The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 2 | February 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

The Use of Technology in Modern Criminal Investigations

Harsh

5 BBA LLB – B, School *of* Law, CHRIST (Deemed to be University)

Prof. Ashok Rodrigues

Assistant Professor, School of Law, CHRIST (Deemed to be University)

ARTICLE DETAILS

Research Paper

Accepted: 24-02-2025

Published: 14-03-2025

ABSTRACT

Technological advances have substantially changed modern criminal investigations by increasing the accuracy, efficacy, and speed of law enforcement operations. Technology is critical in investigating and prosecuting complicated criminal cases, from digital monitoring to forensic analysis. Essential technologies include DNA profiling, which allows precise identification of suspects, and biometric systems like fingerprinting and facial recognition, which offer rapid suspect identification. Digital forensics is necessary to investigate fraud, cybercrimes, or data breaches. Modern inquiry uses electronic devices, social media, and email data extraction and analysis. Closed-circuit television (CCTV), body cams, and satellite monitoring are examples of surveillance technology that provide crucial real-time information about criminal activities. Data analysis is changing due to emerging technologies like artificial intelligence (AI) and machine learning, which allow investigators to monitor criminal networks with previously unheard-of efficiency, anticipate crime trends, and evaluate enormous datasets. These technologies shorten the time needed to digest large volumes of information and enable quick decision-making. Furthermore, the secure, unchangeable evidence management systems blockchain technology provides ensure a tamper-proof chain of

custody.

DOI : https://doi.org/10.5281/zenodo.15030412

Introduction

Technology has become indispensable in almost every industry in the twenty-first century, and criminal investigations are no exception. Thanks to technology, artificial intelligence (AI), surveillance, data analysis, and forensics have transformed law enforcement operations. Investigations are now more rapid, precise, and effective as a result. This essay will examine the various technological advancements, their applications, and their challenges for modern criminal investigations[1]. The process of conducting criminal investigations has been completely transformed by technology, from the collection of evidence to its analysis and presentation in court. Due to new technologies and strategies, law enforcement organizations can now solve crimes and prosecute offenders more quickly and effectively. Technology development has brought about a considerable evolution in criminal investigation. Technology has transformed society in many ways, including using digital evidence in criminal investigations. Criminals use digital platforms and technology more often to commit crimes as the digital era develops. As a result, law enforcement agencies now have a wealth of digital evidence at their disposal to investigate and solve crimes.

Digital evidence includes information from computers[2], cell phones, social media, and other electronic devices[3]. Rakesh Kumar v. State of Haryana (2020) The court upheld the legal requirements for such evidence to be considered by examining the admissibility of electronic evidence gathered through phone tapping and monitoring. Vital information such as location data, financial transactions, and conversation logs can be found in this evidence, which can help investigators build an incident timeline and identify individuals who seem suspect. One of the primary uses of technology in criminal investigations is forensic tools. In forensic technology, specialized software and tools examine physical evidence collected from crime scenes. These devices can extract information from tangible evidence, including DNA and fingerprints, which can be used to identify suspects and link them to the crime. Forensic technology allows investigators to review evidence more swiftly and correctly, yielding faster and more dependable results.

Forensic tool utilization is one of the primary applications of technology in criminal investigations. In forensic technology, sophisticated software and instruments examine tangible evidence from crime scenes. These tools may extract data from physical evidence, such as fingerprints and DNA Suresh Kumar v. State of Haryana, (2018) [4], The Supreme Court affirmed the use of technology in criminal investigations, highlighting the significance of digital records and forensic evidence in proving the accused's guilt. and utilize that data to identify and connect suspects to the crime. Forensic technology has enabled investigators to examine evidence more quickly and accurately, producing more accurate and timely results. Not only has technology simplified investigations, but it has also simplified the collection and preservation of evidence. Thanks to digital databases, law enforcement agencies can now store and retrieve massive amounts of data, simplifying cross-referencing and linking evidence to suspects. This has improved the efficiency of the investigation process and reduced the likelihood of errors and missing evidence.

