Article 2 Review

In the article "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview," Raed Faqir (2023) aims to discover how artificial intelligence (AI) is currently being used in the judicial system and investigations and describe the impacts that using AI in criminal investigations has caused. To help accomplish this, Faqir created four research objectives to narrow the research's scope and find information in the current research body relevant to his topic. The first is to determine the current techniques and extent to which law enforcement uses AI in its digital criminal investigations. Second, this article seeks to determine how the law regulates evidence obtained through AI technologies and how such evidence's admissibility in court is judged. The third is to gather information to make recommendations about how to ensure that the integration of AI with the judicial process is done in such a way that maintains the current rights of all involved in an investigation. Finally, Faqir wishes to use the knowledge gained from a review of the current body of research to learn the likely future uses of AI in digital criminal investigations and provide guidance for effective applications.

Faqir (2023) collected data from a wide range of primary and secondary sources. The primary sources included court opinion, written law, and scientific and technical resources relating to procedural laws, regulations, and rules. For secondary sources, Faqir gathered articles from various legal databases, cyber and criminal investigation publications, and legal journals. After collecting this data, the content analysis method was employed to study it further and draw conclusions. According to Christen Erlingsson and Petra Brysiewicz (2017), content analysis is a process by which researchers take large amounts of written data and attempt to extract its core themes in concise statements, phrases, and words. After identifying and confirming the main ideas of a text, researchers will transform statements, phrases, and words into more abstract and succinct ideas that are easier to classify. Researchers performing content analysis must then create themes and categories into which they will place the text’s main ideas. By doing this, content analysis makes it easier for researchers to find correlations between resources discussing similar topics.

Faqir (2023) created a qualitative scientific research study using primarily a normative juridical research methodology. According to Taekema (2018), normative legal studies seek to evaluate how current laws, regulations, and legal proceedings are being used and judge whether their current use is just or unjust. Additionally, normative legal studies often attempt to provide recommendations for improving the legal system based on their findings. Faqir’s (2023) research fits the criteria of normative juridical research because it conducts a comprehensive literature review to assess the current state of AI in criminal investigations and provides two lists of recommendations on how AI can be used more ethically and effectively. Furthermore, based on the Module 1 PowerPoint for this class, this article uses archival research methodology because its data is drawn exclusively from existing written resources.

Faqir (2023) incorporated several social science principles discussed in module 2 of this course. For example, Faqir demonstrated parsimony throughout his research paper. The most noteworthy example is in the conclusion, where a list of bullet points provides succinct, easy-to-understand recommendations for the future use of AI in criminal investigations. By doing this, one does not have to be a researcher, be an AI expert, or read and digest the entire body of relevant research to benefit from this paper and utilize its findings. Additionally, AI use in digital criminal investigations is related to determinism. Throughout the paper and in the conclusion, Faqir emphasizes predictive analysis as one of AI's primary current and future applications in law enforcement. This acknowledges that past information and online events can be used to effectively predict and prevent potential future criminal activity. Finally, while Faqir's research did not have research subjects in the traditional sense of the term, he still exemplified ethical neutrality. Faqir showed significant consideration for the rights and privacy of those who may be investigated using AI techniques based on the recommendations of his paper. By making it a priority that AI should be applied in law enforcement within the boundaries of the currently guaranteed rights of individuals, it is apparent that Faqir cares about protecting the rights of those who may be subjected to his recommendations.

Faqir (2023) discusses many topics related to this class's materials throughout his article. For instance, current research shows that AI can significantly increase the accuracy and transparency of digital criminal investigations. This demonstrates the concepts of human factors and human-centered design, described in modules four and seven, respectively. Because humans created the judicial system to settle human affairs and conflicts, designing AI systems used in legal proceedings in a way that produces fair outcomes for all involved is essential. Incorporating transparency caters to people because it allows them to validate the results of an AI-assisted investigation, which improves trust in the technology. Without human trust, AI technology would likely not be accepted as a tool for settling human affairs. Additionally, designing and incorporating AI that provides greater accuracy would compensate for humans' often fallible memories and decision-making tendencies.

Additionally, this article is also relevant to this class's discussion of sociology and social systems in module 8. Faqir (2023) places a strong emphasis on AI in relation to social systems, particularly courts and law enforcement agencies. He shows concern for these social systems by analyzing the current impacts of AI on them and providing recommendations for how AI integration can be carried out while protecting the rights that people expect and are already ensured by these social systems. Additionally, Faqir lays out the differences between several global legal systems and concludes that the use of AI should be tailored to meet the legal criteria for each. As a result, he demonstrates awareness of and respect for existing social institutions.

