IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# The Impact Of Technology On Criminal Investigations And Evidence

**Dr. Princy Singla**

princysingla1987@gmail.com

**Abstract**

In the evolving landscape of criminal investigations, technology has emerged as a transformative force, revolutionizing evidence collection and law enforcement operations. This study explores the integration of advanced tools such as artificial intelligence, big data analytics, digital forensics, and biometrics in modern policing. By enhancing the speed, accuracy, and credibility of investigations, these technologies address traditional limitations and adapt to the challenges posed by cybercrime and sophisticated criminal activities. Historical milestones, including fingerprint and DNA analysis, laid the groundwork for contemporary advancements such as 3D crime scene reconstruction and predictive policing. Digital forensics now plays a pivotal role in uncovering crucial electronic evidence, while surveillance technologies like CCTV, drones, and facial recognition have expanded investigative reach. However, the ethical implications of these tools, particularly concerning privacy, bias, and data security, require careful consideration. This study also highlights disparities in technological access among law enforcement agencies, stressing the need for capacity-building initiatives. Future trends point toward increased reliance on AI and data-driven policing, demanding stringent ethical standards and transparent governance. Through examining these developments, the study offers policy recommendations to guide responsible technology integration, ensuring that innovation enhances justice while safeguarding civil liberties.

**Keywords:** Criminal Investigations, Law Enforcement, Artificial Intelligence, Big Data Analytics, Digital Forensics, Biometrics, Fingerprint, DNA Analysis and Facial Recognition

## 1. Introduction: Technology's Role in Modern Criminal Investigations

In today's rapidly evolving world, technology has become an indispensable tool in criminal investigations. The integration of digital tools and advanced analytical systems has significantly improved the ability of law enforcement agencies to solve complex cases and ensure justice. Technologies such as artificial intelligence (AI), big data analytics, digital forensics, and biometric identification have transformed traditional investigative methods. These technologies not only enhance the speed and efficiency of investigations but also improve the accuracy and credibility of the evidence collected, helping reduce human errors and biases. Investigative agencies now rely heavily on predictive analytics to anticipate criminal behavior and prevent crimes before they occur (Dinesh, 2024).

Moreover, the growing sophistication of cybercrimes and digital offenses has necessitated a parallel evolution in investigative technologies. The use of AI algorithms in identifying crime patterns and serial offenses, as discussed by Bessonov (2022), has opened new avenues in criminalistics and evidence analysis (Bessonov, 2022). The capacity to analyze vast volumes of data quickly and accurately ensures that investigators can find links and patterns that would otherwise remain hidden using traditional methods. Digital footprints, forensic analysis of electronic devices, and blockchain technologies for evidence tracking are now integral parts of the

investigative process. This technological transformation has not only streamlined operations but has also led to higher conviction rates and greater public trust in the criminal justice system. As technology continues to evolve, its role in criminal investigations will only deepen, influencing how law enforcement tackles increasingly sophisticated crimes. By embracing new tools and methodologies, criminal justice systems are better positioned to protect communities, uphold justice, and adapt to the changing nature of crime.

### 1.1. Importance of Technology in Contemporary Law Enforcement

The advent of technology has revolutionized contemporary law enforcement, offering new methods to detect, prevent, and solve crimes efficiently. Modern policing now relies on advanced surveillance systems, automated fingerprint identification, facial recognition technology, and real-time crime mapping. These technological tools have drastically improved law enforcement's ability to monitor public spaces, manage data, and coordinate operations across different agencies. The deployment of AI in policing not only enhances operational efficiency but also contributes to data-driven decision-making, reducing biases and improving transparency (Akhmedova & Ugli, 2023).

Furthermore, innovative systems such as the Criminal Investigation Tracker enable law enforcement to manage cases digitally, integrate evidence management, and collaborate more effectively across jurisdictions. Wadhwa et al. (2022) explain how this system assists in streamlining evidence analysis, reducing human errors, and enhancing case outcomes (Wadhwa et al., 2022). The use of predictive policing models, which leverage data analytics to identify potential crime hotspots, enables proactive interventions that can prevent crimes before they occur. These technological advancements underscore the critical role that technology plays in shaping modern law enforcement practices, ensuring public safety, and enhancing the efficiency and accountability of the criminal justice system. As technology becomes more ingrained in policing, continuous adaptation and ethical considerations will be essential to balance security with the protection of civil liberties. Thus, the importance of technology in contemporary law enforcement lies not only in operational enhancements but also in its capacity to promote a more just and transparent criminal justice system.

### 1.2. Scope and Objectives of the Study

The scope of this study encompasses the exploration of how emerging technologies have reshaped criminal investigations and evidence handling. It aims to assess the integration of digital tools such as AI, machine learning, forensic data analysis, and blockchain in streamlining investigative processes and improving evidence management. This research intends to provide a comprehensive understanding of the benefits and challenges associated with technological advancements in criminal investigations. Specifically, it will analyze how technology enhances the speed, accuracy, and reliability of investigations while considering the legal and ethical implications of its use (Elshobake & Sakka, 2024).