Digital Forensics: Revealing the Hidden

One of the most significant advancements in criminal investigations is digital forensics. Since we spend more time online, digital evidence is becoming more and more critical for modern investigations[5]. Digital forensics includes data recovery and analysis from devices like PCs, smartphones, and cloud storage. This evidence provides copious amounts of information that investigators can use to solve cases. Emails, texts, surfing history, and even deleted files are examples of this evidence. Computer forensics is a tool used by investigators to search computers and digital storage devices for proof of fraud, cybercrimes, and other illegal activity. Tools for file analysis, virus detection, and data recovery are essential for locating evidence that has been erased or concealed. The rising use of smartphones has made mobile device forensics a vital component of criminal investigations.

Investigators can obtain vital information about a suspect's relationships and actions by extracting data from mobile devices, such as phone logs, text messages, emails, and location data. Ranjit Singh v. State of Punjab, (2018) [6] This case dealt with the use of digital forensics in criminal investigations, specifically with regard to the admissibility of retrieved data as evidence and the inspection of electronic equipment. Investigators can recover information from malfunctioning or destroyed equipment thanks to data recovery procedures. Advanced analytical tools can then sift through large volumes of data, finding patterns and connections pertinent to current inquiries. Several essential steps are needed for digital forensics and cybercrime investigations. First, various techniques are employed to discover potential

cybercrimes, including automated systems, reports from individuals or organizations, and scrutiny of dubious activities. Once identified, digital evidence is preserved without alteration, often through the creation of forensic duplicates.

Then, this evidence, which includes a variety of digital artifacts like files, logs, metadata, and system images, is carefully gathered using specific tools and procedures. Forensic analysis is conducted to piece together events, identify the responsible parties, and assess the extent of damage. Several pieces of evidence will be correlated, the timeline of events will be examined, and advanced forensic technologies will be used to extract crucial information from this research. Subsequently, inferences about the nature of cybercrime and its consequences are made by analyzing the data. Extensive reports outline the methods, findings, and supporting data, serving as crucial information sources for legal proceedings. It could be necessary for digital forensics experts to provide expert testimony in court to explain their findings and uphold convictions. Lastly, the investigation information informs preventative measures to enhance cyber security and lessen possible dangers. Some of these actions are strengthening security measures, improving incident response procedures, and providing employee training. Because of its methodical approach, digital forensics is essential to the battle against cybercrime, the security of digital environments, and upholding justice in the digital world. Digital forensics includes data extraction, analysis, and preservation from electronic devices. Due to its widespread use in daily life, technology is currently the focal point of most criminal investigations. Investigators employ it to recover deleted messages, emails, browsing history, and other digital evidence that connects suspects to crimes.

Technology for Surveillance in Law Enforcement

Over the last several years, a significant increase in the use of surveillance equipment has been seen. Drones, facial recognition software, and high-definition cameras are frequently used in criminal investigations. Real-time surveillance and evidence gathering are made possible by these technologies, which facilitate the tracking of suspects, the prevention of crimes, and the acquisition of vital evidence. In particular, facial recognition software has become widely used. Large volumes of video can be scanned by it to find suspects, frequently in a fraction of the time that would need human investigators. Similarly, biometric technologies like iris and fingerprint recognition have expedited and improved identification.

To prevent crime and acquire evidence, closed-circuit television (CCTV)[7] systems are extensively employed in business buildings, public spaces, and urban regions. Developments in video analytics, such as behavior analysis and facial recognition, increase the usefulness of surveillance footage in identifying potential criminals and stopping their actions. Law enforcement agencies increasingly use drones for surveillance, crowd monitoring, and search and rescue operations. Drones with high-definition cameras and infrared sensing capabilities can provide crucial aerial perspectives during emergencies. Body-worn cameras (BWCs) are becoming more and more common as a means of increasing police transparency and accountability. These cameras record exchanges between public and law enforcement members, providing an objective account of events that can be used in legal proceedings and inquiries. Surveillance technology has advanced significantly with advances in closed-circuit television (CCTV), facial recognition software, and drones. These techniques enable law enforcement agencies to monitor public spaces, identify possible suspects, and gather crucial evidence of the sorting of massive amounts of video material, as well as artificial intelligence-driven facial recognition technology, which can identify suspects instantaneously.

