Accepted for publication in
The Handbook on the Sociology of Artificial Intelligence,
forthcoming from Emerald in 2026.

FORENSIC SCIENCE AND SOCIOLOGY IN THE ERA OF AI

Rahulrajan Karthikeyan and Moses Boudourides

Rahulrajan Karthikeyan, Arizona State University, rkarthi5@asu.edu

Moses Boudourides, Northwestern University, Moses.Boudourides@northwestern.edu

Moses Boudourides is a faculty member of the Northwestern University School of Professional Studies Data Science Online Graduate Program. In 2022-23 he served as Professor of Practice at the Arizona State University School of Public Affairs. Previously, he was a Professor of Computational Mathematics at the University of Patras in Greece and the Department of Electrical and Computer Engineering at the Democritus University of Thrace, also in Greece. His expertise spans Applied and Computational Mathematics, Network Science, and Computational Social Science.

Rahulrajan Karthikeyan recently graduated with a Master's degree in Computer Science from the Ira A. Fulton Schools of Engineering at Arizona State University. He served as a Machine Learning Research Assistant in the Cooperative Robotics Systems Lab (CRS) and co-founded the Google Developer Student Club (DSC) at ASU. His accomplishments include winning more than 20 hackathons and coding challenges. During his studies, he completed CSE 575: Statistical Machine Learning with Professor Moses Boudourides, which led to ongoing collaboration on various computational research projects.

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 in ways less constrained by predefined hypotheses, allowing for the discovery of unexpected patterns and the generation of theories from the digital traces of human activity (McFarland et al., 2015; Goldberg, 2015). However, this process is never entirely free of human assumptions, as the framing of prompts, selection of data, and interpretive choices inevitably shape which patterns emerge and how they are understood. Recognizing this interplay between human judgment and AI-driven pattern discovery highlights both the opportunities and the challenges of forensic social science, paving the way for a more evidence-based approach to studying society that 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 and Rudin, 2023).

KEYWORDS:

(Please supply 6-10 keywords for your Chapter to help with depository and online searches)

1. Forensic Social Science
2. Digital Forensics
3. Crime Scene Analysis
4. Cybercrime
5. Biometric Technologies
6. Facial Recognition
7. Interpretable and Explainable AI
8. Science Colonization
9. Machine Learning
10. Natural Language Processing

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.

As a matter of fact, AI-driven forensic research could be considered "more" inductive than traditional sociology because it draws explicitly on abductive reasoning, which is the mode of inference first formulated by Peirce (1931). For Peirce, abduction is the inferential process through which a plausible explanatory hypothesis is conceived when confronting surprising or anomalous observations that elude explanation under existing theoretical frameworks. Whereas deduction applies general rules to particular cases and induction derives generalizations from repeated instances, abduction begins with anomalies and seeks the most coherent and illuminating explanation for them. Peircean abduction constitutes the generative moment of scientific discovery, wherein novel explanatory hypotheses emerge to render unexpected or puzzling phenomena intelligible. As Goldberg (2015) notes, by transcending the traditional divide between theoretical formulation and empirical observation, abduction has been recognized as a fertile epistemological strategy for fostering conceptual innovation within the social sciences (Timmermans & Tavory, 2014). As Goldberg (2015) explains, Big Data and machine learning techniques do not simply test predefined hypotheses; rather, they generate unexpected patterns and anomalies, prompting theoretical discovery through surprise. This approach mirrors the detective work in Eco's *The Name of the Rose*, where Brother William of Baskerville articulates what abduction entails: "Solving a mystery is not the same as deducing from first principles. Nor does it amount simply to collecting a number of particular data from which to infer a general law. It means, rather, facing one or two or three particular data apparently with nothing in common, and trying to imagine whether they could represent so many instances of a general law you don't yet know, and which perhaps has never been pronounced" (Eco, 1983, p. 307). In forensic social science, AI's ability to process vast, unstructured, and multidimensional datasets makes this abductive potential more visible and systematic than in traditional sociology, where such inferential leaps often remain implicit. By treating the digital traces of social life as evidence to be compiled and interpreted, AI-assisted inquiry opens new conceptual frontiers, enabling theoretical discovery that emerges not solely from preformulated questions but

also from the unexpected empirical surprises that these computational methods reveal (Goldberg, 2015).

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[1]-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

[1] From a non-technical perspective, 'interpretability' in machine learning means how easily humans can understand why a model made a particular prediction or decision.

