Computer Applications, 180*(6), 1-10.

Al-Amiriyeen, J. M. S. (2022). Artificial Intelligence in Crime Investigation: A Comparative Study. *Al-Mezan Journal of Islamic and Legal Studies, 9*(3), 449-478.

Al-Awaram, W. ( 2014). Legality of the Electronic Evidence on Criminal Search. *Journal of Jurisprudence and Law,* (20), 100.

Al-Ghafri, H. b. S. i. (2007). *Criminal Policy against Cybercrime: A Comparative Study* (Doctoral Thesis, Faculty of Law, Ain Shams University, Cairo).

Al-Ghafri, H. b. S. i. (2009). *Investigation and Collection of Evidence on Cybercrime*. Arab Renaissance House, Cairo.

Al-Hassan, A. M. (2010). *Using AI Applications in University Libraries: Designing an Expert Reference System for the University of Khartoum Library* (Doctoral Thesis, Department of Library and Information Sciences, Faculty of Arts, University of Khartoum).

Al-Radvani, M. K. A. (2014). Police Investigations into Cybercrime Challenges. *Arab Journal of Security Studies, 30*(61), 180.

AL-Salahin, S. A., & Rahman, A. (2017). *Modern criminal evidence and its depictions: a study compared to Libyan law* (Master's thesis, World City University, Kuala Lumpur).

Ali, T. F. T., & Al-Junaid, A. B. M. (2009). *Distinguishing the image of faces using synthetic neural networks* (Master's thesis, University of Omdurman).

Andrejevic, M. (2019). Automating surveillance. *Surveillance & society, 17*(1/2), 7-13. https://doi.org/10.24908/ss.v17i1/2.12930

Arshey, M., & Viji, K. A. (2021). Thwarting cyber crime and phishing attacks with machine learning: a study. In *7th International Conference on Advanced Computing and Communication Systems (ICACCS)* (Vol. 1, pp. 353-357). IEEE. https://doi.org/10.1109/ICACCS51430.2021.9441925

Azhari, A. R. M. K. (2020). *Developing a Comprehensive Framework for the Investigation of Cybercrime* (Ph.D. Thesis, Graduate School, Sudan University of Science and Technology).

Babylon, A. Y. M. Z. (2019). The Role of AI Systems in Forecasting Crime. *Journal of Police Thought, 28*(110), 59-133.

Badawi, A. T. (2022). *Legal System for Smart Robots with Artificial Intelligence Technology: UAE as a Model - A Comparative Analysis of EU Robotics Civil Code Rules 2017 and Korean Robot Ethics Charter Project*. Ennahda Scientific Publishing and Distribution House, Cairo.

Barbara, J. J. (2015). Digital Forensics and the Admissibility of Electronic Evidence. *John Marshall Journal of Computer & Information Law, 33*(3), 287-316.

Bharadwaj, A. S., & Suresh, S. (2008). Narcos Analysis & Protecting the Rights of the Accused. *Nalsar Student Law Review, 4*(12), 121-133. https://nslr.in/wp-content/uploads/2019/03/NSLR-Vol-4-No-12.pdf

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55. https://doi.org/10.5281/zenodo.22387

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., Yang, J., Toner, H., & Fong, R. (2020). Toward trustworthy AI development: mechanisms for supporting verifiable claims. *arXiv preprint arXiv:2004.07213*. https://doi.org/10.48550/arXiv.2004.07213

Casey, E. (2000). *Digital evidence and computer crime: forensic science, computers and the Internet*. Academic Press. https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-and-computer-crime-forensic-science-computers-and

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, Inc. https://dl.acm.org/doi/book/10.5555/2021194

Cicchini, M. D. (2016). Admissibility of Digital Evidence in Criminal Prosecutions. *Criminal Law Bulletin, 52*(5), 1133-1156.

Costantini, S., De Gasperis, G., & Olivieri, R. (2019). Digital forensics and investigations meet artificial intelligence. *Annals of Mathematics and Artificial Intelligence, 86*(1), 193-229. https://doi.org/10.1007/s10472-019-09632-y

Dahabreh, F. (2023). *The continued usage of artificial intelligence in the United Arab Emirates public sector organisations: An extended information system success model* (Doctoral dissertation, Northumbria University). https://nrl.northumbria.ac.uk/id/eprint/51629/

Daniel, L., & Daniel, L. (2012). *Digital forensics for legal professionals: Understanding Digital Evidence From The Warrant To The Courtroom*. Elsevier Inc. https://doi.org/10.1016/C2010-0-67122-7

Daudi, M. (2022). Forensic Medicine: Its Conception and Relevance in the Criminal Justice System. *Journal of Jurisprudence for Legal and Economic Studies, 11*(2), 404-405.

