Submitted to the edited volume
'Handbook on the Sociology of Artificial Intelligence'
to be published by Emerald

Forensic Science and Sociology in the Era of AI

Rahulrajan Karthikeyan and Moses Boudourides

ABSTRACT

The integration of artificial intelligence (AI) into forensics, beyond its traditional use in law enforcement, is transforming how social phenomena are analyzed and understood. AI—encompassing big data, machine learning, and computational techniques—has become a powerful tool in forensic analysis across several areas (Lawless, 2022): (i) uncovering patterns in human behavior and mapping social relationships within communities or organizations; (ii) adapting techniques from physical crime scene analysis to study social dynamics and collective behaviors; (iii) applying forensic analysis to digital data to investigate online activities, social media interactions, and cybercrime; and (iv) employing facial recognition and other biometric technologies to study group behavior and demographics.

Moreover, the intersection of forensic social science and AI extends into emerging technological areas (Roy et al.,2024): (i) integrating wearable technologies, such as smartwatches and fitness trackers, to gather real-time social data; (ii) using Natural Language Processing (NLP) to analyze conversations on social media and other online interactions; and (iii) utilizing Geographic Information Systems (GIS) to collect and analyze geographic data, studying spatial relationships in social contexts.

At the same time, the advancement of AI has dramatically expanded the scope of social science research, allowing for the analysis of vast, multidimensional datasets that provide a deeper understanding of social behavior. Historically, sociology was largely driven by hypothesis testing and statistical modeling, which often required researchers to focus on specific variables. In contrast, AI enables a more inductive approach, where big data can be explored without preconceived notions, allowing for the discovery of new patterns and the generation of theories from the digital traces of human activity (McFarland et al., 2015) (Goldberg, 2015). This evolution in forensic social science paves the way for a more evidence-based approach to studying society, which could significantly reshape sociological theory and practice (Goldberg, 2015).

However, the use of AI, particularly in high-stakes areas like criminal forensics, raises significant ethical and legal concerns, especially when relying on black-box AI systems that obscure their decision-making processes. In particular, the convergence of AI, sociology, and forensics has also sparked concerns about the potential risks of colonization of engineering and computer science over social science. While interdisciplinary collaboration can foster innovation, the situation becomes problematic when engineering frameworks might overshadow sociological perspectives, reducing complex social behaviors to mere data points. To counter this, scholars argue for a balanced approach—termed **forensic social science**—which integrates AI's computational power with the theoretical depth of sociology (McFarland et al., 2015) (Goldberg, 2015).

In criminal forensics, AI is increasingly being used to analyze complex evidence, such as DNA mixtures, facial recognition, and recidivism risk assessments. However, many of these AI systems operate as black boxes, meaning their internal workings are opaque and not fully understandable by humans. This lack of

transparency poses a problem, as it prevents legal professionals—including judges and lawyers—from fully assessing the reliability of AI-generated forensic evidence. Furthermore, black-box AI can amplify biases and inaccuracies, leading to unfair outcomes in the criminal justice system. Recent research challenges the assumption that black-box AI is inherently more accurate than interpretable models and advocates for "glass-box" AI systems that are transparent and understandable (Garrett et al.,2023).

1. INTRODUCTION

The convergence of artificial intelligence (AI), forensic science and sociology marks a pivotal moment in the evolution of both scientific investigation and social research. Traditionally, forensic science has operated within the bounds of criminal justice, focused on uncovering physical evidence to support legal outcomes (Lawless, 2022, p.20 and p.43). Similarly, sociology has been grounded in hypothesis-driven models, seeking to explain social behavior through structured, often statistical, methodologies. However, the rapid advancement of AI has encompassed machine learning, big data analytics and computational modeling which has begun to redefine the landscape of both disciplines by introducing powerful new tools for analyzing not only physical evidence but also complex social patterns.

This shift is giving rise to a new paradigm: Forensic Social Science, which applies AI-driven forensic methodologies to the study of human behavior, social networks, and digital traces. In this model, forensic science extends beyond its conventional scope to include the analysis of online activity, social media interactions, and collective behavior in both physical and digital spaces (Goldberg, 2015). Simultaneously, sociology benefits from AI's capacity to process vast, unstructured datasets, enabling more nuanced and inductive insights into societal dynamics (McFarland et al., 2015). This interdisciplinary approach not only deepens our understanding of crime, justice, and behavior but also challenges traditional boundaries between the physical and social sciences.

Emerging technologies such as Natural Language Processing (NLP), Geographic Information Systems (GIS) and biometric analysis have found applications across this hybrid space (Lawless, 2022, p.106). They allow for real-time monitoring of public sentiment, mapping of social influence networks, and the forensic analysis of digital environments. The integration of these tools into sociological inquiry enables scholars to reconstruct social phenomena from digital footprints which is mirroring the way forensic experts analyze crime scenes through physical traces. This has prompted scholars to call for a reimagining of both forensic and sociological practices, emphasizing collaboration, transparency and ethical accountability (McFarland et al., 2015) (Goldberg, 2015).

Yet, this integration is not without risks. The growing reliance on AI in high-stakes forensic contexts has raised concerns about the opacity of "black-box" algorithms, which often lack interpretability and accountability (Goldberg, 2015). When applied to social data, these systems risk reducing complex human experiences to simplistic data points, thereby marginalizing context and nuance. Moreover, as AI-driven techniques often originate in engineering and computer science which permeate social science research, questions arise about the colonization of sociological thought by technocratic frameworks (Nayerifard et al., 2023, pp.3-4) (McFarland et al., 2015). These concerns underscore the need for a balanced approach, one that leverages computational power without compromising the theoretical and ethical foundations of sociology.

Thus exploring the multidimensional relationship between AI, forensic science and sociology. It examines how AI is transforming digital and physical forensics, reshaping sociological inquiry, and giving rise to new interdisciplinary practices. By grounding this exploration in both historical context and emerging research, the paper aims to illuminate the opportunities and challenges that define Forensic Social Science in the era of AI (Nayerifard et al., 2023, p.3). Ultimately, it advocates for an ethically grounded, interpretability-focused and interdisciplinary framework that ensures technological advancement serves justice and deepens our understanding of society.

2. BASICS OF FORENSICS

Forensic science, in a broad sense, is the application of science to both criminal and civil laws that are enforced by police agencies within a criminal justice system (Saferstein et al., 2021, p.3). As modern society has grown increasingly complex, so too has its dependence on a robust legal system to govern personal, corporate, and governmental actions. This evolution has deepened the integration of scientific technology into the enforcement and regulation of laws. From monitoring environmental regulations and food safety to investigating violent crimes and digital fraud, forensic science plays an essential role in ensuring justice and accountability.

At its most fundamental level, forensic science is mainly about applying the principles and methods of the physical and natural sciences to the analysis of crime-scene evidence (Saferstein et al., 2021, p.4). While science cannot resolve all the psychological and sociological causes behind criminal behavior, it does offer objective, reliable, and reproducible methods for uncovering factual details from the remnants of a crime. This objectivity has made forensic scientists vital participants in the criminal justice process (Saferstein et al., 2021, pp.4-5).

The term “forensic science” encompasses a wide array of scientific disciplines and professions. The American Academy of Forensic Sciences, for instance, recognizes 11 primary sections within forensic science: Criminalistics, Digital and Multimedia Sciences, Engineering Science, General, Jurisprudence, Odontology, Pathology/Biology, Physical Anthropology, Psychiatry/Behavioral Science, Questioned Documents, and Toxicology (Saferstein et al., 2021, pp.3-4). However, even this extensive list is not exhaustive. Professions such as fingerprint analysis, toolmark identification, and forensic photography also fall within the broad umbrella of forensic science.

(i) Historical Foundations and Pioneers

Forensic science owes its development to several foundational figures. Mathieu Orfila (1787–1853), known as the father of forensic toxicology, published the first scientific treatise on detecting poisons and their effects on animals (Saferstein et al., 2021, p.5). Alphonse Bertillon (1853–1914) introduced anthropometry, a system of bodily measurements for identifying individuals, which was a forerunner to

modern fingerprinting. Francis Galton (1822–1911) conducted the first definitive study of fingerprints and developed a classification method that underpins today's systems (Saferstein et al., 2021, pp.5-7).