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

Digital forensics has evolved from ad hoc practices to a sophisticated domain addressing criminal activities ranging from fraud and cyberattacks to social phenomena analysis. This transformation reflects rapid technological advancement and the growing pervasiveness of digital technologies, establishing digital forensics as both a technological and sociological tool in contemporary investigations (Lawless, 2022, pp. 125-127; Jones & Winster, 2022).

(i) Historical Context and Evolution

Digital forensics origins are intertwined with computing evolution (Whitcomb, 2002). Early practices lacked standardized procedures, exemplified by Clifford Stoll's 1980s investigation where a $0.75 accounting discrepancy led to uncovering a sophisticated cyber intrusion by "Hunter," who was stealing information for the Soviet KGB (Stoll, 1989). This case demonstrated digital forensics potential before formal recognition (Casey, 2011, p. 3).

The rise of home computing in the 1980s and Internet in the 1990s broadened the field (Pollitt, 2010) from simple hacking and fraud to complex crimes including illegal pornography and large-scale financial fraud (Casey, 2011, pp. 10-11; Bossler et al., 2015, pp. 254-257). The "Golden Age" (1999-2007) benefited from standardized systems like Microsoft Windows and recognized file formats, simplifying evidence extraction (Garfinkel, 2010, p. 66). However, mobile device proliferation and IoT emergence introduced new challenges as smartphones, tablets, and smart devices became encrypted data repositories with proprietary software (Fakiha, 2024, pp. 79-82; Caviglione et al., 2017, p. 12).

Modern society's reliance on communication networks, mobile devices, cloud computing, and IoT has transformed investigations in scope and complexity (Noblett et al., 2000; Caviglione et al., 2017, pp. 14-15). Cyber physical systems integration into industries and government services emphasized digital forensics necessity for security, cybercrime mitigation, and courtroom evidence provision (Kaushik et al., 2022). New threats emerged including identity theft, cyberbullying, data leakage, malware-infected IoT devices, and DDoS attacks (Janarthanan et al., 2021, p. 229).

Cross-border cybercrime nature complicates investigations, requiring cooperation between jurisdictions with different legal frameworks (Alenezi, 2023). Traditional evidence preservation and analysis face difficulties from data volume explosion and diversity. File system encryption, self-destructing records, and cloud storage create barriers requiring innovative access methods before permanent erasure (Chaurasia et al., 2017, p. 14; Caviglione et al., 2017, pp. 12-13).

Network forensics faces similar challenges with immense traffic volumes making comprehensive analysis impractical. Encryption protocol adoption reduces network traffic visibility, while attackers use anti-forensic techniques including onion routing, traffic padding, and packet obfuscation (Rodrigues et al., 2017, pp. 4-6). Modern malware incorporates anti-forensic measures like polymorphic code and encryption, while cybercriminals employ steganography and remote file-wiping. Crime-as-a-service models, including ransomware-as-a-service platforms, enable sophisticated attacks by non-technical individuals (Keijzer, 2020, pp. 11-12; Caviglione et al., 2017, pp. 13-15).

(ii) AI Role in Digital Forensics

Artificial intelligence has transformed digital forensics by addressing challenges associated with growing evidence volume and complexity. AI's ability to process vast datasets revolutionized investigator approaches, enabling pattern identification, information extraction, and event reconstruction (Ribaux and Souvignet, 2020). AI-powered natural language processing analyzes communication logs, emails, and social media posts, providing insights into digital footprints particularly valuable in organized crime or terrorism cases requiring relationship network uncovering.

Machine learning algorithms automated repetitive tasks like sorting millions of files to identify investigation-relevant ones (Nayerifard et al., 2023, p. 31). Predictive analytics explores criminal behavior anticipation based on digital activity patterns, though ethical and legal concerns remain (Bossler et al., 2015, pp. 622-625). AI video analysis enables CCTV footage investigation, tracking individuals across cameras and predicting movements based on behavior patterns. As an exemplary case from science fiction, Philip K. Dick’s 1956 short story *The Minority Report* and its 2002 Spielberg film adaptation are often cited as cautionary tales about predictive analytics. In both versions, law enforcement relies on a system—telepaths in the story, “precogs” in the film—to foresee crimes before they occur and arrest individuals pre-emptively. The narrative underscores the dangers of such prediction, including false positives, systemic bias, erosion of due process, the creation of self-fulfilling prophecies, and the denial of free will. Though fictional, *The Minority Report* resonates strongly with contemporary debates on predictive policing, algorithmic bias, and the ethics of

forecasting human behavior.