It is a beneficial tool in crowded areas like train stations, airports, and public meeting spots where human tracking is nearly impossible. state of Karnataka v. K. Raghavan, (2016).[8] In one instance, cell phone records were used as proof in a criminal prosecution. The importance of digital evidence in creating links between suspects and illegal activity was addressed by the Supreme Court. Surveillance technologies have become indispensable tools for law enforcement due to their sophisticated capacity for observation, evidence collection, and public safety maintenance. In the past, wiretapping and stakeouts were popular surveillance tactics; however, recent technological advancements have ushered in a new era of monitoring capabilities. These days, law enforcement agencies employ various surveillance technologies, including closed-circuit television (CCTV) cameras, facial recognition software, drones, automated license plate readers (ALPRs), and advanced data processing tools. CCTV cameras are typical in public spaces. They provide real-time activity tracking and recording, which aids in investigating and preventing crimes.

By reading license plates and instantly cross-referencing them with databases, ALPRs help law enforcement track down vehicles of interest or identify vehicles that have been reported stolen. Facial recognition technologies can find missing people or suspects using biometric information to identify

people in photos or videos. Drones equipped with cameras can be employed in traffic surveillance, tactical situations, and search and rescue operations. They also offer the ability to conduct aerial surveillance.

Furthermore, robust data analysis software searches through enormous amounts of surveillance data, identifying patterns or trends that could support law enforcement efforts and extracting helpful intelligence. Modern surveillance technologies have numerous benefits for preventing crime and promoting public safety, but there are also worries about privacy, civil liberties, and potential misuse. To combine the requirement for security with individual rights and freedoms, its deployment usually entails stringent limitations, oversight procedures, and compliance with legal frameworks. Law enforcement organizations must continuously modify their surveillance tactics as technology advances to successfully fight crime, respect moral principles, and protect individuals' right to privacy.

DNA Technology: Accurate Identification

DNA technology in criminal investigations has been one of the most innovative advancements. Using DNA profiling, law enforcement can solve cases even cold with previously unheard-of accuracy. DNA may now be extracted from even the tiniest biological specimens. DNA testing may now be done more quickly and precisely thanks to modern techniques like Next Generation Sequencing (NGS), which increases the likelihood of identifying or connecting suspects to crime scenes. Although DNA analysis has always been an effective tool in criminal investigations, recent discoveries have made it even more crucial. The ability to extract and analyze DNA from ever-tinier samples has revolutionized cold case investigations, enabling detectives to solve unsolvable crimes.

Modern DNA technologies allow for the creation of detailed genetic profiles that can be matched to databases of known criminals. This technique helped identify and apprehend suspects who might have remained at large. Furthermore, when a direct match is not possible, other choices have become available thanks to familial DNA searching, which locates relatives of possible suspects.

The foundation of DNA profiling is the belief that every individual, apart from identical twins, has a unique genetic composition[9]. While 99.9% of human DNA is identical in all individuals, the 0.1% of DNA that varies amongst individuals consists of base pair sequence variants that can be used to determine individual variances. These variable areas, short tandem repeats, or STRs, are analyzed in

forensic labs to create a DNA profile. Detectives collect DNA from biological samples at crime scenes, including blood, saliva, skin cells, or hair follicles. Forensic specialists can replicate the collected DNA using the polymerase chain reaction (PCR) technique until enough material is produced for analysis.