Leone Lattes (1887–1954) devised a method for determining blood groups from dried bloodstains, applying it to criminal investigations. Calvin Goddard (1891–1955) pioneered the use of the comparison microscope for firearm identification. Albert S. Osborn (1858–1946) laid the foundation for forensic document examination, while Hans Gross (1847–1915) promoted the integration of scientific principles into criminal investigation. Edmond Locard (1877–1966), often called the father of modern forensic science, established the first police crime lab and articulated the exchange principle: whenever two objects come into contact, there is a transfer of material (Saferstein et al., 2021, p.7).

(ii) Locard's Exchange Principle

Locard formulated what is now a cornerstone of forensic science. This principle posits that whenever two objects come into contact, there is always an exchange of materials. In the context of criminal investigations, this means that a perpetrator will both bring something into the crime scene and leave with something from it (Saferstein et al., 2021, pp.7-8). This trace evidence, no matter how minute it is, like fibers, hair, skin cells, soil, or other materials which can be critical in linking a suspect to a crime. Locard's principle emphasizes the meticulous collection and analysis of evidence, as even the smallest trace can yield significant investigative breakthroughs. It forms the scientific basis for the recovery and interpretation of physical evidence, guiding both crime scene investigators and forensic analysts in their work (Saferstein et al., 2021, p.8 and p.24).

(iii) Development and Structure of Crime Laboratories

The establishment and expansion of crime laboratories represent one of the most significant milestones in the institutionalization of forensic science. The origins of formal crime labs in the United States date back to 1923, when August Vollmer, a progressive police chief in Los Angeles, initiated the country's first forensic laboratory (Saferstein et al., 2021, p.8). This lab marked a pioneering effort to systematically apply scientific principles to criminal investigations at the municipal level. Less than a decade later, the Federal Bureau of Investigation (FBI), under the leadership of J. Edgar Hoover, launched a national forensic laboratory in 1932. Over the decades, this facility has evolved into the largest and most comprehensive forensic science institution in the world, thus handling over a million examinations annually and offering services to law enforcement agencies across the country.

The rapid development of forensic laboratories was largely influenced by two major forces: the rising crime rates in the mid-20th century and the judicial reforms of the 1960s (Saferstein et al., 2021, pp.8-11). Landmark Supreme Court decisions during this period emphasized defendants' rights and placed greater evidentiary burdens on prosecutors. As a result, law enforcement agencies could no longer rely solely on confessions or eyewitness accounts and began to prioritize scientifically evaluated evidence, thereby increasing demand for forensic lab services. Furthermore, the explosion of drug-related

offenses since the 1960s necessitated the chemical analysis of seized substances, further contributing to the expansion of forensic services.

The structure of crime laboratories varies significantly depending on jurisdiction and geographic region. In the United States, labs operate at the federal, state, and local levels. At the federal level, several major agencies run specialized labs such as FBI, DEA, ATF, U.S. Postal Inspection Service (Saferstein et al., 2021, p.8 and p.10).

At the state level, several states such as California, Florida, and Virginia have developed model systems that include regional and satellite laboratories managed under a centralized state department. This structure allows for specialization, uniformity, and sharing of resources while ensuring timely access to forensic services across widespread jurisdictions (Saferstein et al., 2021, pp.7-9). In contrast, local laboratories that are typically affiliated with city police departments or county sheriff's offices who serve urban centers with higher crime rates and more localized casework needs.

Internationally, the organization of forensic laboratories differs based on government structure and law enforcement models. In the United Kingdom, the former Forensic Science Service (FSS) operated as a centralized, government-run entity providing nationwide forensic services until it was dissolved in 2012 due to budgetary concerns. The privatization that followed led to the rise of third-party laboratories contracted by police departments (Saferstein et al., 2021, p.9). In Canada, forensic science services are distributed among three main publicly funded centers: the Royal Canadian Mounted Police (RCMP) regional labs, the Centre of Forensic Sciences in Toronto, and the Laboratoire de sciences judiciaires et de médecine légale in Montreal.

(iv) Core Units of a Full-Service Crime Laboratory

A fully equipped crime laboratory is divided into several core units, each tasked with analyzing specific categories of evidence. The Physical Science Unit applies chemistry, physics, and geology to identify and compare materials such as drugs, glass, explosives, and soil using tools like spectroscopy and chromatography (Saferstein et al., 2021, pp.12-13). The Biology Unit, staffed with biologists and biochemists, handles DNA profiling, bodily fluids, hair, fibers, and even botanical evidence. The Firearms Unit examines weapons, bullets, cartridge cases, and gunpowder residues, often using comparison microscopes to match bullets to specific firearms. Meanwhile, the Document Examination Unit focuses on handwriting, ink, and paper authenticity in legal documents, and the Photography Unit employs various imaging techniques—digital, infrared, ultraviolet, and X-ray—for both documentation and courtroom presentations.

In addition to these core units, many laboratories operate specialized divisions to support broader forensic investigations. The Toxicology Unit tests biological samples for drugs, alcohol, and poisons, often collaborating with medical examiners. The Latent Fingerprint Unit recovers hidden fingerprints using powders, chemicals, and light sources, comparing them against national databases like IAFIS. Some labs also maintain a Polygraph Unit to assist in interviews, and a Voiceprint Analysis Unit, which

uses spectrographic techniques to link suspects to recorded audio. Another critical component is the Crime Scene Investigation (CSI) Unit, a mobile team that collects, packages, and preserves physical evidence at the crime scene while documenting it through photography and reconstruction methods (Saferstein et al., 2021, pp.12-13).

The structure and capabilities of crime laboratories continue to evolve in response to advancing technologies, judicial demands, and shifting criminal patterns. Modern labs must adapt to new types of evidence, such as encrypted digital data and biometric identifiers, all while upholding the rigorous scientific and legal standards required for admissibility in court (Saferstein et al., 2021, pp.10-13). Flexibility, specialization, and ongoing training remain essential for forensic labs to deliver timely and reliable investigative support in an increasingly complex legal landscape.

(v) The Role of the Forensic Scientist and Future Directions

Forensic scientists perform two primary functions: analyzing physical evidence and providing expert testimony in court. Their work is grounded in the scientific method which is a process of formulating hypotheses, conducting experiments, and validating findings through reproducible results. Unlike confessions or eyewitness testimony, which are susceptible to bias and error, physical evidence offers a more reliable foundation for legal conclusions.

The admissibility of scientific evidence in court has been shaped by landmark cases such as Frye v. United States (1923) and Daubert v. Merrell Dow Pharmaceuticals (1993). While Frye emphasized general acceptance within the scientific community, Daubert introduced criteria including peer review, error rates, and standards of methodology, giving judges greater responsibility as “gatekeepers” (Saferstein et al., 2021, pp.17-18 and p.25).

In the courtroom, forensic scientists serve as expert witnesses, explaining their findings to judges and juries in a clear, unbiased manner. Their credibility depends not only on academic credentials and professional experience but also on their ability to communicate scientific concepts effectively.

The value of a crime lab is diminished if law enforcement personnel are not trained to properly recognize, collect, and preserve evidence (Saferstein et al., 2021, pp.17-23). Many agencies now maintain specially trained evidence technicians who work closely with forensic scientists. These technicians receive ongoing training and operate with the proper tools and protocols to ensure the integrity of evidence.

Forensic science continues to evolve with advancements in technology and analytical methods. DNA profiling has transformed criminal investigations, while digital forensics is increasingly important in cybercrime cases. However, challenges remain, including backlog of case samples, standardization of methods, and the ongoing need for training and ethical oversight (Saferstein et al., 2021, pp.18-19).

Popular media, particularly shows like CSI: Crime Scene Investigation, have both increased public interest in forensics and distorted expectations through the effect called “CSI effect” (Saferstein et al.,

2021, p.4). These portrayals often oversimplify or exaggerate the speed and certainty of forensic analyses, creating misconceptions among jurors and the general public.

Ultimately, forensic science serves a critical function in modern society, bridging the gap between science and law to uncover truth and deliver justice (Saferstein et al., 2021, pp.3-4). Its continued advancement depends on rigorous research, ethical practice, interdisciplinary collaboration, and robust public understanding.