Despite advancements, AI reliance raises transparency and bias questions. Many models operate as "black boxes" with non-interpretable decision-making processes, creating trust issues in high-stakes cases. In contrast, “glass-box AI” refers to systems whose decision-making processes are designed to be transparent and interpretable to humans.[2] In the context of digital forensics, scholars advocate for “glass-box” systems that prioritize interpretability to enable effective legal scrutiny of forensic evidence (Ribaux et al., 2020, pp. 45–46).

(iii) Challenges in Digital Forensics

While AI mitigated some challenges, others persist. Device and data format diversity remains pressing, with IoT proliferation creating file format explosion requiring specific codecs. Missing codecs can stall investigations entirely (Lawless, 2022, p. 127). Digital evidence integration into broader frameworks presents challenges as it often represents one component requiring synthesis with other forensic evidence like DNA or fingerprints. Data volume complicates this integration, overwhelming investigators and impeding timely analysis (Ribaux et al., 2020, pp. 40-47).

Ethical considerations involve law enforcement agency participation in both evidence collection and analysis, raising impartiality questions and potential conflicts of interest. Critics argue practitioners should operate independently to avoid interpretation biases. Standardized protocols and professional certification programs are essential for ensuring digital forensics practice reliability and integrity.

Digital forensics represents a critical intersection of technology, society, and law. Its evolution from ad hoc practice to specialized discipline reflects growing digital evidence importance in contemporary investigations. AI has been transformative, enabling practitioners to tackle device diversity and complexity challenges. However, continued evolution requires navigating significant ethical, professional, and technological hurdles. Balancing innovation with accountability and transparency remains essential for ensuring digital forensics remains a trusted and effective justice tool (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 investigation accuracy, efficiency, and scope. As Kloosterman et al. (2015) noted, "this technological revolution in forensic science could lead to a paradigm shift in which a new role of the forensic

[2] It is a common misconception that applying the "glass-box" label to large language models implies a complete, human-level comprehension of their billions of individual parameters. A more accurate definition refers to the development of an external architecture that provides meaningful interpretability. This is achieved through mechanisms like transparent data sourcing, output attribution, and post-hoc explanation methods that illuminate the model's decision-making pathways. Therefore, the objective is not literal transparency of the model's internal state, but rather a functional transparency that makes its operations visible and scrutable from a user's perspective, thereby supporting trust, accountability, and diagnostics.

expert will emerge as developer of evidence analyzers and custodian of integrated forensic platforms." This highlights the growing need for forensic experts to both analyze evidence and manage technological innovation.

Among the most significant advancements are artificial intelligence applications, particularly Machine Learning and Deep Learning techniques analyzing large, complex datasets across forensic domains. Notable AI techniques include sentiment analysis using neural networks and transformer architectures to track public opinion shifts, natural language processing for cultural narrative exploration, predictive modeling for systemic vulnerability forecasting, graph neural networks for social network mapping, image and video recognition for visual media analysis, and unsupervised learning methods for latent structure identification (Liu, 2020; Vaswani et al., 2017; Blei, Ng, & Jordan, 2003; Devlin et al., 2019; Breiman, 2001; Chen & Guestrin, 2016; Hamilton, Ying, & Leskovec, 2017; Krizhevsky, Sutskever, & Hinton, 2012; van der Maaten & Hinton, 2008).

By automating and enhancing data analysis, these technologies have empowered forensic scientists to process evidence on unprecedented scale and speed. In digital forensics, ML and DL algorithms are employed in malware analysis, image and video forensics, network and IoT forensics, and mobile and memory forensics to identify patterns within vast digital evidence volumes (Qadir & Noor, 2021). These computational advancements play critical roles in cybercrime investigations and multimedia data analysis. As AI technologies evolve, applications expand from enhancing camera image and DNA sample analysis to enabling pattern recognition and crime scene reconstruction (Dudek et al., 2023).

Machine learning techniques continue expanding across image processing, text analysis, voice recognition, and optical character recognition domains, with growing digital forensics applications for extracting insights from vast evidence amounts (Mitchell, 2010). ML methods assist investigators in efficiently analyzing large datasets through data mining and knowledge discovery conceptual models, enhancing critical information uncovering ability (Quick and Choo, 2014; Qadir and Varol, 2020). Supervised ML methods are widely used in live digital forensics for real-time IoT environment data analysis, where billions of interconnected sensors generate diverse data types posing significant investigator challenges. ML-driven frameworks provide robust solutions enabling rapid anomaly detection and intrusion event classification (Kebande et al., 2015).