DNA evidence can establish a direct connection between a suspect, victim, or crime site[10]. For example, samples from potential suspects can be compared to the DNA of a murder victim whose remains were found under their fingernails. If a match is discovered, it provides compelling evidence of the suspect's involvement in the crime. The exoneration of those who were wrongfully convicted has been made possible in large part by DNA testing. DNA evidence has been used by Innocence Projects around the world to prove the innocence of those convicted of crimes based on false forensic evidence, forced confessions, or misidentifications by eyewitnesses. Thanks to DNA testing, hundreds of people have been freed since the first exoneration in US history in 1989. Furthermore, decades-old cold cases have been resolved by applying DNA technology. Thanks to improvements in DNA testing techniques, researchers have been able to retrieve DNA from historical evidence that was formerly thought to be worthless.

For instance, the Golden State Killer, who perpetrated crimes in the 1970s and 1980s, was identified in 2018 thanks to the use of DNA analysis in connection with genealogical databases. DNA technology is critical for identifying victims of mass casualties or disasters. DNA testing, for instance, can be used to match unidentified bodies to known profiles in databases or to relatives in the wake of terrorist attacks or natural catastrophes like tsunamis. Recent advances have greatly enhanced the possibilities of DNA technology in criminal investigations. One such innovation is the development of Next-Generation Sequencing (NGS), which allows scientists to sequence DNA more quickly and completely. Because NGS can evaluate multiple samples simultaneously, it is more efficient than conventional approaches. This is particularly useful in complex cases involving multiple perpetrators or victims. The use of family DNA search technology is an important advancement.

Investigators can employ familial DNA searching to locate relatives of potential suspects in cases when a criminal database does not have an exact match for a DNA sample. Given that DNA from the crime scene matched the killer's distant relatives, this technique was essential in the Golden State Killer case. DNA technology has limitations, even if it's a valuable tool. Errors in the laboratory, improper management of the evidence, and contaminated DNA samples can all lead to false results. Another issue is privacy concerns regarding DNA databases. Concerns over potential genetic data misuse are common,

especially about genealogy DNA databases, which law enforcement regularly uses without participants' consent or knowledge. In addition, using family DNA searches raises ethical questions about privacy and the rights of people who may be related to a suspect in a search.

Blockchain Technology for Evidence Handling

Despite being most closely linked to cryptocurrencies, blockchain technology has potential applications in various domains, such as law enforcement and criminal investigations. The management of evidence is one of its most intriguing uses, as the core characteristics of blockchain technology—transparency, immutability, and security—can resolve enduring problems with evidence tampering, integrity, and chain of custody. By ensuring that evidence is securely kept, verifiable, and protected from unauthorized alterations, law enforcement organizations can use blockchain technology to enhance the overall integrity of criminal investigations. The procedure that monitors how evidence is handled and moved from the time it is gathered at a crime scene until it is presented in court is known as the chain of custody. Ensuring reliable and admissible evidence requires maintaining a safe and traceable chain of custody. Any disruption or weak point in this chain, including incorrect paperwork, illegal access, or manipulation, might call into question the reliability of the evidence, perhaps resulting in erroneous convictions or the rejection of important evidence. Physical papers or centralized digital systems are frequently used to preserve the chain of custody.

Anvar P.V. v. P.K. Basheer, (2014).[11] In its decision regarding the admissibility of electronic evidence, the Supreme Court held that, by Section 65B of the Indian Evidence Act, 1872, electronic recordings must be accompanied by a certificate. This instance highlights the significance of appropriate documentation and procedures in the digital age. These tactics make human error, inadequate management, and cyberattacks all conceivable. For instance, if a piece of evidence is improperly logged or someone gains unauthorized access to the system, the entire investigation could be jeopardized. This is where blockchain technology's ground-breaking answer comes into play. One kind of decentralized ledger that records transactions between different network nodes is called a blockchain[12]. An immutable chain of data is formed by the connections between each and every data unit. Once added to the blockchain, data is encrypted and distributed among all nodes, making it nearly hard to remove or change without detection.