The study's objectives include evaluating the impact of modern investigation technologies on solving complex criminal cases and understanding how these technologies influence judicial proceedings and evidence admissibility. It will also investigate the evolving role of law enforcement personnel in the digital age, focusing on how technology demands new skills and competencies among investigators. According to Bahteev and Cvetkova (2024), effective integration models and algorithms are necessary for optimizing forensic activities and ensuring that technological innovations align with legal standards and practical needs (Bahteev & Cvetkova, 2024). Ultimately, this study seeks to contribute valuable insights for law enforcement agencies, policymakers, and legal professionals on the strategic adoption and ethical use of technology in criminal justice.

## 2. Historical Evolution of Technology in Law Enforcement

The integration of technology into law enforcement has a rich and transformative history. Initially, criminal investigations relied heavily on eyewitness accounts and rudimentary evidence collection, often leading to unreliable outcomes. The late 19th and early 20th centuries marked major milestones with the advent of fingerprint analysis and crime scene photography, which set the foundation for scientific investigative methods. As forensic science matured, techniques such as blood typing and ballistic analysis were developed,

greatly enhancing the precision and reliability of crime-solving efforts. Dinesh (2024) emphasizes that modern criminal investigation systems now leverage data aggregation and predictive analytics to significantly improve investigative efficiency (Dinesh, 2024). In the digital age, the incorporation of databases, facial recognition technologies, and artificial intelligence (AI) has transformed law enforcement practices, facilitating quicker suspect identification and more efficient case management. Moreover, highlight how AI, coupled with digital profiling, has led to the emergence of cyber-detectives who are specially equipped to tackle technology-driven crimes. Complementing these advances, Korma (2024) illustrates the growing significance of a technology-based approach in criminal investigations, where digital forensic tools have become crucial for maintaining the integrity of evidence and achieving higher conviction rates (Korma, 2024).

### 2.1. Impact of Technological Milestones on Crime-Solving

1. **Fingerprint Analysis (Late 1800s)**|: Fingerprinting introduced a reliable, scientific method of identifying individuals. It replaced unreliable eyewitness testimony and established a standardized identification system, dramatically increasing the accuracy of criminal investigations.
2. **DNA Fingerprinting (1980s)**|: The development of DNA analysis revolutionized forensic science by allowing for near-certain suspect identification. It became a cornerstone in solving violent crimes and exonerating the wrongly convicted (Korma, 2024).
3. **Automated Fingerprint Identification Systems (AFIS)**|: AFIS enhanced the speed and reliability of fingerprint matching, significantly reducing the time required for investigations and expanding the capabilities of law enforcement to solve cases efficiently (Dinesh, 2024).
4. **Cyber Forensics (2000s)**|: Cyber forensics became vital in combating cybercrime. By enabling the extraction of digital evidence from devices and networks, it has become indispensable in solving crimes such as identity theft and hacking (Singh et al., 2023).
5. **Artificial Intelligence and Predictive Policing**|: Recent developments in AI allow for predictive policing, where crime patterns are analyzed to prevent future crimes. This has made law enforcement more proactive and effective in crime prevention (Elshobake & Sakka, 2024).
6. **3D Crime Scene Reconstruction**|: Advancements like 3D laser scanning technology now allow forensic teams to recreate crime scenes digitally. This preserves evidence in detailed virtual formats and aids jurors in visualizing the events accurately
7. **Face Recognition Systems**|: Modern facial recognition software assists in the quick identification of suspects from public surveillance footage. This significantly accelerates the investigation process and increases the chances of timely apprehension.

## 3. Digital Forensics: Unlocking Evidence in the Digital Age

Digital forensics has become a cornerstone of modern criminal investigations, providing the methods and tools necessary to uncover critical evidence stored in electronic formats. As crimes increasingly involve digital devices, from smartphones to cloud servers, the role of digital forensics is expanding rapidly. It encompasses the identification, preservation, extraction, and analysis of digital data to reconstruct events and support legal proceedings. Digital forensics is vital for solving cybercrimes, financial frauds, and even traditional crimes that involve digital footprints (Sahay, 2020). The discipline now covers specialized fields such as mobile forensics, network forensics, and cloud forensics, addressing the complexity of modern technologies and their ubiquitous presence in daily life (Selim & Ali, 2024). Additionally, as data encryption and security measures evolve, digital forensics professionals are tasked with staying ahead through constant adaptation and technological proficiency (Vala & Vekariya, 2024). In a digital era where information is power, digital forensics not only aids law enforcement in cracking cases but also ensures that the collected evidence meets stringent legal standards for admissibility in courts.