Deep learning models, particularly convolutional neural networks, demonstrate exceptional performance in adversarial image forensics, tamper detection, and computer forensics (Bernacki et al., 2020). DL techniques handle vast, divergent datasets encountered in forensic investigations, offering high accuracy in network traffic analysis and cyber intrusion detection (Koroniotis et al., 2019). These models are instrumental in video forensics, enhancing tampered or explicit content detection and streamlining investigation processes. In image manipulation detection, DL methods effectively identify subtle visual data alterations, ensuring digital evidence integrity particularly in forgery or falsified documentation cases (Etim and Szefer, 2024).

Automation represents a key emerging technology focus, with AI systems playing central roles in streamlining investigative processes. By automating repetitive tasks like file sorting and evidence triage, AI significantly reduces large dataset analysis time (Du et al., 2023). AI-powered automated

tools enhance forensic team capacity for efficient complex case management, allowing investigators to focus on high-level analysis and decision-making. These systems are particularly impactful in multimedia forensics, enabling automated cyber threat, sexual exploitation content, and network vulnerability detection (Jarrett & Choo, 2021). These advancements improve efficiency while enhancing investigation reliability and objectivity by minimizing human error.

Despite emerging technology promise, implementation challenges remain. A major issue is ML and DL model vulnerability to adversarial attacks, which can compromise forensic analysis accuracy (Nayerifard et al., 2023). Additionally, rapid technological innovation pace often outstrips forensic tool development, necessitating continuous research and adaptation. Future forensic technology directions include advanced AI tool integration for encrypted data handling, computer vision, and fingerprinting. These innovations aim to address existing limitations while expanding forensic science capabilities. 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 machine learning and deep learning, are reshaping forensic science landscapes. By addressing data complexity and volume challenges, these technologies enable more accurate and efficient investigations, paving advancement ways in digital forensics, IoT forensics, and multimedia analysis. As the field continues evolving, balancing innovation with ethical considerations and addressing vulnerabilities will be critical to ensuring forensic science integrity and effectiveness in the AI era.

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 (McFarland 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 computational tools "have created demand for new methods that reduce/simplify the dimensionality of data, identify novel patterns and relations, and predict outcomes, from computational ethnography and computational linguistics to network science, machine learning, and in situ experiments" (McFarland et al., 2015, p. 1).

Yet, the emergence of patterns in AI-driven research is never automatic or entirely neutral. Patterns arise from the combination of statistical regularities in the data and the framing decisions made by the social scientist, such as which datasets are selected, how variables are defined, and which algorithms or prompts are applied. In this sense, the social scientist is usually looking for signals—whether correlations, clusters, or anomalies—while remaining open to unexpected structures that the data might reveal. The process is thus bidirectional: the social scientist guides the AI by curating data and specifying computational tasks, while the analysis can, in turn, prompt the social scientist to consider new hypotheses or theoretical interpretations that were not initially anticipated. This interplay underscores a central methodological concern: if the AI or dataset appears to "prompt" the social scientist without critical reflection, there is a risk of overfitting to coincidental patterns or reinforcing existing biases. Therefore, responsible computational sociology requires maintaining a reflective stance, recognizing that both human judgment and machine discovery co-produce the patterns we study.

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.

McFarland et al. (2015) highlight that the rise of big data encourages a convergence of perspectives and methods across sociology, computer science, and related fields, creating a potential "trading zone" where interdisciplinary collaboration can flourish despite differing terminologies and research cultures. Drawing on Galison (1997) and Collins et al. (2007), they describe trading zones as spaces where boundary objects—shared data, analytic techniques, or methodological tools—enable communication and joint problem-solving across disciplinary divides. Collins et al. (2007) also discuss

how certain trading zones—especially enforced or coercive ones—are shaped by power asymmetries in which dominant methods or data structures are imposed, thereby influencing participation in ways that may ultimately catalyze new research fields. McFarland et al. (2015) thus position big data not only as a technical resource but as a sociological force, capable of transforming the intellectual and social networks of the social sciences through the creation of such trading zones.