3. DIGITAL FORENSICS (DF)

Digital forensics has evolved into a cornerstone of modern forensic science, reflecting the rapid technological advancements and the growing pervasiveness of digital technologies and devices in everyday life. What began as an isolated effort to combat basic computer crimes has grown into a sophisticated domain capable of addressing a wide range of criminal activities. From fraud and cyberattacks to the analysis of social phenomena and societal trends, digital forensics now plays a dual role as both a technological and a sociological tool in contemporary investigations (Lawless, 2022, pp.125-127)(Jones & Winster, 2022).

(i) Historical Context and Evolution of Digital Forensics

The roots of digital forensics are deeply intertwined with the evolution of computing itself (Whitcomb, 2002). In its early years, it was an ad hoc practice carried out by individuals with limited resources and no standardized procedures. A notable example is Clifford Stoll's investigation in the 1980s, documented in The Cuckoo's Egg, which exemplifies the ingenuity required to track digital crimes before formal methodologies existed. While working as a systems administrator at Lawrence Berkeley National Laboratory, Stoll identified a minor accounting discrepancy of just $0.75. Initially dismissed as a simple error, this anomaly ultimately led him to uncover a sophisticated cyber intrusion. A hacker using the alias "Hunter" was exploiting the system to infiltrate U.S. military and government networks, stealing sensitive information for the Soviet KGB (Stoll, 1989). This case foreshadowed the breadth of digital forensics, highlighting its potential for analyzing digital data even before it was formally recognized as a vital investigative tool (Casey, 2011, p.3).

The rise of home computing in the 1980s and the advent of the Internet in the 1990s significantly broadened the field of digital forensics (Pollitt, 2010). Initially, investigations focused on relatively simple computer-related offenses such as hacking and minor fraud. However, as digital crime became more complex, U.S. law enforcement agencies began collaborating to enhance their expertise and develop specialized training programs to address these emerging challenges (Casey, 2011, pp.10-11).

Subsequently, as digital networks grew, so did the sophistication of crimes including illegal pornography, exploitation and large-scale financial fraud (Bossler et al., 2015, p.254 and pp.256-257). During the so-called "Golden Age" of digital forensics, which ranged between 1999 to 2007, the investigators benefited from the ubiquity of standardized operating systems like Microsoft Windows and widely recognized file formats, which simplified evidence extraction and analysis (Garfinkel, 2010, p.66).

The subsequent rapid proliferation of mobile devices and the emergence of the Internet of Things (IoT) introduced new challenges, as smartphones, tablets, smartwatches, and even gaming consoles became repositories of personal data, often safeguarded by encryption and proprietary software (Fakiha, 2024, p.79 and p.82). These developments created significant challenges for digital forensics practitioners, who struggled to retrieve and interpret data from increasingly diverse and secure platforms (Caviglione et al., 2017, p.12). The need for specialized tools, such as codecs to decode proprietary file formats, became a critical issue, with investigators often unable to proceed due to a lack of compatible technologies (Lawless, 2022, p.127). This limitation was compounded by the rapid pace of innovation, which constantly outpaced the development of forensic tools.

Furthermore, as digital forensics matured, it became increasingly integrated with the rapid growth of information and communication technology (ICT) (Noblett et al., 2000). Modern society's reliance on communication networks, mobile devices, cloud computing, and the Internet of Things has transformed forensic investigations, both in scope and complexity (Caviglione et al., 2017, pp.14-15). The integration of cyber physical systems (CPS) into industries, businesses, and government services has further emphasized the necessity of digital forensics in maintaining security, mitigating cybercrimes and providing courtroom admissible evidence (Kaushik et al., 2022).

This transformation has also led to the proliferation of new cyber threats and forensic challenges, including identity theft, cyberbullying, data leakage via social engineering, malware-infected IoT devices and distributed denial-of-service (DDoS) attacks through botnets (Janarthanan et al., 2021, p.229). Such crimes not only affect individuals but also cause significant socioeconomic disruptions for enterprises and governmental institutions. As a result, law enforcement agencies (LEAs) and forensic experts must continuously adapt their investigative methods to keep up with these evolving threats (Caviglione et al., 2017, p.12).

A major issue complicating digital forensics investigations is the cross-border nature of cybercrimes, which often require cooperation between jurisdictions with vastly different legal frameworks (Alenezi, 2023). The process of tracking an attacker across international networks is highly complex and legal limitations regarding digital evidence access can create significant roadblocks. Investigators must navigate these legal constraints while ensuring that forensic methodologies comply with ethical and procedural standards to maintain the integrity of evidence in court (Caviglione et al., 2017, pp.12-13).

Traditional forensic techniques involve preserving and analyzing digital evidence from storage media, such as hard drives and USB devices. Investigators typically create forensic images with exact digital copies of a device’s storage which is to ensure that evidence remains unaltered. However, with the explosion in data volume and diversity, forensic experts now face increasing difficulties in efficiently extracting and analyzing massive amounts of stored information (Caviglione et al., 2017, pp.14-15).

Moreover, the growing use of file system encryption and self-destructing digital records has complicated evidence collection. Many modern operating systems, including Linux, macOS and Android now feature default encryption, making data extraction nearly impossible without decryption keys. In addition, solid-state drives (SSDs) with built-in encryption and cloud-based storage platforms introduce new barriers, requiring forensic investigators to develop innovative methods to access and recover digital evidence

before it is permanently erased. (Chaurasia et al., 2017, p.14)

Another critical area of digital forensics is network forensics, which focuses on capturing and analyzing digital communications and data flows. Investigators rely on network logs, packet captures and intrusion detection system alerts to trace attackers and reconstruct cyber incidents. However, modern network infrastructures generate immense amounts of traffic, making it impractical to store and analyze every packet. Additionally, the widespread adoption of encryption protocols has significantly reduced visibility into network traffic, complicating forensic analysis.

Despite these advancements, attackers have developed anti-forensic techniques such as onion routing (Tor), traffic padding and deep packet obfuscation, to evade detection, making real-time network forensic investigations increasingly difficult. (Rodrigues et al., 2017, p.4 and p.6).

Reverse engineering plays a key role in malware analysis and forensic investigations of sophisticated cyber threats. By deconstructing malicious software, forensic analysts can determine its functionality, identify its origin, and trace its command-and-control structure. However, modern malware often incorporates anti-forensic measures, such as polymorphic code, encryption, and multi-stage execution, which make it increasingly resistant to forensic analysis (Caviglione et al., 2017, p.13).

Additionally, cybercriminals have begun using steganography, cryptographic obfuscation, and remote file-wiping techniques to remove forensic traces from compromised systems. These anti-forensic strategies pose significant hurdles, requiring forensic teams to develop novel de-obfuscation methods, real-time forensic logging, and memory forensics techniques to retrieve crucial evidence before it is lost (Caviglione et al., 2017, pp.14-15).

The continuous advancement of cloud computing, IoT, and decentralized digital infrastructures further complicates forensic investigations. The adoption of crime-as-a-service (CaaS) models has allowed even non-technical individuals to execute sophisticated cyberattacks using pre-configured malware kits, botnet services, and anonymized payment systems. For example, ransomware-as-a-service (RaaS) platforms now enable criminals to deploy mass ransomware campaigns with minimal effort, creating new forensic challenges (Keijzer, N., 2020, pp.11-12).

To counter these threats, forensic experts advocate for the development of international forensic standards, privacy-preserving investigation techniques and cross jurisdictional cooperation frameworks. However, establishing a globally recognized forensic methodology remains a challenge due to legal, ethical and privacy related concerns. Future forensic investigations will require a balance between technological innovation, ethical considerations, and legislative frameworks to ensure that forensic science remains both effective and legally compliant. (Caviglione et al., 2017, pp.14-15).

(ii) AI role in Digital Forensics

Artificial intelligence (AI) has transformed the practice of digital forensics, addressing many of the challenges associated with the growing volume and complexity of digital evidence. AI's ability to process and analyze vast datasets has revolutionized the way investigators approach digital evidence by allowing them to identify patterns, extract key information and reconstruct events more effectively (Ribaux et al., 2020, p.38). For example, AI-powered natural language processing (NLP) is widely used to analyze communication logs, emails and social media posts, providing insights into the digital footprints of suspects and victims. This has proven particularly valuable in cases involving organized crime or terrorism, where uncovering networks of relationships is critical.