### 3.1. Key Techniques in Digital Evidence Collection

The collection of digital evidence demands precision, integrity, and adherence to established forensic protocols. One essential technique is disk imaging, which creates a bit-by-bit copy of a storage device to ensure the original data remains untampered during analysis (Sahay, 2020). Memory forensics is another critical method, enabling the retrieval of volatile data, such as encryption keys and running processes, from a system's RAM before it is lost upon shutdown (Selim & Ali, 2024). Additionally, network traffic analysis allows investigators to capture and inspect data packets moving across networks, helping trace cyber intrusions and unauthorized access. As cloud computing gains dominance, cloud forensics has emerged as an indispensable technique, tackling the challenges of data stored remotely and often across multiple jurisdictions (Vala & Vekariya, 2024). Other methods like mobile forensics, file carving, and hash analysis ensure comprehensive data recovery and verification, preserving evidence integrity. Collectively, these techniques not only enhance the breadth of investigations but also ensure that the evidence collected stands up to legal scrutiny, maintaining the chain of custody essential for courtroom proceedings.

### 3.2. Challenges in Digital Data Recovery and Preservation

While digital forensics opens new avenues for investigations, it faces significant challenges in data recovery and preservation. One major hurdle is encryption, which protects data from unauthorized access but also impedes forensic retrieval efforts, requiring sophisticated decryption methods (Rakha, 2024). Another persistent issue is data fragmentation, where information is scattered across storage sectors, complicating the recovery and reassembly of coherent evidence (Selim & Ali, 2024). The proliferation of cloud services introduces jurisdictional complications, as data stored in different countries may be subject to varying legal frameworks, delaying or obstructing access (Vala & Vekariya, 2024). Furthermore, the sheer volume of data generated daily overwhelms existing forensic tools, demanding constant advancements in processing power and analytical capabilities. The volatility of RAM data and the continual evolution of operating systems and encryption technologies add layers of complexity. These challenges necessitate ongoing research, development of new forensic methodologies, and cross-border legal cooperation to ensure that digital evidence remains robust, admissible, and capable of withstanding rigorous examination in judicial settings.

## 4. Surveillance Technologies and Their Investigative Applications

Surveillance technologies have become integral tools in modern criminal investigations, providing law enforcement with enhanced capabilities for monitoring and evidence collection. Devices like closed-circuit television (CCTV) cameras, body-worn cameras, and drones have revolutionized real-time surveillance and evidence preservation. CCTV systems help deter crime and assist in reconstructing events post-incident, offering crucial visual documentation for investigations (Slobogin & Brayne, 2022). Body-worn cameras promote transparency and accountability by recording police interactions, a practice that fosters community trust and aids legal proceedings. Additionally, drones provide aerial surveillance capabilities, especially useful in inaccessible or high-risk areas, expanding the scope of monitoring without endangering officers (Mohamed et al., 2023). The integration of artificial intelligence and machine learning in surveillance systems enhances real-time criminal detection and identification, significantly improving investigative outcomes (Y M, 2024). As surveillance technologies advance, they must be balanced against privacy concerns and ethical considerations, ensuring that investigative gains do not come at the expense of civil liberties.

### 4.1. Role of CCTV, Drones, and Body-Worn Cameras

The use of CCTV, drones, and body-worn cameras has reshaped the landscape of criminal investigations. CCTV systems are a staple in urban security infrastructures, offering continuous monitoring and invaluable post-incident footage that assists in suspect identification and crime reconstruction (Slobogin & Brayne, 2022). Body-worn cameras have become essential for ensuring transparency during police-public interactions, reducing complaints against officers and providing impartial evidence in contentious cases. They are crucial for enhancing trust between communities and law enforcement agencies. Drones offer unprecedented

flexibility and coverage, allowing law enforcement to conduct surveillance over large or difficult terrains with minimal risk to personnel. Their deployment is increasingly common in managing public events, searching for missing persons, and monitoring high-crime areas (Mohamed et al., 2023). Together, these technologies not only enhance investigative efficiency but also contribute to proactive crime prevention strategies. However, their expanded use raises important debates on privacy rights and the need for regulatory frameworks to safeguard individual freedoms while maximizing public safety.

### 4.2. Facial Recognition and Geolocation Tracking in Criminal Investigations

Facial recognition and geolocation tracking technologies have introduced sophisticated methods to criminal investigations, providing precision and efficiency previously unattainable. Facial recognition software analyzes facial features to match individuals with images stored in databases, assisting in suspect identification and missing person cases (Bhatt et al., 2024). This technology, when combined with CCTV and mobile footage, accelerates the identification process and enhances the success rates of investigations. Geolocation tracking, often enabled by GPS data from smartphones or vehicle systems, allows law enforcement to reconstruct suspects' movements, establish alibis, and pinpoint crime locations. The integration of artificial intelligence into these systems further refines accuracy and operational effectiveness, reducing manual processing times. However, the widespread use of facial recognition and geolocation technologies has sparked serious concerns regarding privacy, consent, and potential misuse, emphasizing the need for robust legal and ethical guidelines (Slobogin & Brayne, 2022). While these technologies are powerful investigative tools, balancing their benefits against risks to civil liberties remains a critical priority.