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. The social forensics approach provides a mechanism for turning a "black box" of pure pattern recognition into a "glass box" of sociological insight. An AI model, on its own, can only identify what patterns exist in the data. It becomes a transparent, interpretable system only when its findings are systematically subjected to the explanatory lens of sociological theory. In the social forensics model, the AI provides the computational visibility, while the sociologist provides the

theoretical clarity. Therefore, 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. This means moving from statistical pattern-finding to sociological diagnosis. For instance, data extraction can reveal the symptoms of a problem (e.g., specific online behaviors are correlated with user churn), but meaning-making provides the diagnosis by explaining the underlying social mechanisms, guided by established theory. Furthermore, as (O'Neil, 2016) cautions, 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 and Rudin, 2023). 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 and Rudin, 2023).

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 and Rudin, 2023). 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 and Rudin, 2023). 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 and Rudin, 2023).

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 long-standing forensic technique, yet it has been criticized for its subjective nature and lack of transparency (Cole, 2005). As Cole (p. 993) observes, the determination of "individualization" (a match) ultimately depends on the examiner's personal judgment of whether there is "sufficient" correspondence between two prints—a standard the professional community has never been able to define with precision or consistency. 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 tool marks 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, 2005).

7. 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 and Rudin, 2023). 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).

In particular, interdisciplinary collaborations between social science and computer science often generate hierarchical knowledge structures, in which particular methods and theoretical frames dominate the exchange. McFarland observes that sometimes the social sciences' adoption of computational techniques tends to favor approaches aligned with computer science, making sociology appear to converge toward that field rather than the reverse. This dynamic may arise from structural factors, such as the greater scale of funding, research output, and citations in computer science, or from epistemic factors, including its emphasis on puzzle-solving and the production of visible progress, which together render it a seemingly more "fit" or convincing practice of inquiry (D. McFarland, personal email, 31 Mar. 2025).

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 and Rudin, 2023; 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. https://arxiv.org/abs/2305.03059

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

Bachrach, B. (2005). *A statistical validation of the individuality of guns using 3D images of bullets* (NCJ No. 213674). U.S. Department of Justice, National Institute of Justice. Retrieved from https://ncjrs.gov/pdffiles1/nij/grants/213674.pdf

Balding, D. J., & Donnelly, P. (1994). The prosecutor's fallacy and DNA evidence. *Criminal Law Review*, 711-721.

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

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*. https://doi.org/113. 10.1037/edu0000485

Biasotti, A., & Murdock, J. (1997). Firearms and toolmark identification: Legal issues and scientific status. In D. L. Faigman, D. H. Kaye, M. J. Saks, & J. Sanders (Eds.), *Modern scientific evidence: The law and science of expert testimony* (Vol. 2, pp. 124–155). West Publishing Co.

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

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Dirichlet allocation. *Journal of Machine Learning Research*, 3, 993-1022. http://www.jmlr.org/papers/v3/blei03a.html

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

Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5-32. https://doi.org/10.1023/A:1010933404324

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.

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

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

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

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*, *2*(6), 1081–1085. https://ijsrcseit.com/CSEIT1726289

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*, (pp. 785–794). ACM. https://doi.org/10.1145/2939672.2939785

Cole, S. A. (2005). More than Zero: Accounting for error in latent fingerprint identification. *Journal of Criminal Law and Criminology*, 95(3), 985-1078. https://scholarlycommons.law.northwestern.edu/jclc/vol95/iss3/10

Collins, H., Evans, R., & Gorman, M. (2007). Trading zones and interactional expertise. *Studies in History and Philosophy of Science*, 38(4), 657–666.

Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of the 2019 Conference of the North*

American Chapter of the Association for Computational Linguistics: Human Language Technologies, 1, 4171–4186. https://doi.org/10.18653/v1/N19-1423

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

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

Dudek, A., Dąbek, A., Sankhla, M. S., & Kumar, N. (2023). Integrating artificial intelligence in forensic science. *E-methodology*, 15, Article 28. https://doi.org/10.15503/emet2023.15.28

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

Eco, U. (1983). *The Name of the Rose* (W. Weaver, Trans.). Harcourt Brace Jovanovich.

Emirbayer, M. (1997). Manifesto for a relational Sociology. *American Journal of Sociology*, 103(2), 281-317. https://doi.org/10.1086/231209

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

Etim, A. & Szefer, J. (2024). Time traveling to defend against adversarial example attacks in image classification. https://arxiv.org/abs/2410.08338

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

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

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

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

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

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

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

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

Hamilton, W. L., Ying, Z., & Leskovec, J. (2017). Inductive representation learning on large graphs. *Advances in Neural Information Processing Systems*, 30, 1025–1035.

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

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.

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

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.