Machine learning algorithms have also automated repetitive tasks in digital forensics such as sorting through millions of files to identify those most relevant to an investigation (Nayerifard et al., 2023 pp.31). Predictive analytics is another application of AI that is being explored to anticipate criminal behavior based on digital activity patterns, although these approaches remain controversial due to ethical and legal concerns (Bossler et al., 2015, pp.622-625). One of the most promising developments is the use of AI for video analysis in cases involving CCTV footage, enabling investigators to track individuals or objects across multiple cameras and even predict movements based on behavior patterns.

Despite these advancements, the reliance on AI raises questions about transparency and bias. Many AI models operate as "black boxes" meaning their decision-making processes are not easily interpretable by humans. This lack of transparency can lead to issues of trust particularly in high-stakes criminal cases. Scholars advocate for the adoption of "glass-box" AI systems that prioritize interpretability and ensure that forensic evidence can be effectively scrutinized by legal professionals (Ribaux et al., 2020, pp.45-46).

(iii) Challenges in Digital Forensics

While AI has mitigated some challenges while others persist. One of the most pressing issues is the sheer diversity of devices and data formats encountered in modern investigations. The proliferation of IOT devices has led to an explosion in the variety of file formats, many of which require specific codecs for decoding. The absence of a suitable codec can stall an investigation entirely as highlighted by practitioners in the mid-2010s (Lawless, 2022, pg.127). For example, the inability to decode a proprietary file format on a smart home device could prevent investigators from accessing critical evidence in a burglary or domestic violence case.

Another significant challenge is the integration of digital evidence into broader investigative frameworks. Digital evidence often represents just one component of a case, requiring careful synthesis with other forms of forensic evidence, such as DNA or fingerprints. This integration is further complicated by the volume of data involved, which can overwhelm investigators and impede timely analysis (Ribaux et al., 2020, p.40 and p.47).

Ethical considerations also loom large in digital forensics. The involvement of law enforcement agencies in both evidence collection and analysis raises questions about impartiality and potential conflicts of interest. Critics argue that digital forensics practitioners should operate independently to avoid biases that might influence the interpretation of evidence. Standardized protocols and professional certification programs are essential to address these concerns and ensure the reliability and integrity of digital forensics practices.

Digital forensics represents a critical intersection of technology, society and the law. Its evolution from an ad hoc practice to a highly specialized discipline reflects the growing importance of digital evidence in contemporary investigations. AI has been a transformative force, enabling practitioners to tackle the challenges posed by the diversity and complexity of digital devices.

However, as digital forensics continues to evolve it must navigate significant ethical, professional and technological hurdles. Balancing innovation with accountability and transparency will be essential to ensuring that digital forensics remains a trusted and effective tool in the pursuit of justice (Lawless, 2022, p.105) (Garfinkel, 2010, pp.64-65).

4. EMERGING TECHNOLOGIES IN FORENSICS

The integration of cutting-edge technologies into forensic science has fundamentally transformed the field, providing essential tools to address increasingly complex challenges and enhancing the accuracy, efficiency, and scope of investigations. As noted by (Kloosterman et al., 2015), "[T]his technological revolution in forensic science could lead to a paradigm shift in which a new role of the forensic expert will emerge as developer of evidence analyzers and custodian of integrated forensic platforms." This paradigm shift highlights the growing need for forensic experts not only to analyze evidence but also to manage and innovate the technological tools that underpin forensic investigations.

Among the most significant advancements of AI in forensic science are those that have enabled the use of advanced **Machine Learning (ML)** and **Deep Learning (DL)** techniques to analyze and interpret large, complex, and diverse datasets across various forensic domains. Notable AI techniques include:

Sentiment Analysis: AI-driven sentiment analysis models, such as those based on recurrent neural networks (RNNs) or transformer architectures like BERT, have been used to track public opinion shifts during elections, pandemics, or social protests. These models analyze textual data from social media or news articles to determine the emotional tone and shifts in public sentiment (Liu, 2020) (Vaswani et al., 2017).
Natural Language Processing (NLP): NLP techniques, including topic modeling and semantic analysis, have been applied to explore cultural narratives across digital platforms. For instance, Latent Dirichlet Allocation (LDA) has been used to uncover hidden themes in large-scale corpora, while transformer models enable deeper semantic understanding (Blei, Ng, & Jordan, 2003) (Devlin et al., 2019).
Predictive Modeling: Machine learning algorithms, such as decision trees, random forests, and gradient boosting machines, have been employed to forecast systemic vulnerabilities, such as income inequality or health disparities. Predictive models trained on socioeconomic and demographic data provide actionable insights into potential risks (Breiman, 2001) (Chen & Guestrin, 2016).
Graph Neural Networks (GNNs): GNNs are instrumental in mapping and analyzing large-scale social networks. These networks help identify influence structures, hidden relationships, or power dynamics in sociological contexts (Hamilton, Ying, & Leskovec, 2017).

Image and Video Recognition: Advances in convolutional neural networks (CNNs) and deep learning have enabled the analysis of visual media, such as memes, videos, or infographics, to understand their role in shaping public discourse and online activism (Krizhevsky, Sutskever, & Hinton, 2012).
Unsupervised Learning Methods: Clustering techniques, such as k-means and hierarchical clustering, and dimensionality reduction methods, like principal component analysis (PCA) or t-SNE, are employed to identify latent structures in datasets, such as demographic groupings or thematic trends in public sentiment (van der Maaten & Hinton, 2008).

By automating and enhancing data analysis, emerging technologies such as Machine Learning (ML) and Deep Learning (DL) have empowered forensic scientists to process and interpret evidence on an unprecedented scale and speed. In digital forensics, for example, ML and DL algorithms are employed in tasks such as malware analysis, image and video forensics, network, IoT, and cyber forensics, as well as mobile, file system, and memory forensics, to identify patterns within vast volumes of digital evidence (Qadir & Noor, 2021). These computational advancements play a critical role in cybercrime investigations and the analysis of multimedia data. Investigating the impact of these innovations is essential for understanding how they can address the increasing volume of digital evidence, enabling forensic professionals to stay ahead of evolving criminal tactics and technological changes. As AI technologies, including ML and DL, continue to evolve, their applications in forensic science expand rapidly—from enhancing the analysis of camera images and DNA samples to enabling pattern recognition and the reconstruction of crime scenes (Dudek et al., 2023).

As machine learning (ML) techniques continue to evolve and expand across various domains, such as image processing, text analysis, voice recognition, and optical and character recognition, their applications in digital forensics have also grown (Mitchell, 2014). In particular, such techniques are increasingly leveraged to extract valuable insights from vast amounts of digital evidence. By applying conceptual models for data mining and knowledge discovery, ML methods assist investigators in efficiently analyzing large datasets, thereby enhancing their ability to uncover critical information (Quick and Choo, 2014) (Qadir and Varol, 2020).

For instance, supervised ML methods are widely used in live digital forensics to analyze real-time data from the Internet of Things (IoT) environments (Kebande et al., 2015). These environments, characterized by billions of interconnected sensors, generate diverse data types that pose significant challenges for investigators. ML -driven frameworks for emergent configurations in IoT forensics provide robust solutions, enabling the rapid detection of anomalies and classification of intrusion events.

Deep learning models, particularly convolutional neural networks (CNNs) have demonstrated exceptional performance in areas such as adversarial image forensics, tamper detection and computer forensics (Bernacki et al., 2020). DL techniques are capable of handling the vast and divergent datasets often encountered in forensic investigations, offering high accuracy in applications like network traffic analysis and cyber intrusion detection (Koroniotis et al., 2019). These models are also instrumental in video forensics, where they enhance the detection of tampered or explicit content, thereby streamlining the investigation process.

In image manipulation detection, DL methods have been shown to effectively identify subtle alterations in visual data, even in the face of adversarial attacks (Norzoi et al., 2023). Such capabilities are critical for ensuring the integrity of digital evidence, particularly in cases involving forgery or falsified documentation.

Automation is a key focus of emerging technologies in forensics, with AI systems playing a central role in streamlining the investigative process. By automating repetitive and labor-intensive tasks, such as file sorting and evidence triage, AI significantly reduces the time required to analyze large datasets (Du et al., 2023). Automated tools powered by AI enhance the capacity of forensic teams to manage complex cases efficiently allowing investigators to focus on high-level analysis and decision-making.