## 5. DNA, Biometrics, and the Science of Identification

DNA and biometric technologies have significantly advanced the science of identification in criminal investigations. DNA profiling, known for its precision, has become a fundamental tool in linking suspects to crime scenes and exonerating the innocent. Advances in genetic technologies, such as mitochondrial DNA analysis and familial searching, have expanded the scope and accuracy of forensic investigations. Alongside DNA, biometric technologies like fingerprint, iris, and facial recognition have been integrated into forensic applications, enhancing the ability to verify identities quickly and reliably. However, the use of biometric and genetic data raises critical ethical concerns, particularly regarding privacy, consent, and the potential for misuse or unauthorized access. As Konovalova et al. (2021) argue, stringent safeguards must be implemented to ensure that the collection, storage, and use of biometric and genetic data respect individuals' rights and maintain the integrity of criminal justice processes (Konovalova et al., 2021). Overall, the intersection of DNA profiling and biometric technology continues to shape a more accurate and ethically mindful future for criminal investigations.

### 5.1. Advances in Genetic Profiling and Crime-Solving

Genetic profiling has evolved from basic DNA fingerprinting to highly sophisticated techniques capable of resolving complex criminal cases. New methods like mitochondrial DNA analysis, short tandem repeat (STR) profiling, and next-generation sequencing have dramatically increased the sensitivity and specificity of genetic investigations. Familial DNA searching, where investigators look for partial matches to relatives of suspects in DNA databases, has proven instrumental in solving cold cases, exemplified by high-profile captures like the Golden State Killer. However, these advances also bring ethical dilemmas, as broader inclusion in DNA databases raises concerns about consent, privacy, and potential biases. As Andreeva and Zaitsev (2021) emphasize, genetic data must be handled with rigorous ethical standards, ensuring that individuals' rights are protected while enabling the effective use of these powerful tools in criminal justice (Andreeva & Zaitsev, 2021). These advancements underscore the dual potential of genetic profiling: groundbreaking crime-solving capabilities alongside significant ethical responsibility.

### 5.2. Biometric Databases and Issues of Accuracy and Bias

Biometric databases have become essential for modern criminal investigations, offering rapid identification through fingerprints, facial recognition, and iris scans. However, their reliability and fairness are increasingly under scrutiny. Although biometric technologies promise efficiency, inaccuracies can arise from poor image

quality, algorithmic limitations, and demographic biases, leading to wrongful identifications (Wang, 2022). Racial and gender biases in facial recognition systems have been particularly concerning, as error rates tend to be higher for minorities and women. Furthermore, the growing scale of biometric databases amplifies privacy risks and the potential for data breaches (Blindenbach et al., 2021). As Konovalova et al. (2021) argue, ensuring the ethical management of biometric databases requires not only technological refinement but also strong legal frameworks to prevent misuse and protect individuals' rights (Konovalova et al., 2021). As reliance on biometrics continues to grow, addressing issues of accuracy, bias, and data protection is crucial to maintain public trust and uphold justice.

## 6. Artificial Intelligence, Predictive Policing, and Big Data Analytics

Artificial intelligence (AI), predictive policing, and big data analytics are reshaping criminal investigations, offering unprecedented capabilities in crime prevention and law enforcement. AI enhances the ability of police agencies to process vast amounts of data, recognize patterns, and predict criminal activity, facilitating a shift from reactive to proactive policing. Predictive policing uses AI algorithms to forecast potential crime hotspots based on historical crime data, allowing law enforcement to allocate resources more efficiently and deter criminal acts before they occur. While these technologies promise to revolutionize policing, they also raise significant concerns regarding fairness, transparency, and bias. According to Berk (2021), predictive policing largely operates through advanced statistical models that can enhance public safety by enabling focused and efficient policing strategies, yet it also involves inherent trade-offs between accuracy, fairness, and operational transparency (Berk, 2021).

### 6.1. Legal and Ethical Challenges in Tech-Driven Investigations

The increasing reliance on technology in criminal investigations brings with it a series of legal and ethical challenges that are reshaping the justice system. Artificial intelligence (AI), big data analytics, and predictive policing promise enhanced efficiency and accuracy, but they also introduce significant risks to fundamental rights such as privacy, due process, and fairness. One major ethical concern is algorithmic bias, where AI systems trained on historical data may perpetuate or even exacerbate existing inequalities, particularly impacting marginalized groups. Lack of transparency in algorithmic decision-making raises questions about accountability and trust in the criminal justice process. Bharati (2024) highlights how the deployment of AI in criminal justice can compromise due process rights if not carefully regulated, emphasizing the need for continuous human oversight and transparent audit mechanisms (Bharati, 2024). Additionally, international practices reveal variations in how different jurisdictions are attempting to manage the integration of AI technologies into law enforcement, particularly at the pre-trial stage. Show that countries like the United States and the United Kingdom have developed comprehensive legal frameworks to regulate the use of AI in criminal investigations, balancing investigative efficiency with privacy protection and public accountability. However, the rapid evolution of technology often outpaces existing laws, creating grey areas in legal practice. Without robust ethical guidelines and legal frameworks, there is a risk that technological tools could erode civil liberties and entrench systemic biases. As such, the future of tech-driven criminal investigations must strike a careful balance between innovation and the preservation of justice, requiring not only technological advancement but also ongoing legal reforms and vigilant ethical scrutiny.