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv, 6*(1). https://doi.org/10.48550/arXiv.1502.03552

Diogenes, Y., & Ozkaya, E. (2019). *Cybersecurity–Attack and Defense Strategies*. Packt Publishing Ltd. https://www.packtpub.com/product/cybersecurity-attack-and-defense-strategies-second-edition/9781838827793

Dogra, V., Verma, S., Kavita, Chatterjee, P., Shafi, J., Choi, J., & Ijaz, M. F. (2022). A Complete Process of Text Classification System Using State-of-the-Art NLP Models. *Computational Intelligence and Neuroscience, 2022*, 1883698. https://doi.org/10.1155/2022/1883698

Dunsin, D., Ghanem, M., & Ouazzane, k. (2022). The Use of Artificial Intelligence in Digital Forensics and Incident Response (DFIR) in a Constrained Environment. *International Journal of Information and Communication Technology, 16*, 280-285. https://repository.londonmet.ac.uk/id/eprint/7708

Fowler, J. S., Volkow, N. D., Kassed, C. A., & Chang, L. (2007). Imaging the addicted human brain. *Science and Practice Perspectives, 3*(2), 4-16. https://doi.org/10.1151/spp07324

Ghassouna, M. J. S. (2019). *Comparative of Face Recognition Techniques* (Master Thesis, Faculty of Higher Studies, Mutah University).

Gless, S. (2019). AI in the Courtroom: a comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law, 51*, 195. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3602038

Gunawan Widjaja, S. J., Sree, S. R., Jasmine, A., & Lourens, M. (2023). Implementing AI Techniques for Combating Cybercrimes in Political Science and Management. *European Chemical Bulletin, 12*(8), 8807-8819. http://dx.doi.org/10.48047/ecb/2023.12.8.716

Hall, S., Sakzad, A., & Choo, K.-K. R. (2021). Explainable artificial intelligence for digital forensics. *WIREs Forensic Science, 4*. http://dx.doi.org/10.1002/wfs2.1434

Hamzawi, S. M. M. (2021). Impact of Artificial Intelligence Technologies on Reshaping Human Resources Management Functions during the Coronavirus Pandemic Crisis. *Arab Journal of Management, 41*, 145-146.

Heaton, J. (2013). *Artificial Intelligence for Humans: Fundamental Algorithms*. Heaton Research, Incorporated. https://www.heatonresearch.com/book/aifh-vol1-fundamental.html

Hess, K. M., Orthmann, C. H., & Cho, H. L. (2016). *Criminal investigation*. Cengage learning. https://www.perlego.com/book/2707195/criminal-investigation-pdf

Hey, A. J., Tansley, D. S. W., & Tolle, K. M. (2011). The fourth paradigm: Data-intensive scientific discovery [point of view]. *Proceedings of the IEEE, 99*(8), 1334-1337. https://doi.org/10.1109/JPROC.2011.2155130

Hilali, A. A. (2014). Freedom of Computer Output in Criminal Issues: A Comparative Study, 1999, p. 49. In Al-Awaram Wahiba, Legality of the Electronic Evidence on Criminal Search. *Journal of Jurisprudence and Law,* (20), 101.

Ibrahim, A. A. (2021). Applications of artificial intelligence in the face of cybercrime. *Legal Journal, 9*(8), 2809-2836.

Iqbal, F., Debbabi, M., & Fung, B. C. (2020). *Machine Learning for Authorship Attribution and Cyber Forensics*. Springer. https://doi.org/10.1007/978-3-030-61675-5

Jaballah, A. M. A. (2022). Means of Protecting Cybersecurity: A rooted Jurisprudence Compared to Contemporary Systems. *Journal of the Faculty of Shari 'a and Law in Assiut, 34*(3), 2230-2296.

Jones, R. (2018). Advances in Digital Forensics. *Journal of Digital Investigations, 3*(2), 45-54.

Kamil, M. F. A. H. (2002). Controls and Limits on the Legitimacy of Modern Means in Criminal Investigation. *Journal of Police Thought, 11*(3), 196- 240.

Kerli Marlin, E. A., & McMahon, M. (2021). Expression Factor: Humanizing the Emerging Digital Discourse Law. *Journal of the Dubai Judicial Institute, 13*(9), 61.

Khalifa, A. M. (2008). Truth Serum and Lie Detector. *National Criminal Journal, 51*(1), 15-30.

Khalifa, S., & Mehira, N. (2021). Lie Detector and Extent Lawfulness in Criminal Evidence. *Journal of Jurisprudence, 13*(9), 9-21.

Leskovec, J., Rajaraman, A., & Ullman, J. D. (2020). *Mining of massive data sets*. Cambridge university press. https://doi.org/10.1017/CBO9781139924801

Lin, J., & Dyer, C. (2010). *Data-Intensive Text Processing with MapReduce*. Springer Nature. https://doi.org/10.1007/978-3-031-02136-7

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution that Will Transform how We Live, Work, and Think*. Houghton Mifflin Harcourt.