AI-powered systems are particularly impactful in multimedia forensics, where they enable the automated detection of cyber threats, sexual exploitation content, and network vulnerabilities (Jarrett & Choo, 2021). These advancements not only improve efficiency but also enhance the reliability and objectivity of forensic investigations by minimizing human error.

Despite the promise of emerging technologies, challenges remain in their implementation. One major issue is the vulnerability of ML and DL models to adversarial attacks which can compromise the accuracy of forensic analyses (Nayerifard et al., 2023). Additionally, the rapid pace of technological innovation often outstrips the development of forensic tools, necessitating continuous research and adaptation.

Future directions in forensic technology include the integration of advanced AI tools for encrypted data handling, computer vision and fingerprinting. These innovations aim to address existing limitations while expanding the capabilities of forensic science. Moreover, fostering interdisciplinary collaboration between computer scientists, forensic practitioners, and sociologists will be essential for developing ethical, transparent, and effective forensic technologies.

Thus, emerging technologies, particularly in machine learning and deep learning are reshaping the landscape of forensic science. By addressing challenges such as data complexity and volume, these technologies enable more accurate and efficient investigations, paving the way for advancements in digital forensics, IoT forensics, and multimedia analysis. As the field continues to evolve, balancing innovation with ethical considerations and addressing vulnerabilities will be critical to ensuring the integrity and effectiveness of forensic science in the era of AI.

5. FORENSIC SOCIAL SCIENCE

(i) The Paradigm Shift in Sociology Through AI and Big Data

Historically, sociology has been characterized by hypothesis-driven inquiry, grounded in classical theories that relied on structured datasets and statistical modeling to test specific relationships. Scholars such as Émile Durkheim and Max Weber laid the foundation for this approach (Ritzer & Murphy, 2023). Durkheim, often considered the father of positivist sociology, emphasized the scientific study of "social facts"—elements of collective life that could be objectively measured and analyzed using statistics. His seminal work *Suicide* (Durkheim, 1897) used statistical analysis to reveal the relationship between social integration and individual behavior, showcasing how macro-level social structures shape personal outcomes. This method of systematically studying social phenomena through statistical relationships became a cornerstone of sociological analysis, which has been influential in various areas, from crime statistics to health disparities (Giddens, Duneier, Appelbaum, & Carr, 2017).

Weber, while prioritizing the subjective meaning of human actions, also embraced scientific rigor. In *The Protestant Ethic and the Spirit of Capitalism* (Weber, 1905), he combined historical and sociological analysis to uncover how cultural values influenced economic behavior. Weber's focus on the interplay of structure and agency set the stage for later sociologists to explore both subjective and objective aspects of social phenomena, blending qualitative insights with quantitative analysis (Bourdieu, 1990). Both Durkheim and Weber demonstrated how empirical and statistical methods could be employed to address complex sociological questions, cementing sociology's role as a science (Bryman, 2012). However, these traditional methods have increasingly been complemented, and in some cases challenged, by more sophisticated computational tools.

Specifically, the integration of AI and big data analytics into contemporary sociological research marks a significant shift from traditional methodologies. Unlike Durkheim's predefined hypotheses or Weber's interpretive frameworks, computational science enables a data-driven inductive approach where patterns emerge from vast, multidimensional datasets (MacFarland et al., 2015). Such computational tools can identify intricate relationships, analyze unstructured data, and generate new sociological insights, effectively expanding the boundaries of empirical research (Savage & Burrows, 2007). This shift reflects the growing recognition that the new computational tools can process and analyze massive datasets, offering new opportunities for sociologists to explore complex social phenomena that were previously difficult to study (Järvinen & Mantere, 2018).

This shift has sparked the emergence of *Forensic Social Science*, a term coined by McFarland, Lewis, and Goldberg (2015). They argue that the advent of big data calls for sociology to adopt methods that mirror forensic investigation—meticulously reconstructing societal phenomena from digital traces. Building on this foundation, Goldberg (2015) emphasized the necessity of Forensic Social Science to address the challenges posed by big data, advocating for approaches that combine computational methods with sociological theory to meaningfully interpret complex datasets. Together, these works established a framework for modern sociology to embrace big data while retaining its theoretical depth.

Interestingly, this turn towards forensic methodologies echoes the ahead-of-their-time ideas of Gabriel Tarde, a French sociologist and contemporary of Durkheim. Tarde, often overlooked due to Durkheim's dominance, emphasized micro-level interactions, such as imitation, invention, and opposition, as the building blocks of social phenomena (Tarde, 1899). His relational approach anticipated modern sociological concerns with networks and the diffusion of ideas (Latour, 2002). For example, Tarde's concept of imitation as a driver of social behavior resonates with the analysis of information spread on social media, where AI algorithms can map how ideas propagate across networks (Papilloud, 2004). Similarly, his emphasis on invention underscores the generative potential of social systems, highlighting the creative interplay between actors (Tarde, 1899).

At the same time, the integration of computational methods and AI in sociology amplifies a long-standing debate about the role of quantification (Espeland & Stevens, 2008). Durkheim's statistical methods aimed to legitimize sociology as a science, but critics have argued that over-reliance on quantitative measures risks oversimplifying the complexities of social life (Bauman, 1992). AI, with its computational power, can exacerbate such reductionism, particularly when algorithms abstract social behaviors into decontextualized data points (Savage & Burrows, 2007). However, forensic social science can help bridge this gap by leveraging AI's computational power to not only analyze data but also contextualize it meaningfully, particularly in critical domains such as criminal justice (Movva, 2021).

(ii) Risks: Colonization of Sociology by Engineering Frameworks

However, this integration is not without its challenges. One of the most significant concerns, as noted by McFarland et al. (2015), is the risk of sociology being colonized by engineering frameworks and hard sciences. The authors argue that the increasing reliance on AI and computational methods threatens to subordinate sociological inquiry to the technical priorities and epistemologies of engineering disciplines. This colonization can manifest in several ways:

Reductionism: Engineering frameworks often prioritize quantification, efficiency, and prediction, reducing complex sociological phenomena to datasets stripped of context and meaning. For instance, Weberian verstehen—the process of interpreting subjective social meanings—risks being overshadowed by purely algorithmic interpretations that prioritize data patterns over human experience.
Loss of Reflexivity: Sociology has long emphasized critical reflexivity, encouraging researchers to question their own assumptions and methodologies. In contrast, engineering paradigms often adopt a technocratic logic that prioritizes problem-solving over critical examination, potentially leading to uncritical applications of AI in sociological contexts.
Ethical Oversights: Engineering solutions may prioritize functionality over ethical considerations, leading to the proliferation of black-box AI systems that lack transparency. This raises significant concerns about accountability, especially when these systems influence high-stakes decisions in areas like criminal justice or public policy.
Instrumentalism: Sociology's rich theoretical tradition, which aims to understand and interpret social action, risks being instrumentalized to serve purely technical goals. Forensic social science, when dominated by engineering priorities, may become a tool for surveillance or social control rather than a means of fostering social justice or understanding.

McFarland et al. (2015) argue that sociology must actively resist this colonization by asserting its unique epistemological contributions, particularly its focus on context, meaning, and human agency. This resistance aligns with Habermas's critique of technocracy (1984), which warned that the unchecked dominance of technological rationality could erode communicative action and interpretive nuance. AI-driven forensic methods must be guided by sociological theory to ensure that social phenomena are not reduced to mere data points devoid of context.

(iii) Toward a Balanced Forensic Social Science

To counteract the risks of the colonization of sociology by engineering frameworks, Goldberg (2015) emphasizes the need for an interdisciplinary approach that integrates AI's computational power with sociology's theoretical depth. This approach has been discussed widely in the literature, stressing the importance of preserving the integrity and reflexivity of sociological thought while utilizing technological advancements. Key aspects of this balanced approach include:

Developing transparent AI systems that align with sociological principles of ethics and accountability. This approach draws on broader discussions about the ethical implications of AI, including the works of O'Neil (2016), who highlights the dangers of opaque algorithmic decision-making, and Binns (2018), who stresses the importance of accountability in AI systems used in social contexts. The literature calls for AI models that are interpretable and transparent to ensure they do not reinforce biases or perpetuate unjust outcomes (Lipton, 2016).