### 6.2. Legal Frameworks: Admissibility and Challenges of Technological Evidence

The admissibility of technological evidence in criminal investigations poses complex challenges requiring careful legal scrutiny. With the rapid advancement of digital forensics, questions around authenticity, chain of custody, and procedural fairness have intensified. Courts must ensure that digital evidence is collected, preserved, and analyzed following strict legal protocols to maintain its admissibility. Stresses that operational investigative activities and expert studies must be properly integrated into criminal cases for judicial acceptance, emphasizing the procedural integrity needed for such Similarly, Mamatkulova (2024) highlights that while technological evidence offers precision, it must meet stringent admissibility standards to protect the rights of defendants and uphold justice (Mamatkulova, 2024). In addition, the emergence of electronic evidence challenges traditional notions of evidence due to its intangible nature, making it critical to adapt procedural laws to accommodate new forms of data. Without clear legal frameworks, the risk of evidence

being dismissed or challenged in court remains high, underlining the need for continuous legal reforms aligned with technological advancements.

### 6.3. Standards for the Admissibility of Digital and Scientific Evidence

Digital and scientific evidence have reshaped criminal investigations, but their admissibility hinges on rigorous standards to ensure fairness and reliability. The primary considerations include authenticity, integrity, relevance, and adherence to procedural safeguards. Zheleva (2021) argues that digital evidence must satisfy strict admissibility criteria, such as authenticity verification, chain of custody documentation, and reliability of the methods used to extract data (Zheleva, 2021). Similarly, emphasizes that compliance with procedural norms and the protection of data integrity are vital to maintaining the legal value of electronic evidence. Courts have increasingly relied on expert testimony to interpret complex scientific data, but concerns about the reliability of emerging techniques persist. Given the dynamic nature of digital technologies, legal systems must continually update standards and best practices to address novel evidentiary challenges. Establishing clear and universally accepted standards for digital and scientific evidence is critical to ensure its effective use while safeguarding defendants' rights and the integrity of the judicial process.

### 6.4. International Differences in Evidence Laws and Their Implications

Variations in evidence laws across countries pose significant challenges in cross-border criminal investigations, particularly with digital evidence. Legal standards governing admissibility can differ widely, affecting how evidence collected in one jurisdiction is treated in another. Pohoretskyi and Lysachenko (2022) highlight that EU countries operate with a mix of controlled and free evidence systems, leading to inconsistencies in the acceptance of foreign-gathered evidence (Pohoretskyi & Lysachenko, 2022). This diversity complicates international cooperation and raises concerns about human rights protections in transnational cases. Further notes that while frameworks like the European Investigation Order aim to streamline evidence-sharing, discrepancies still arise, often causing legal conflicts over admissibility standards. These differences underscore the importance of developing harmonized international legal frameworks to ensure that evidence can be lawfully and reliably used across borders. Without such coordination, disparities may lead to the exclusion of crucial evidence, undermining the effectiveness of global criminal justice efforts.

## 7. Ethical Dilemmas: Privacy, Civil Liberties, and Surveillance Overreach

The expansion of surveillance technologies and digital evidence collection has brought ethical dilemmas to the forefront of criminal justice. Balancing effective crime-fighting with respect for privacy and civil liberties is a persistent challenge. Rakha (2024) asserts that without robust legal and ethical safeguards, the invasive nature of digital surveillance risks violating fundamental human rights (Rakha, 2024). Technologies such as facial recognition, predictive policing, and mass data collection may lead to overreach, particularly against marginalized groups. Leontieva and Toderica (2024) emphasize that evidence obtained through invasive means must meet strict admissibility standards to prevent abuses and preserve the legitimacy of the legal system (Leontieva & Toderica, 2024). The use of surveillance must therefore be guided by principles of proportionality, necessity, and transparency to protect individuals' freedoms. Ethical frameworks must evolve alongside technological advancements, ensuring that the pursuit of security does not compromise the foundational rights that underpin democratic societies.

### 7.1. Balancing Public Safety with Privacy Rights

Balancing public safety with privacy rights remains a central ethical tension in tech-driven investigations. As surveillance and data collection become more sophisticated, ensuring that these tools do not infringe on fundamental rights is crucial. Matis (2024) points out that the rise of digital evidence and electronic surveillance calls for stronger protections around personal data and private communications. Overzealous surveillance can lead to unwarranted intrusions into private life, undermining trust in law enforcement and judicial institutions. further argue that surveillance policies must incorporate oversight mechanisms and judicial review to ensure that law enforcement practices are fair and non-discriminatory. Ultimately, achieving the right balance requires laws that allow for effective crime prevention while setting clear boundaries to

protect civil liberties (Matis, 2024). Legal frameworks should mandate accountability, ensuring that public safety measures remain proportionate and respectful of individuals' privacy.