Furthermore, Faqir (2023) discusses in multiple locations how machine learning algorithms and AI can be used to observe patterns in human behavior and predict a subject's likely future actions, which is related to module four's ideas on psychological factors affecting the risk of cyber offending. For instance, Faqir outlines how natural language processing models can gather text-based information about online criminal activities and compare them to the activity associated with an ongoing investigation. This is related to the subspecialty of cognitive psychology, which studies the mental processes of individuals and the impacts of their thoughts and perceptions on behavior. By compiling and analyzing the text-based information that an investigation subject posts online, investigators get a glimpse at how the individual thinks and makes decisions. AI can then compare the results of analyzing known online criminal activities and make predictions about the potential risks of the current investigation subject.

Faqir's (2023) recommendations on the strengths of AI use in digital criminal investigations relate to Kathleen Carley's (2020) seven social cybersecurity research areas, particularly diffusion and social cyber-forensics, as discussed in module 10. Chief among these are social cyber-forensics and diffusion. Because vast amounts of social activity coincide across multiple social media networks, it can be difficult for people to track when potential criminal activity is brewing. However, AI may be able to address this issue by continuously monitoring real-time information in cross-platform environments. By analyzing real-time data, AI could address social cyber-forensics by identifying the source of a particular problem and the platform from which it originates. AI could then track the diffusion of this information by noting who interacted with it and determining how and when the information spread to other platforms and groups. By doing this, AI may be able to predict which malicious activities and social media campaigns may present the highest-risk threats and alert law enforcement of measures that may need to be taken to prevent such threats.

One potential challenge using AI in law enforcement could pose for marginalized groups is that it may reinforce existing systemic prejudices. While Faqir (2023) claims that current studies show that AI can eliminate bias and lead to more equitable, fair outcomes, this may not be entirely true. There are several instances where AI tools have demonstrated racist tendencies, such as being more likely to describe people of color as "criminals" based solely on pictures (Raikes, 2023). This likely stems from the reality that AI algorithms are trained using human-generated content. As a result, AI's decision-making capabilities are fundamentally based on human behavior and thus should not be considered a completely unbiased arbiter. Treating AI tools as such could end extremely poorly for marginalized groups because it could solidify unfair judgments against them as "objective truths" to the general public because they are made by "unbiased" machines. Based on Faqir's (2023) emphasis on AI's usefulness in analyzing vast amounts of data, AI could benefit marginalized groups disproportionately incarcerated and targeted by law enforcement. Specialized AI algorithms could be created and provided with arrest data, previously and recently enacted laws, and judicial proceedings to perform pattern analysis. This pattern analysis would aim to identify trends and biases related to specific laws and enforcement tactics that may contribute to the unfair treatment of particular groups. This would provide valuable information to people with power that they can consider to modify, create, or repeal laws to achieve equal treatment of all people by law enforcement and the judicial system.

Faqir (2023) makes a societal contribution in his paper by providing two lists of recommendations about the use of AI in law enforcement. First, he makes a list focused on individuals' privacy rights. These recommendations include not neglecting to go through proper channels to obtain a warrant for searching digital devices and collecting data, focusing on collecting only quality, necessary information rather than collecting as much data on an individual as possible, and respecting the privacy of collected information by implementing effective data protection methods, such as encryption. A second list of recommendations is provided at the end of the paper's conclusion. These are more general and provide guidance about potential law-enforcement applications where AI could be most beneficial, primarily concerning data analysis and pattern recognition. Using AI in this way can help forecast crime, prioritize high-risk cases, identify suspects using biometrics, prevent crime using smart surveillance, and optimize investigative management tasks. In addition to providing recommendations, this article is valuable because it supplies a comprehensive review of existing literature that may be fragmented because AI is a relatively new technology that recently began experiencing rapid development and penetrating many aspects of society. By doing so, this article provides a unified compilation of data about the current state of AI use in digital criminal investigations. As a result, this paper acts as a foundational starting point for further research into AI use in law enforcement.

References

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, *7*(3), 93–99. https://doi.org/10.1016/j.afjem.2017.08.001

Faqir, R. S. A. (2023). Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. *Internation Journal of Cyber Criminology*, *17*(2), 77–94.

Raikes, J. (2023, April 21). *AI can be racist: Let's make sure it works for everyone*. Forbes. https://www.forbes.com/sites/jeffraikes/2023/04/21/ai-can-be-racist-lets-make-sure-it-works-for-everyone/?sh=2243e9792e40

Taekema, S. (2018). Theoretical and normative frameworks for legal research: Putting theory into practice. *Law and Method*. https://doi.org/10.5553/rem/.000031