Training sociologists in computational methods while encouraging critical reflection on their implications. This idea resonates with the interdisciplinary education advocated by scholars like Klein (1990), who argues for the importance of training scholars from different disciplines to engage critically with both the methods and the implications of the tools they use. This critique has gained momentum as sociologists increasingly encounter the need to navigate technical data analytics within their own research practices (McFarland, Lewis, & Goldberg, 2015).
Using AI as a tool to enhance, rather than replace, the interpretive and theoretical strengths of sociology. Here, AI should be understood as a complement to sociological theory, not as a replacement for the nuanced and context-specific understanding that traditional sociological methods offer. As noted by Lazer et al. (2009), while computational techniques allow for broader data analysis, they must always be grounded in sociological theory to ensure that interpretations do not lose sight of social context and meaning.

In essence, forensic social science should not passively adopt engineering methods but actively adapt them to serve sociological goals. As McFarland et al. (2015) argue, forensic social science must focus on blending empirical, computational insights with critical sociological theories that explore issues of power, inequality, and agency in social processes. By grounding AI techniques in sociological theory, researchers can ensure that their work not only uncovers new patterns but also contributes to a deeper understanding of the human experience.

Such a "balanced approach" aligns with calls for critical interdisciplinarity (Klein, 1990), which avoids the dominance of one discipline over another. In contrast to the potential colonization of sociology by engineering frameworks, Forensic Social Science should foster genuine collaboration where:

Sociologists contribute theoretical depth and interpretive frameworks, ensuring that AI-driven analyses remain grounded in humanistic concerns (Bloor, 1997).
Computer scientists provide technical expertise in data analysis and modeling, offering the computational tools needed to process large-scale data effectively (Domingos, 2015).
Ethicists ensure adherence to principles of justice, fairness, and transparency, tackling the growing concerns about the biases embedded in AI algorithms (O'Neil, 2016).

Such collaboration can mitigate the risks of technological determinism—where technology drives social change in a one-directional manner (Winner, 1986)—and reinforce the dual role of sociology as both a science and a moral enterprise.

(iv) A Transformative Vision

Forensic Social Science represents a transformative vision for sociological research in the digital age. By integrating the computational power of AI with the nuanced insights of sociological theory, it offers the potential to uncover novel patterns and dynamics within complex social systems. However, this integration also raises significant ethical and epistemological challenges, particularly as AI-driven methods risk reducing human behavior to mere data points. To succeed, forensic social science must remain firmly rooted in sociology's critical and reflexive traditions, ensuring that technological advancements serve to enhance, rather than overshadow, the discipline's core commitment to understanding human agency and social meaning.

This approach resonates with the call for a "sociological imagination"—a concept famously articulated by (C. Wright Mills, 1959) to describe the ability to connect individual experiences to broader social structures. In the digital realm, where vast amounts of data are generated through individual interactions, forensic social science can operationalize this imagination by contextualizing data within the lived realities of individuals and communities. For example, (Brayne, 2021) demonstrates how AI-driven data in policing can be critically analyzed through a sociological lens, ensuring that ethical considerations and social contexts are not overlooked. Similarly, (Eubanks, 2018) critiques the unreflective use of AI in social systems, advocating for a more socially informed approach to data analysis that prioritizes equity and justice.

By prioritizing meaning-making over mere data extraction, forensic social science ensures that sociological research remains not only relevant but also deeply impactful in addressing the complexities of contemporary society. As (O'Neil, 2016) warns, the unexamined use of algorithms and big data can exacerbate inequalities and undermine democratic processes. Forensic social science, therefore, plays a crucial role in bridging the gap between computational analysis and meaningful interpretation, ensuring that data is understood within its social, cultural, and ethical contexts. This aligns with(Ferguson's, 2017) argument that the rise of big data policing requires a critical sociological perspective to prevent the misuse of technology and protect vulnerable populations.

6. INTERPRETABLE ALGORITHMIC FORENSICS

As previously noted, forensic science is crucial to the criminal justice system, offering objective evidence that can help establish guilt or innocence. However, the complexity of forensic methodologies and the increasing reliance on advanced technologies have raised concerns about the interpretability and explainability of forensic evidence. Interpretability refers to the ability to understand the reasoning behind a forensic analysis, while explainability involves communicating that reasoning in a clear and accessible manner (Garrett & Rudin, 2020). These concepts are critical for ensuring transparency, accountability, and trust in forensic science. In what follows, we will explore the significance of interpretable and explainable forensic science, drawing on the works of Garrett and Rudin, along with other key references in the field. Additionally, we will examine the challenges associated with achieving interpretability and explainability in forensic practice and explore strategies to address them.

Interpretability and explainability are essential for maintaining the credibility and reliability of forensic science. In the criminal justice system, forensic evidence is often presented to judges and juries who may lack the technical expertise to understand complex scientific analyses. Without clear explanations, there is a risk that forensic evidence will be misinterpreted or given undue weight, potentially leading to wrongful convictions or acquittals (Garrett & Rudin, 2020).

The legal system places a high value on transparency and accountability. Forensic scientists have an ethical obligation to ensure that their findings are presented in a manner that is both accurate and understandable to non-experts (National Research Council, 2009). This is particularly important in cases involving probabilistic evidence, such as DNA profiles or fingerprint matches, where the risk of misinterpretation is high (Thompson, 2013). For example, the "prosecutor's fallacy" occurs when the probability of a match between evidence and a suspect is conflated with the probability of the suspect's guilt, leading to erroneous conclusions (Balding & Donnelly, 1994).

Public trust in forensic science has been eroded by high-profile cases of wrongful convictions and forensic errors, such as the misidentification of bite marks or the misuse of hair microscopy (Innocence Project, 2020). Interpretable and explainable forensic science can help rebuild this trust by demonstrating that forensic analyses are based on sound scientific principles and are subject to rigorous scrutiny (Garrett & Rudin, 2020). Transparency in forensic methodologies and the ability to explain results in plain language are key to achieving this goal.

Despite their importance, interpretability and explainability face significant challenges in forensic science. These challenges stem from the complexity of forensic methodologies, the use of probabilistic reasoning, and the potential for cognitive biases.

Complexity of Forensic Methodologies: Many forensic techniques, such as DNA profiling, fingerprint analysis, and firearm examination, involve complex scientific principles and statistical models. For example, DNA mixture interpretation requires the use of sophisticated software to deconvolute overlapping genetic profiles and calculate likelihood ratios (Butler, 2015). While these methods are highly accurate, they can be difficult to explain to non-experts, particularly when the results are presented in probabilistic terms (Thompson, 2013).
Probabilistic Reasoning: Probabilistic reasoning is a cornerstone of modern forensic science, but it is also a source of confusion and misinterpretation. For instance, the likelihood ratio (LR) is a common metric used to express the strength of forensic evidence. However, without proper explanation, LRs can be misunderstood or misrepresented in court (Aitken & Taroni, 2004). This highlights the need for forensic scientists to communicate probabilistic results in a way that is both accurate and accessible.
Cognitive Biases: Cognitive biases can undermine the interpretability and explainability of forensic evidence. Confirmation bias, for example, occurs when forensic scientists unconsciously favor evidence that supports their initial hypotheses while disregarding contradictory evidence (Kassin, Dror, & Kukucka, 2013). This can lead to errors in analysis and interpretation, as well as a lack of transparency in reporting findings. Addressing cognitive biases requires rigorous training, standardized protocols, and independent verification of results (National Research Council, 2009).

Achieving interpretability and explainability in forensic science requires a multifaceted approach that includes methodological transparency, effective communication, and the use of interpretable models.

Methodological transparency is the foundation of interpretable and explainable forensic science. Forensic scientists must document their procedures, assumptions, and limitations in a clear and comprehensive manner (Garrett & Rudin, 2020). This includes providing detailed descriptions of analytical techniques, statistical models, and validation studies. For example, the Scientific Working Group on DNA Analysis Methods (SWGDAM) has developed guidelines for the validation and interpretation of DNA evidence, which include requirements for transparency and reproducibility (Butler, 2015).
Effective communication is essential for explaining forensic evidence to non-experts. Forensic scientists should use plain language and visual aids, such as charts, graphs, and diagrams, to convey complex concepts (National Research Council, 2009). For instance, the use of likelihood ratios can be explained using analogies, such as comparing the strength of evidence to the odds of winning a lottery (Aitken & Taroni, 2004). Additionally, forensic experts should be trained in courtroom testimony to ensure that their explanations are clear, concise, and free of jargon.
Interpretable Models: The use of interpretable models is another strategy for enhancing the interpretability and explainability of forensic science. Interpretable models are those that provide insights into the reasoning behind their predictions, making them easier to understand and validate

(Rudin, 2019). For example, decision trees and rule-based systems are inherently interpretable because they break down complex decisions into a series of simple, logical steps. In contrast, black-box models, such as deep neural networks, are difficult to interpret and may not be suitable for forensic applications where transparency is critical (Garrett & Rudin, 2020).