### 7.2. Ethical Use of Surveillance and Data Collection Technologies

The ethical use of surveillance and data collection technologies in criminal investigations demands careful regulation to avoid misuse and protect rights. Surveillance tools must be deployed transparently and only when absolutely necessary to prevent abuses of power. Rakha (2024) warns that mass data collection without stringent oversight can lead to function creep, where technologies designed for security are repurposed for broader, often intrusive surveillance (Rakha, 2024). Matis (2024) suggests that the ethical collection and use of digital evidence require strict adherence to principles of consent, minimalism, and accountability (Matis, 2024). Ensuring that data collection practices are proportionate and subject to independent oversight is essential for maintaining public trust. As surveillance technologies evolve, so must the ethical frameworks that govern their use, ensuring that technological advantages do not come at the cost of the democratic values they are meant to protect.

## 8. Technological Disparities and Capacity Building in Law Enforcement

The rapid integration of technology into law enforcement has revealed stark disparities in technological access and capacity between agencies. While larger, urban police departments are equipped with advanced tools like big data analytics, AI-driven crime prediction, and real-time surveillance, many smaller or rural agencies lack the infrastructure and funding to adopt similar technologies. These gaps in technological capacity affect not only operational efficiency but also the ability to maintain public trust through transparent, evidence-based policing practices. Bondarenko et al. (2022) emphasize that the complexity of law enforcement work, compounded by inadequate resources, often leads to deteriorating performance and morale among officers (Bondarenko et al., 2022). Capacity-building programs, such as targeted training and technological assistance, have emerged as effective strategies to bridge these gaps. Fleiter, Flieger, and Susanj (2023) document successful initiatives where partnerships with international organizations helped build sustainable enforcement capabilities, particularly in developing contexts (Fleiter, Flieger, & Susanj, 2023). Additionally, Haley and Burrell (2025) argue that AI integration into law enforcement strategies can be transformative but must be paired with capacity-building efforts to ensure equitable benefits across agencies (Haley & Burrell, 2025). Addressing technological disparities through sustained investment and policy reform is essential to ensure that all law enforcement agencies, regardless of size or location, can leverage technological advancements for effective and fair policing.

### 8.1. Gaps in Technological Access Among Law Enforcement Agencies

Despite the rapid advancements in policing technologies, significant gaps persist in technological access among law enforcement agencies, often based on geographic location and agency size. Rural and small-town departments frequently operate with outdated equipment and lack access to tools like AI analytics, cyber-forensics, and advanced surveillance systems, which are increasingly standard in larger urban departments. These disparities not only impede the effectiveness of investigations but also widen inequalities in the administration of justice. Fleiter, Flieger, and Susanj (2023) highlight that even basic enforcement capabilities can be compromised without sufficient investment in technological infrastructure and officer training (Fleiter, Flieger, & Susanj, 2023). Furthermore, Sholihah and Hidayatullah (2023) stress that international collaborations, as seen in capacity-building initiatives in Indonesia, offer valuable models for addressing these gaps by providing resources, training, and infrastructural support (Sholihah & Hidayatullah, 2023). However, Haley and Burrell (2025) caution that without parallel investments in digital literacy and operational capacity, introducing advanced technology may create more challenges than solutions for under-resourced agencies (Haley & Burrell, 2025). Therefore, bridging the technological divide requires not only financial investment but also strategic planning, training, and policy innovation to ensure equitable access to technology across the spectrum of law enforcement agencies.

## 9. Future Trends and Recommendations for Ethical Technology Integration

The future of law enforcement will be heavily shaped by technological integration, with trends pointing toward broader adoption of AI, big data analytics, and real-time surveillance systems. As these technologies evolve, their ethical use becomes paramount. Borum (2020) highlights that intelligence-led policing models will likely dominate, with data-driven decision-making at their core (Borum, 2020). However, warns of potential risks, such as algorithmic biases and privacy infringements, if such technologies are not carefully regulated. Ethical frameworks must be developed to ensure transparency, accountability, and fairness in technological deployment. Khan and Khan (2024) emphasize that real-time data processing can dramatically enhance law enforcement operations, but it must be accompanied by stringent data protection measures to prevent misuse (Khan & Khan, 2024). Going forward, law enforcement agencies must adopt a proactive stance toward ethical technology integration by embedding regular audits, bias assessments, and community consultations into their operational models. The emphasis must be on using technology not just for enhanced efficiency but for building public trust, promoting fairness, and protecting civil liberties. Preparing for these future trends requires balancing innovation with robust ethical standards and transparent governance practices.

### 9.1. Policy Recommendations for Responsible Technology Use

To ensure the responsible use of technology in law enforcement, a set of comprehensive policy recommendations is essential. First, governments must establish clear legal frameworks that define permissible uses of surveillance, data analytics, and AI tools. Khan and Khan (2024) advocate for regular assessments of technology use to ensure compliance with human rights standards (Khan & Khan, 2024). Second, public transparency measures, such as reporting on the use of surveillance technologies, should be mandated to foster community trust. Emphasizes the need for strict oversight bodies to monitor algorithmic decision-making, preventing potential abuses and biases. Third, community engagement initiatives must be launched to involve citizens in discussions about the deployment and limits of policing technologies (Sholihah & Hidayatullah, 2023). Finally, Fleiter, Flieger, and Susanj (2023) propose that law enforcement personnel receive continuous training on ethical standards and technological competencies (Fleiter, Flieger, & Susanj, 2023). Together, these measures can ensure that technological advancements enhance law enforcement capabilities while respecting civil liberties and promoting social justice.