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. https://doi.org/10.1016/j.jarmac.2013.01.001

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

Kebande, Victor & Venter, H.s. (2015). A functional architecture for cloud forensic readiness large-scale potential evidence analysis. https://doi.org/10.13140/RG.2.1.1052.1440

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

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

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

Koroniotis, N., & Moustafa, N., & Sitnikova, E., & Turnbull, B. (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. https://doi.org/10.1016/j.future.2019.05.041

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 25, 1097–1105.

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.

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

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

Lazer, D. M. J., Pentland, A. S., Adamic, L. A., Aral, S., Barabási, A. L., Brewer, D., Christakis, Contractor, Fowler, J., Gutmann, M., Jebara, T., King, G., Macey, M., Roy, D., Van Alstyne, M. (2009). Computational Social Science. *Science*, 323(5915), 721–723. https://doi.org/10.1126/science.1167742

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

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

McFarland, D. A., Lewis, K., & Goldberg, A. (2015). Sociology in the era of big data: The ascent of forensic social science. *American Sociologis*t, 46(3), 299–307. https://doi.org/10.1007/s12108-015-9291-8

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

Mitchell, F. (2010). The use of artificial intelligence in digital forensics: An introduction. *Digital Evidence and Electronic Signature Law Review*, 7, 36–41. https://doi.org/10.14296/deeslr.v7i0.1922

Movva, R. (2021). Fairness deconstructed: A sociotechnical view of 'fair' algorithms in criminal justice. https://doi.org/10.48550/arXiv.2106.13455

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

Nayerifard, T. , Amintoosia, H. , Bafghia, A. G., & Dehghantanhab, A. (2023). Machine learning in digital forensics: A systematic literature review. https://doi.org/10.48550/arXiv.2306.04965

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

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

Papilloud, C. (2004). Understanding interactivity with Gabriel Tarde. *Distinktion: Journal of Social Theory*, 5(2), 83–102. https://doi.org/10.1080/1600910X.2004.9672893

Peirce, C. S. (1931)**.** *Collected Papers of Charles Sanders Peirce* (C. Hartshorne & P. Weiss, Eds., Vols. 1–6). Harvard University Press.

Pollitt, M. (2010). History of digital forensics: Insights from two decades. *Forensic Science International*, 169(1), 11-19.

Qadir, S., & Noor, B. (2021). Applications of machine learning in digital forensics. *International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, Islamabad, Pakistan, pp. 1-8. https://doi.org/10.1109/ICoDT252288.2021.9441543

Qadir, A. M., & Varol, A. (2020). The role of machine learning in digital forensics. *In 2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–5). IEEE. https://doi.org/10.1109/ISDFS49300.2020.9116298

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges, *Digital Investigation,* 11(4), 273-294. https://doi.org/10.1016/j.diin.2014.09.002

Ribaux, O., & Souvignet, T. R. (2020). “Hello are you available?” Dealing with online frauds and the role of forensic science. *Forensic Science International: Digital Investigation*, 33, 300978. https://doi.org/10.1016/j.fsidi.2020.300978

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

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

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

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. https://doi.org/10.1038/s42256-019-0048-x

Saferstein, R., & Roy, T. (2021). *Criminalistics: An introduction to forensic science* (13th ed.). Pearson.

Savage, M., & Burrows, R. (2007). The coming crisis of empirical sociology. *Sociology*, 41(5), 885-897. https://doi.org/10.1177/0038038507080443

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

SWGDAM. (2017). *Guidelines for the validation of probabilistic genotyping systems*. Scientific Working Group on DNA Analysis Methods.

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

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

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.

Timmermans, S., & Tavory, I. (2014) Theory construction in qualitative research: From grounded theory to abductive analysis. *Sociological Theory* 30(3): 167–186. https://doi.org/10.1177/0735275112457914

van der Maaten, L., & Hinton, G. (2008). Visualizing data using t-SNE. *Journal of Machine Learning Research*, 9, 2579–2605. http://www.jmlr.org/papers/v9/vandermaaten08a.html

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. https://proceedings.neurips.cc/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

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

Whitcomb, C. M. (2002). An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, 1(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

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

INSERT ANY TABLES / FIGS / PICTURES / ILLUSTRATIONS / TABLES HERE (or attach them in separate documents)

Notes for Chapter Authors:

Please ensure that each Table/Fig/Picture/Illustration you use is fully sourced. Where you have used a Table/image that has been published before (this can be online or in another publication) please ensure that you obtain a written permission for use in this publication prior to submitting your chapter. If in doubt as to whether you require a permission, please ask your Volume Editors.