Several case studies illustrate the importance of interpretability and explainability in forensic science and highlight best practices for achieving these goals.

DNA mixture interpretation is a complex process that involves separating and analyzing genetic profiles from multiple contributors. The development of probabilistic genotyping software, such as STRmix and TrueAllele, has improved the accuracy and reliability of mixture interpretation (Butler, 2015). However, these tools also raise challenges for interpretability and explainability. To address these challenges, forensic scientists have developed guidelines for validating and interpreting probabilistic genotyping results, as well as training programs to help experts communicate their findings effectively (SWGDAM, 2017).

Fingerprint analysis is a well-established forensic technique, but it has faced criticism for its subjective nature and lack of transparency (Cole, 2005). To improve interpretability and explainability, researchers have developed automated fingerprint identification systems (AFIS) that use algorithms to match prints based on objective criteria (Ashbaugh, 1999). These systems provide detailed explanations of their matching decisions, making it easier for forensic experts to validate and communicate their results. Firearm examination involves comparing toolmarks on bullets and cartridge cases to determine whether they were fired from the same weapon. This process has traditionally relied on subjective visual comparisons, which can be difficult to explain in court (Biasotti & Murdock, 1997). To address this issue, researchers have developed quantitative methods for toolmark analysis, such as 3D imaging and statistical modeling, which provide objective and interpretable results (Bachrach, 2013).

8. CONCLUSIONS

The convergence of forensic science, sociology, and artificial intelligence has ushered in a transformative era marked by both unprecedented opportunity and profound responsibility (Lawless, 2022, pp.125-127) (Goldberg, 2015)(McFarland et al., 2015). As the landscape of forensic science expands from traditional laboratory-based analyses to sophisticated digital forensics and AI-powered investigative tools, it is becoming increasingly clear that the discipline is no longer confined to physical evidence alone. It now encompasses the forensic examination of digital behavior, social networks, biometric data, and massive unstructured datasets that reflect human activity in both virtual and real-world spaces.

This evolution has given rise to *Forensic Social Science* which is a paradigm that marries the computational power of AI with the contextual depth of sociological theory (Goldberg, 2015)(McFarland et al., 2015). This interdisciplinary approach enables the reconstruction of complex social phenomena from digital traces while retaining a critical, reflexive lens grounded in human agency and meaning (Lawless, 2022) (Devlin et al., 2019). At the same time, the shift toward algorithmic systems in criminal justice and forensic analysis raises urgent concerns regarding transparency, bias, and interpretability (Garrett & Rudin, 2020). The risks of over-reliance on black-box models, the potential colonization of sociological inquiry by engineering priorities, and the erosion of public trust necessitate a balanced framework that upholds both scientific rigor and ethical responsibility (Goldberg, 2015)(McFarland et al., 2015) (Nayerifard et al., 2023, pp.3-4).

To realize the full promise of AI-enhanced forensic science, the field must prioritize interpretable and explainable systems, foster genuine interdisciplinary collaboration, and maintain a steadfast commitment to justice, fairness, and transparency (Garrett & Rudin, 2020) (National Research Council, 2009). Only by embedding ethical considerations, legal safeguards, and sociological reflexivity into the fabric of forensic practice can we ensure that technological progress truly serves the public good (O'Neil, 2016; Klein, 1990) (McFarland et al., 2015). In this way, *Forensic Social Science* is not merely a convergence of disciplines which is a critical project aimed at preserving human dignity and advancing equitable knowledge in an age increasingly defined by data.

REFERENCES

Aitken, C. G. G., & Taroni, F. (2004). Statistics and the Evaluation of Evidence for Forensic Scientists. John Wiley & Sons.

Alenezi, A.M. (2023). Digital and Cloud Forensic Challenges. *ArXiv, abs/2305.03059*.

Ashbaugh, D. R. (1999). Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology. CRC Press.

A.M. Qadir and A. Varol. (2020). The Role of Machine Learning in Digital Forensics, In: IEEE International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5.

Bachrach, B. (2013). A Validation Study of the BulletTRAX-3D System. Journal of Forensic Sciences, 58(3), 617-624.

Balding, D. J., & Donnelly, P. (1994). The Prosecutor's Fallacy and DNA Evidence. Criminal Law Review, 711-721.

Biasotti, A. A., & Murdock, J. E. (1997). Firearms and Toolmark Identification: The Scientific Reliability of the Forensic Science Discipline. Academic Press.

Butler, J. M. (2015). Advanced Topics in Forensic DNA Typing: Methodology. Academic Press.

Bauman, Z. (1992). *Intimations of Postmodernity*. Routledge.

Bloor, D. (1997). *Knowledge and Social Imagery* (2nd ed.). University of Chicago Press.

Bourdieu, P. (1990). *The Logic of Practice*. Stanford University Press.

Brayne, S. (2021). *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.

Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford University Press.

Bossler, A., Holt, T. J., & Seigfried-Spellar, K. C. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Dirichlet Allocation. *Journal of Machine Learning Research*, 3, 993-1022.

Breiman, L. (2001). Random Forests. *Machine Learning*, 45(1), 5-32.

1. Lawless, C. (2022). *Forensic Science: A Sociological Introduction*, 2nd Edition. London and New York: Routledge. DOI: http://dx.doi.org/10.4324/9781315760551

2. Roy, R. R., Tanwar, S., & Batra, U. (Eds.) (2024). *Cyber Security and Digital Forensics: Select Proceedings of the International Conference, ReDCySec 2023*. Singapore: Springer. DOI: https://doi.org/10.1007/978-981-99-9811-1

3. McFarland, D. A., Lewis, K., & Goldberg, A. (2015). Sociology in the Era of Big Data: The Ascent of Forensic Social Science. *American Sociologist*, 46(3), 299–307. DOI: https://doi.org/10.1007/s12108-015-9291-8

4. Goldberg, A. (2015). In Defense of Forensic Social Science. *Big Data & Society*, 2(2), 1–3. DOI: https://doi.org/10.1177/2053951715601145

5. Garrett, B. L., & Rudin, C. (2023). Interpretable Algorithmic Forensics. *Proceedings of the National Academy of Sciences*, 120(41), e2301842120. DOI: https://doi.org/10.1073/pnas.2301842120

6. Nayerifard, T. , Amintoosia, H. , Bafghia, A. G., & Dehghantanhab, A. (2023). Machine Learning in Digital Forensics: A Systematic Literature Review. arXiv:2306.04965. https://doi.org/10.48550/arXiv.2306.04965

7. Saferstein, R., & Roy, T. (2021). *Criminalistics: An introduction to forensic science*, 3. Pearson.

8. Jones, G. M., & Winster, S. G. (2022). In M. M. Ghonge, S. Pramanik, R. Mangrulkar, & D.-N. Le (Eds.), *Cyber Security and Digital Forensics* (pp. 115-118). Scrivener Publishing Wiley.

9. Whitcomb, Carrie. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence*, 1(1).

10. Stoll, C. (1989). The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Doubleday.

11. Casey, Eoghan. (2011). Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3.

12. Pollitt, M. (2010). History of Digital Forensics: Insights from Two Decades. Forensic Science International, 169(1), 11-19.

14. Garfinkel, S. L. (2010). Digital forensics: The next 10 years. *Digital Investigation, 7*(Supplement), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

15. Fakiha, B. (2024). Unlocking digital evidence: Recent challenges and strategies in mobile device forensic analysis. *Journal of Internet Services*, 2(2). https://doi.org/10.58346/jisis.2024.i2.005

16. Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. *Forensic Science Communications*, 2(4), 1-13.

17. Kaushik, K., Dahiya, S., Bhardwaj, A., & Maleh, Y. (Eds.). (2022). *Internet of Things and Cyber Physical Systems: Security and Forensics* (1st ed.). CRC Press.