## 10. Admissibility of Electronic Evidence Under BSA, 2023 and IT Act, 2000

In the Bharatiya Sakshya Adhiniyam (BSA), 2023, Sections 61 and 63 are crucial for the admissibility of electronic evidence. Section 61 recognizes electronic records as primary evidence, allowing original electronic data to be presented in court without any alterations. Meanwhile, Section 63 governs the admissibility of electronic records as secondary evidence, treating certified copies or outputs with hash values as valid proof. These provisions provide legal certainty regarding the authentication and reliability of digital evidence. Additionally, the Information Technology Act, 2000 (IT Act), particularly Section 65B, plays a significant role by defining the certification process for electronic records. It ensures that electronic documents, when accompanied by proper certification and procedural safeguards, are admissible in court. Together, these legal frameworks enhance the evidentiary value of electronic records and uphold the integrity of digital evidence in judicial proceedings (Bharatiya Sakshya Adhiniyam, 2023; Information Technology Act, 2000).

## 11. Conclusion

Technology has fundamentally reshaped criminal investigations, providing law enforcement agencies with powerful tools to combat crime more efficiently and accurately. From traditional fingerprinting to modern AI-driven predictive policing, technological evolution has streamlined investigative processes and improved evidence reliability. Digital forensics, surveillance technologies, genetic profiling, and biometrics have become cornerstones of contemporary policing, enabling faster case resolution and enhancing public safety. Yet, the rapid advancement of these technologies brings significant ethical and legal challenges, including concerns over privacy rights, data protection, algorithmic biases, and surveillance overreach. Disparities in technological access across agencies further complicate equitable law enforcement, necessitating targeted capacity-building efforts. As AI and big data analytics continue to permeate law enforcement practices,

balancing innovation with ethical responsibility is crucial. Future integration must emphasize transparency, fairness, and respect for civil liberties. Policy recommendations stress the importance of clear legal frameworks, community engagement, robust oversight, and continuous training to ensure responsible technology use. Ultimately, the sustainable adoption of technology in criminal investigations demands a deliberate and principled approach, ensuring that technological progress strengthens—not undermines—justice and public trust in the criminal justice system.

## References


[1]. Dinesh,, C. (2024). Criminal Investigation System. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. https://doi.org/10.55041/ijsrem33811.

[2]. Bessonov, A. (2022). The Use of Information Technologies in Crime Investigation. Siberian Criminal Process and Criminalistic Readings. https://doi.org/10.17150/2411-6122.2022.1.94-100.

[3]. Akhmedova, G., & Ugli, E. (2023). THE ROLE OF MODERN TECHNOLOGIES IN OPERATIONAL AND INVESTIGATIVE ACTIVITIES. The American Journal of Political Science Law and Criminology. https://doi.org/10.37547/tajpslc/volume05issue04-05.

[4]. Wadhwa, M., Jha, T., Prasad, B., Bajaj, A., Nagpal, L., & Bura, D. (2022). A Hybrid approach on Tracking Criminal Investigation and Suspect Prediction. 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 1, 20-23. https://doi.org/10.1109/com-it-con54601.2022.9850763.

[5]. Elshobake, M., & Sakka, A. (2024). Legal Implications of Emerging Technologies in Criminal Investigations: Current Challenges and Catalysts for Change. International Journal of Social Science Research. https://doi.org/10.5296/ijssr.v12i2.21965.

[6]. Bahteev, D., & Cvetkova, A. (2024). Models of Integrating Modern Technologies into Law Enforcement Activities. Bulletin of Kemerovo State University. Series: Humanities and Social Sciences. https://doi.org/10.21603/2542-1840-2024-8-2-222-230.

[7]. Korma, V. (2024). The Technology-Based Aspect of Using the Criminal Investigation Technique to Perform Investigative Actions. Forensics analyst. https://doi.org/10.18572/2072-442x-2024-2-13-16.

[8]. Singh, V., Dixit, A., Pandey, S., Kumar, B., Pachouri, V., & Sahu, M. (2023). Role of Artificial Intelligence in Criminal Investigation. 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS), 1-4. https://doi.org/10.1109/iQ-CCHESS56596.2023.10391288.

[9]. Sahay, S. (2020). Digital Forensics. Advanced Computing and Communications. https://doi.org/10.34048/2020.4.f2.

[10]. Selim, A., & Ali, I. (2024). The Role of Digital Forensic Analysis in Modern Investigations. Journal of Emerging Computer Technologies. https://doi.org/10.57020/ject.1445625.

[11]. Vala, J., & Vekariya, V. (2024). The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection. International Journal of Life Sciences Biotechnology and Pharma Research. https://doi.org/10.69605/ijlbpr_13.6.2024.80.

[12]. Rakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review. https://doi.org/10.22201/iij.24485306e.2024.2.18892.