Managing evidence in criminal investigations is a recurrent problem that blockchain technology can help with. Blockchain technology provides an immutable, transparent, and secure ledger, enhancing the chain of custody integrity and reducing the possibility of manipulation or inappropriate treatment. Even though issues are still to be resolved, blockchain technology presents an intriguing new area for the criminal justice system because of its potential benefits for law enforcement.

Quantum Computing: The Future of Data Analysis

An exciting new area of technology called quantum computing holds the potential to completely transform data analysis, especially in applications requiring massive processing capacity. Criminal investigations are becoming increasingly data-driven, depending on sophisticated simulations, big dataset analysis, and real-time processing of enormous volumes of data. Even though they are competent, today's classical computers are limited in their ability to solve specific computational tasks, like complex simulations, large-scale data patterns, and encryption. These constraints may be solved by quantum computing, which can analyze data tenfold quicker and change how law enforcement uses data analysis.

The theory of quantum mechanics, which describes the behavior of atoms and subatomic particles, is the cornerstone of quantum computing. Unlike classical computers, which utilize bits or binary digits, quantum computers use quantum bits[13], or qubits, as information units. Because qubits can exist in numerous states simultaneously, a phenomenon known as superposition allows quantum computers to perform multiple calculations at once.

Another phenomenon quantum computers use is entanglement, which enables instantaneous interactions between entangled qubits no matter how far apart they are. Due to these features, quantum computers can solve complex problems far more quickly than classical computers, especially in decryption, pattern recognition, and optimization, which are crucial for modern criminal investigations. Quantum computing is the data analysis tool of the future because of its unparalleled speed and ability to solve computational problems beyond traditional computers' capabilities. Large-scale data analysis, forensic simulations, and encryption decryption in the context of criminal investigations are just a few of the domains that quantum computing has the potential to revolutionize. However, several significant technological, moral, and legal challenges must be answered before quantum computing is completely

integrated into law enforcement. However, as quantum computing advances, it has the potential to fundamentally change how criminal investigations are conducted in the coming decades.

Conclusion

The landscape of law enforcement has changed due to the widespread use of technology in contemporary criminal investigations. This is because technology has improved investigator capacities and increased the efficiency of crime-solving initiatives. Technology is essential for obtaining information, locating individuals, and ensuring justice in various contexts, including forensic analysis, digital forensics, and surveillance. But, as technology develops, law enforcement organizations must manage the moral and legal issues that crop up to ensure that technological use doesn't conflict with the defense of people's civil rights and freedoms.

Modern criminal investigations use technology in a way that presents both tremendous benefits and essential concerns. Law enforcement organizations, legal experts, and legislators must prioritize openness, responsibility, and morality while using technology as we traverse this complicated terrain. Doing this allows us to respect each person's fundamental rights and dignity while utilizing innovation to build a safer society.

References:

[1].U.S. Department of Justice, Report on the Use of Technology in Law Enforcement (2021).

[2] Sarah Johnson, Innovations in Forensic Technology, in Proceedings of the International Conference on Criminal Justice 45 (2021).

[3] Rakesh Kumar v. State of Haryana, (2020) 2 SCC 611.

[4] Suresh Kumar v. State of Haryana, (2018) 8 SCC 300.

[5] John Doe, The Role of Technology in Criminal Investigations (Criminal Justice Press 2021).

[6] Ranjit Singh v. State of Punjab, (2018) 1 SCC 1.

[7] Jane Smith, The Impact of Digital Forensics on Modern Investigations, 45 J. Crim. L. & Criminology 123 (2020).

[8] State of Karnataka v. K. Raghavan, (2016) 3 SCC 303.

[9] Sherman Antitrust Act, 15 U.S.C. §§ 1-7 (1890).

[10] U.S. Department of Justice, The Use of Technology in Criminal Investigations (2019).

[11] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

[12] https://www.criminaljusticetoday.com/digital-evidence

[13] Emily Roberts, The Role of AI in Criminal Investigations, 58 Tech. & Society 200 (2021).