18. Janarthanan, T., Bagheri, M., & Zargari, S. (2021). *IoT Forensics: An Overview of the Current Issues and Challenges*. In *Digital Forensic Investigation of Internet of Things (IoT) Devices* (pp. 223-255). Springer.

20. Rodrigues, G. A. P., Albuquerque, R. D. O., de Deus, F. E. G., de Sousa Jr., R. T., de Oliveira Júnior, G. A., García Villalba, L. J., & Kim, T. H. (2017). Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection. *Applied Sciences*, 7(10), 1082. https://doi.org/10.3390/app7101082

21. Keijzer, N. (2020, June 25). *The new generation of ransomware - An in-depth study of ransomware-as-a-service*. University of Twente.

22. Ribaux, O., Baylon, A., & Lock, M. (2020). The integration of digital forensics into criminal investigations: Challenges and opportunities. Journal of Forensic Sciences, 65(2), 407-415. DOI: 10.1111/1556-4029.14201.

23. Chaurasia, R. K., & Sharma, P. (2017). Solid state drive (SSD) forensics analysis: A new challenge. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*.

24. Kloosterman, W. P., Francioli, L. C., Hormozdiari, F., Marschall, T., Hehir-Kwa, J. Y., Abdellaoui, A., Lameijer, E. W., Moed, M. H., Koval, V., Renkens, I., van Roosmalen, M. J., Arp, P., Karssen, L. C., Coe, B. P., Handsaker, R. E., Suchiman, E. D., Cuppen, E., Thung, D. T., McVey, M., Wendl, M. C., … Guryev, V. (2015). Characteristics of de novo structural changes in the human genome. *Genome research*, *25*(6), 792–801. https://doi.org/10.1101/gr.185041.114

25. Liu, B. (2020). *Sentiment Analysis: Mining Opinions, Sentiments, and Emotions*. Cambridge University Press.

26. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention Is All You Need. *Advances in Neural Information Processing Systems*, 30, 5998–6008.

28. Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. *NAACL-HLT 2019*.

30. Chen, T., & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 785-794.

31. Hamilton, W. L., Ying, Z., & Leskovec, J. (2017). Inductive Representation Learning on Large Graphs. *Advances in Neural Information Processing Systems*, 30, 1025–1035.

32. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet Classification with Deep Convolutional Neural Networks. *Advances in Neural Information Processing Systems*, 25, 1097–1105.

33. van der Maaten, L., & Hinton, G. (2008). Visualizing Data Using t-SNE. *Journal of Machine Learning Research*, 9, 2579–2605.

34. S. Qadir and B. Noor, "Applications of Machine Learning in Digital Forensics, (2021) *International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, Islamabad, Pakistan, 2021, pp. 1-8, doi: 10.1109/ICoDT252288.2021.9441543.

35. Dudek et al., Integrating artificial intelligence in forensic science (2023), https://doi.org/10.15503/emet2023.15.28

36. F. Mitchell. (2014), The use of Artificial Intelligence in digital forensics: An introduction. Digital Evidence and Electronic Signature Law Review 7.

37. D. Quick, K.K.R. Choo. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges, Digital Investigation 11 (4) (2014) 273-294

39. Kebande, Victor & Venter, H.s. (2015). A Functional Architecture for Cloud Forensic Readiness Large-scale Potential Evidence Analysis. 10.13140/RG.2.1.1052.1440.

40. Bernacki, Matthew & Vosicka, Lucie & Utz, Jenifer & Warren, Carryn. (2020). Effects of Digital Learning Skill Training on the Academic Performance of Undergraduates in Science and Mathematics. Journal of Educational Psychology. 113. 10.1037/edu0000485.

41. Koroniotis, Nickolaos & Moustafa, Nour & Sitnikova, Elena & Turnbull, Benjamin. (2019). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. Future Generation Computer Systems. 100. 779-796.

42. (Norzoi et al., 2023)

Du, Y., Li, S., Torralba, A., Tenenbaum, J. B., & Mordatch, I. (2023). Improving factuality and reasoning in language models through multiagent debate. *arXiv*. https://doi.org/10.48550/arXiv.2305.14325

Jarrett A, Choo K-KR. The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Sci*. 2021; 3:e1418. https://doi.org/10.1002/wfs2.1418
.

50. Domingos, P. (2015). *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. Basic Books.

51.Durkheim, É. (1897). *Suicide: A Study in Sociology*. The Free Press.

52. Emirbayer, M. (1997). Manifesto for a Relational Sociology. *American Journal of Sociology*, 103(2), 281-317.

53. Espeland, W. N., & Stevens, M. L. (2008). *A Sociology of Quantification*. *European Journal of Sociology, 49*(3), 401–436. https://doi.org/10.1017/S0003975609000150

54. Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*.

55. Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.

56. Giddens, A., Duneier, M., Appelbaum, R. P., & Carr, D. (2017). *Introduction to Sociology* (10th ed.). W.W. Norton & Company.

57. Goldberg, A. (2015). In Defense of Forensic Social Science. *Big Data & Society*, 2(2), 1–3. https://doi.org/10.1177/2053951715601145

58. Habermas, J. (1984). *The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society*. Beacon Press.

59. Järvinen, M., & Mantere, S. (2018). A Data-Driven Approach to Sociological Analysis. *Sociological Methods & Research*, 47(3), 587-623.

60. Klein, J. T. (1990). *Interdisciplinarity: History, Theory, and Practice*. Wayne State University Press.

61. Latour, B. (2002). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.

62. Latour, B. (2002). Gabriel Tarde and the End of the Social. In P. Joyce (Ed.), *The Social in Question: New Bearings in History and the Social Sciences* (pp. 117-132). Routledge.

63. Lazer, D. M. J., Pentland, A. S., Adamic, L. A., Aral, S., Barabási, A. L., Brewer, D., Christakis, N. A., Fowler, J. H., Vespignani, A., & Watts, D. J. (2009). Computational Social Science. *Science*, 323(5915), 721–723. https://doi.org/10.1126/science.1167742

64. Lipton, Z. C. (2016). The Mythos of Model Interpretability. *Proceedings of the 2016 ICML Workshop on Human Interpretability in Machine Learning*. https://arxiv.org/abs/1606.03490

65.Mills, C. W. (1959). *The Sociological Imagination*. Oxford University Press.

66.Movva 2021 https://doi.org/10.48550/arXiv.2106.13455

67.O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.

68.Papilloud, 2004, https://doi.org/10.1080/1600910X.2004.9672893

69.Ritzer, G., & Murphy, W. W. (2023). *Essentials of Sociology* (7th ed.). SAGE Publications.

70.Savage, M., & Burrows, R. (2007). The Coming Crisis of Empirical Sociology. *Sociology*, 41(5), 885-897.

71.Tarde, G. (1899). *Les Lois de l'Imitation*. Félix Alcan.

72.Tarde, G. (1899). *Social Laws: An Outline of Sociology*. Macmillan.

73.Weber, M. (1905). *The Protestant Ethic and the Spirit of Capitalism*. Scribner.

74.Winner, L. (1986). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press.

Cole, S. A. (2005). More than Zero: Accounting for Error in Latent Fingerprint Identification. Journal of Criminal Law and Criminology, 95(3), 985-1078.

Garrett, B. L., & Rudin, C. (2020). Interpretable and Explainable Forensic Science. Annual Review of Criminology, 3, 1-22.

Innocence Project. (2020). Forensic Science Misconduct. Retrieved from https://www.innocenceproject.org

Kassin, S. M., Dror, I. E., & Kukucka, J. (2013). The Forensic Confirmation Bias: Problems, Perspectives, and Proposed Solutions. Journal of Applied Research in Memory and Cognition, 2(1), 42-52.

National Research Council. (2009). Strengthening Forensic Science in the United States: A Path Forward. National Academies Press.

Rudin, C. (2019). Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. *Nature Machine Intelligence*, 1(5), 206-215.

SWGDAM. (2017). Guidelines for the Validation of Probabilistic Genotyping Systems. Scientific Working Group on DNA Analysis Methods.

Thompson, W. C. (2013). The Role of Probability in Forensic Science. In A. Jamieson & A. Moenssens (Eds.), Wiley Encyclopedia of Forensic Science. John Wiley & Sons.