[13]. Slobogin, C., & Brayne, S. (2022). Surveillance Technologies and Constitutional Law. Annual review of criminology, 6, 219 - 240. https://doi.org/10.1146/annurev-criminol-030421-035102.

[14]. Mohamed, N., Ahmed, A., Alsharif, A., & ElKhozondar, H. (2023). Employing AI-Driven Drones and Advanced Cyber Penetration Tools for Breakthrough Criminal Network Surveillance. 2023 IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), 1-6. https://doi.org/10.1109/WIECON-ECE60392.2023.10456514.

[15]. M, M. (2024). Surveillance System for Real Time High Precision Recognition of Criminal. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. https://doi.org/10.55041/ijsrem35615.

[16]. Slobogin, C., & Brayne, S. (2022). Surveillance Technologies and Constitutional Law. Annual review of criminology, 6, 219 - 240. https://doi.org/10.1146/annurev-criminol-030421-035102.

[17]. Bhatt, C., Semwal, M., Aswal, P., Goswami, V., Rawat, S., & Dhanalakshmi, R. (2024). Real Time Surveillance Criminal Detection System. 2024 Second International Conference on Advances in Information Technology (ICAIT), 1, 1-8. https://doi.org/10.1109/ICAIT61638.2024.10690333.
[18]. Konovalova, V., Stratonov, V., & Savelieva, I. (2021). Biometric personal data and their use in the investigation of criminal offences. Journal of the National Academy of Legal Sciences of Ukraine. https://doi.org/10.37635/jnalsu.28(4).2021.289-300.
[19]. Andreeva, O., & Zaitsev, O. (2021). Ethic principles of using genetic information during criminal jurisdictional activity. BULLETIN of L.N. Gumilyov Eurasian National University. Law Series. https://doi.org/10.32523/2616-6844-2021-136-3-86-97.
[20]. Wang, Y. (2022). Criminal law imputation path for biometric information. Applied Mathematics and Nonlinear Sciences, 0. https://doi.org/10.2478/amns.2021.2.00280.
[21]. Blindenbach, J., Jagadeesh, K., Bejerano, G., & Wu, D. (2021). Avoiding genetic racial profiling in criminal DNA profile databases. Nature Computational Science, 1, 272 - 279. https://doi.org/10.1038/s43588-021-00058-3.
[22]. Berk, R. (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement. Annual Review of Criminology. https://doi.org/10.1146/annurev-criminol-051520-012342.
[23]. Bharati, R. (2024). Ethical Implications of AI in Criminal Justice: Balancing Efficiency and Due Process. RESEARCH REVIEW International Journal of Multidisciplinary. https://doi.org/10.31305/rrijm.2024.v09.n07.014.
[24]. Mamatkulova, K. (2024). ADMISSIBILITY OF EVIDENCE AS A FEATURE OF EVIDENCE IN CRIMINAL PROCEEDINGS. International Journal of Business, Law and Political Science. https://doi.org/10.61796/ijblps.v1i8.178.
[25]. Zheleva, O. (2021). On the Concept of Electronic Evidence and the Criteria for Their Admissibility. Ugolovnaya yustitsiya. https://doi.org/10.17223/23088451/17/9.
[26]. Pohoretskyi, M., & Lysachenko, Y. (2022). ADMISSIBILITY OF EVIDENCE IN THE CRIMINAL PROCEDURE LAW OF THE EUROPEAN UNION AND ITS IMPACT ON CRIMINAL JUSTICE IN UKRAINE. Herald of criminal justice. https://doi.org/10.17721/2413-5372.2022.3-4/20-34.
[27]. Matis, J. (2024). Certain aspects of criminal evidence and digital evidence. Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2024.02.116.
[28]. Bondarenko, V., Okhrimenko, I., Bilevych, N., Rohovenko, M., Tsurkan, O., & Holyk, V. (2022). Tendency of Dynamics of Physical and Mental Working Capacity of Law Enforcement Officers at Different Stages of their Professional Activities. Acta Balneologica. https://doi.org/10.36740/abal202204115.
[29]. Fleiter, J., Flieger, M., & Susanj, R. (2023). Strengthening Speed and Child Restraint Enforcement Capacity in the Philippines. Journal of Road Safety. https://doi.org/10.33492/jrs-d-22-00034.
[30]. Haley, P., & Burrell, D. (2025). Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety. Law, Economics and Society. https://doi.org/10.30560/les.v1n1p46.
[31]. Borum, R. (2020). Scientific and Technological Advances in Law Enforcement Intelligence Analysis. Advanced Sciences and Technologies for Security Applications. https://doi.org/10.1007/978-3-030-41287-6_6.
[32]. Khan, M., & Khan, M. (2024). Real-Time Data Processing Systems in Modern Law Enforcement: A Technical Analysis. International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2024.v06i06.30723.
[33]. Bharatiya Sakshya Adhiniyam, No. 47, Acts of Parliament, 2023 (India).
[34]. Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[35]. (Bharatiya Sakshya Adhiniyam, 2023)
[36]. (Information Technology Act, 2000)