Melby, A. B. N. (2021). Adaptation of Metadata as Supporting Evidence in Digital Criminal Investigation Processes: Proposed Model. *Arab Journal of Criminal Evidences and Forensic Sciences, 3*(2), 3060-3077.

Mijwil, M., Mohammad, A., & ChatGpt. (2023). Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime. *Iraqi Journal For Computer Science and Mathematics, 4*(1), 65-70. https://doi.org/10.52866/ijcsm.2023.01.01.0019

Mohammed, B. M. M. (2023, March 15). *Interpretable Artificial Intelligence, AI Platform in Arabic*. Artificial intelligence in the Arabic language. https://aiinarabic.com/explainable-artificial-intelligence/#1604

Mohammed, M. I., & Ameerah, A. A. H. (2022). Automated Reading of Arabic Lines: Applied Study in Artificial Intelligence Technologies. *Arabic International Journal of Library and Information Studies, 1*(4), 133-180.

Mohsin, K. (2020). Regulation of AI and AI Crimes. *Available at SSRN 3552140*. https://dx.doi.org/10.2139/ssrn.3552140

Ohlhorst, F. J. (2012). *Big data analytics: turning big data into big money* (Vol. 65). John Wiley & Sons. https://www.wiley.com/en-gb/-p-9781118239049

Rigano, C. (2019, October 8). *Using artificial intelligence to address criminal justice needs*. National Institute of Justice. https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

Rosario, D., Romano, J., & Borel-Donohue, C. (2011). *Spectral and Polarimetric Imagery Collection Experiment*. Army Research Lab Technical Report ARMET-TR-11027. https://apps.dtic.mil/sti/citations/ADA608586

Sadiku, M. N., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cybersecurity. *International Journal of Engineering Research and Advanced Technology, 6*(5), 1-7. https://doi.org/10.31695/IJERAT.2020.3612

Saqr, W. M. A. a.-M. (2021). Criminal Responsibility for AI Crimes. *Law Spirit Magazine,* (96), 59.

Schmidt, M. J. (2016). Admissibility of Digital Evidence in Civil Litigation. *South Dakota Law Review, 61*(2), 225-251.

Scroggins, A. T. (2019). The Admissibility of Digital Evidence in Criminal Prosecutions. *American Criminal Law Review, 56*(1), 27-70.

Silva, K. B. N. D., Dharmasiri, K. S., Buddhadasa, M. P. A. A., & Ranaweera, K. G. N. U. (2021). Criminal Investigation: A Brief Review of Importance of Biological Evidence. *European Scholar Journal, 2*(8), 8-12. https://scholarzest.com/index.php/esj/article/view/1125

Smith, J. (2020). *Digital Forensics: Principles and Practices*. New York: Routledge.

Tahfah, F. A. M. (2020). Limits to the Exclusion of Evidence of Criminal and Practical Artificial Intelligence Techniques Obtained by Illicit Means: A Comparative Study between Anglo-Saxon and Latino Systems. *Law Spirit Journal,* (91), 683.

Talbani, S. I., & Fadi, H. S. (2014). Use of Synthetic Neural Networks to Predict Crime Rates in the Gaza. *Hakma Journal, 22*, 298-323.

Taqiya, B., & Al-Wasifi, S. I. (2012). Prediction Using the Combination of Synthetic Neural Networks and Box and Jenkins Models: Applied Study. *Egyptian Journal of Business Studies, 36*(2), 527-548.

Taylor, D. (2023, October 28). *What is Big Data? Introduction, Types, Characteristics, Examples*. Guru99. https://www.guru99.com/what-is-big-data.html

Vamathevan, J., Clark, D., Czodrowski, P., Dunham, I., Ferran, E., Lee, G., Li, B., Madabhushi, A., Shah, P., & Spitzer, M. (2019). Applications of machine learning in drug discovery and development. *Nature reviews Drug discovery, 18*(6), 463-477. https://doi.org/10.1038/s41573-019-0024-5.

Verma, A., & Ramanathan, K. (2022). Data Privacy Preservation in Digital Forensics Investigation. *American Institute of Physics Conference Series, 2519*(1), 030051. https://doi.org/10.1063/5.0109813

Verma, S., & Gupta, N. (2020). Application of Artificial Intelligence in Cybersecurity. In H. S. Saini, R. Sayal, R. Buyya, & G. Aliseri (Eds.), *Innovations in Computer Science and Engineering: Proceedings of 7th ICICSE* (pp. 65-72). Springer Singapore. https://doi.org/10.1007/978-981-15-2043-3_9

Wairimu, B. (2023, Feb 26). *The Rise of Cybersecurity Threats and How to Protect Your Business*. LinkedIn. https://www.linkedin.com/pulse/rise-cybersecurity-threats-how-protect-your-business-brenda-wairimu

Wexler, C. (2018). Crime Has Been Changing, and Police Agencies Need to Catch Up. In *The Changing Nature of Crime And Criminal Investigations* (pp. 4-8). Police Executive Research Forum. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf