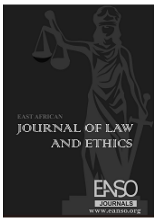

East African Journal of Law and Ethics
eajle.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-532X| Online ISSN: 2707-5338
Title DOI: https://doi.org/10.37284/2707-5338

EANSO
EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Digital Policing in Kenya: Opportunities and Challenges

Prof. John Ndikaru wa Teresia, PhD[1]

[1] The Technical University of Kenya, P. O. Box 57173-00200, Nairobi, Kenya.
[*] Author's Email: jndikaru@gmail.com

Article DOI: https://doi.org/10.37284/eajle.8.1.2970

Date Published:

08 May 2025

Keywords:

Bribe, Cyber Terrorism, Digital Policing, Artificial Intelligence, Crime, Corruption, Drone Technology, Cybercrime, Digitisation, Electronic Communication, Criminal, Fraud.

ABSTRACT

The advancement of technology has permeated all facets of life, including policing. This is necessary considering that many human activities and interactions today are facilitated by technology. In that respect, criminals have also leveraged technology to pursue their agendas. This makes it naturally logical for policing to advance in the same direction to curtail criminality perpetrated in the digital space. On one hand, technology helps policing efforts achieve their ends more efficiently, compared to the traditional methods that relied on hardcopy footprints to track criminals and criminality. On the other hand, technology is prone to abuse by law enforcement agencies in terms of breaching privacy and misuse of private data to undertake extra-legal investigations. This discourse delves into the adoption of policing by law enforcement agencies in Kenya in light of the opportunities and challenges presented so far. The paper advocates for strengthening the existing data protection laws and enforcing compliance to realise a transparent and accountable digital policing system, which balances security needs with privacy rights. There is also a need for implementing strict regulations and establishing oversight mechanisms to ensure facial recognition and Artificial Intelligent (AI) tools are deployed responsibly, ethically, and in a manner that upholds fundamental rights and freedoms in law enforcement. Besides, the establishment and implementation of training programs will go a long way in ensuring that law enforcement officers have the requisite skills and knowledge to effectively deploy the digital tools at their disposal. This is imperative for ensuring that they observe the legal mechanisms and protocols for collecting digital evidence and therefore, make it admissible in courts during prosecution. This will also empower them to knowledgeably navigate the legal and ethical pitfalls inherent in the deployment of digital policing tools, and therefore, safeguard the constitutional rights of members of the public.

APA CITATION

wa Teresia, J. N. (2025). Digital Policing in Kenya: Opportunities and Challenges. *East African Journal of Law and Ethics*, *8*(1), 150-167. https://doi.org/10.37284/eajle.8.1.2957

CHICAGO CITATION

wa Teresia, John Ndikaru. 2025. "Digital Policing in Kenya: Opportunities and Challenges." *East African Journal of Law and Ethics* 8 (1), 150-167. https://doi.org/10.37284/eajle.8.1.2957.

HARVARD CITATION

wa Teresia, J. N. (2025) "Digital Policing in Kenya: Opportunities and Challenges" *East African Journal of Law and Ethics*, 8(1), pp. 150-167. doi: 10.37284/eajle.8.1.2957.

IEEE CITATION

J. N., wa Teresia "Digital Policing in Kenya: Opportunities and Challenges.", *EAJLE*, vol. 8, no. 1, pp. 150-167, May. 2025.

MLA CITATION

wa Teresia, John Ndikaru. "Digital Policing in Kenya: Opportunities and Challenges." *East African Journal of Law and Ethics*, Vol. 8, no. 1, May. 2025, pp. 150-167, doi:10.37284/eajle.8.1.2957.

INTRODUCTION

Kenya is one of the great adopters of technology in Africa. For instance, as of January 2024, there were 66.04 million mobile connections in the country, which far surpassed the current population of 55 million (Ekanem, 2024; Kisio & Wa Teresia, 2024), representing a penetration rate of 118.7 percent (Ekanem, 2024; Mangi & Kandiri, 2024). This is not surprising because Kenya is the mother of the mobile money transfer service, first conceived as MPESA by Safaricom Limited, which has since been adopted by mobile service providers across the globe (Asser et al., 2025).

The Internet has become a necessity for a significant population, with official statistics showing there were 22.71 million users in 2024, representing a penetration rate of 40.8 percent (Mangi & Kandiri, 2024). During the same time, 13.05 million Kenyans, who accounted for 23.5 percent of the population, were active social media users (Asser et al., 2025; Kisio & Wa Teresia, 2024). Additionally, more than 90 percent of Kenyans frequently use digital services such as mobile phones or the Internet to receive or send money and to purchase products or services (Mangi & Kandiri, 2024). The e-governance platform, E-citizen, has reported a growing trend in access to government services via digital interaction, with about 27 percent of Kenyans frequently using it (Mangi & Kandiri, 2024).

Therefore, the digital space in Kenya is vibrant, supporting the social, political and economic facets of life. This vibrancy is, however, undermined by criminal elements that have manifested in various forms of cyber criminals, which have warranted an equal use of digital tools to combat such criminality.

REVIEW OF RELATED LITERATURE

Digital Policing

Fussey & Sandhu, (2022) consider digital policy as a modern approach to law enforcement, which integrates technology, digital tools, and data analytics in the quest to bolster crime prevention, investigation capabilities, and public safety. This implies that digital policing shifts from traditional methods involving manual approaches to crime prevention and management (Galis et al., 2025; Montasari et al., 2023; Pepper & McGrath, 2025). Digital policing is, therefore, not only technology-enabled but also data-driven in the sense that it uses digital resources to facilitate effective, efficient, and proactive decision-making (Galis et al., 2025; Montasari et al., 2023). According to Campbell, (2024), digital policing involves a broad scope of technological advancements that include digital surveillance, big data analytics, and artificial intelligence, which significantly contribute to a police system that is transparent and more responsive.

In essence, digital policing refers to the use of digital tools to support police operations (Galis et al., 2025; Pepper & McGrath, 2025). It also involves the use of digital resources to improve and streamline communication between law enforcement agencies and the public (Davis et al., 2022; Fussey & Sandhu, 2022a). A key aspect of digital policing is predictive analytics, in which case AI-powered algorithms process large volumes of data to map out crime patterns, predict potential criminal activities, and therefore, inform the deployment of resources accordingly (Montasari et al., 2023; Pepper & McGrath, 2025). Pepper & McGrath, (2025) note that this proactive approach is invaluable to law enforcement when anticipating threats and undertaking measures that forestall criminality.

According to Arrigo & Sellers, (2021), cybercrime investigation constitutes another salient component of digital policing. Crimes such as online fraud, identity theft, hacking and cyberterrorism have become increasingly prevalent in the current digital dispensation (Arrigo & Sellers, 2021; Pepper & McGrath, 2025; Wilson-Kovacs & Wilcox, 2023). Law enforcement agencies have therefore turned to digital policing tools to investigate and combat these crimes effectively (Arrigo & Sellers, 2021; Pepper & McGrath, 2025). In particular, digital forensics has proved invaluable for retrieving and analysing electronic evidence from digital devices (Kaufmann & Lomell, 2025; Wilson-Kovacs & Wilcox, 2023), thereby aiding law enforcement agencies in the prosecution of cyber criminals (Fussey & Sandhu, 2022a; Montasari et al., 2023).

Another defining feature of digital policing involves the use of surveillance technologies, such as body-worn cameras (Arrigo & Sellers, 2021; Galis et al., 2025; Wilson-Kovacs & Wilcox, 2023), facial recognition systems (Kaufmann & Lomell, 2025; Pepper & McGrath, 2025; Wilson-Kovacs & Wilcox, 2023) and Internet of Things (IoT) devices (Kaufmann & Lomell, 2025; Wilson-Kovacs & Wilcox, 2023). The use of these tools has enhanced accountability (Arrigo & Sellers, 2021; Wilson-Kovacs & Wilcox, 2023), improved situational awareness (Galis et al., 2025; Kaufmann & Lomell, 2025; Wilson-Kovacs & Wilcox, 2023), and assisted in identifying suspects more accurately (Arrigo & Sellers, 2021; Pepper & McGrath, 2025; Wilson-Kovacs & Wilcox, 2023).

Additionally, digital policing extends to social media monitoring and open-source intelligence (OSINT) (Arrigo & Sellers, 2021; Kaufmann & Lomell, 2025; Wilson-Kovacs & Wilcox, 2023). In this case, law enforcement agencies monitor and analyse publicly available information on social media platforms to track criminal activities and detect threats (Montasari et al., 2023; Pepper & McGrath, 2025). They also use the platforms to engage with communities on matters regarding the management and prevention of crime (Afzal & Panagiotopoulos, 2024). Evidently, social media platforms have become a valuable source of intelligence through which law enforcement agencies have been able to swiftly respond to emerging incidents (Afzal & Panagiotopoulos, 2024; Fussey & Sandhu, 2022a), spread awareness, and foster public participation in crime prevention efforts (Arrigo & Sellers, 2021; Montasari et al., 2023; Pepper & McGrath, 2025).

Mobile policing applications have also revolutionised the operation of law enforcement agencies. Through the mobile policing platforms officers can access real-time data (Arrigo & Sellers, 2021; Pepper & McGrath, 2025); report incidents electronically (Arrigo & Sellers, 2021; Kaufmann & Lomell, 2025; Wilson-Kovacs & Wilcox, 2023), and communicate seamlessly with their teams (Montasari et al., 2023; Pepper & McGrath, 2025). Afzal & Panagiotopoulos, (2024) point out that law enforcement agencies have developed case management systems, which have automated record-keeping, and thus ensured quick retrieval of information, and reduced paperwork.

Background of Digital Policing in Kenya

In Kenya, the evolution of digital policing has largely been in pursuit of improving efficiency, transparency, and accountability in law enforcement. Law enforcement agencies have, thus, resorted to integrating digital tools in their work to enhance their effectiveness in data-driven decision-making, citizen engagement, and, more importantly, crime management (Kemboy & Zakayo, 2024; Mangi & Kandiri, 2024; Mutung'u, 2021). Arguably, the motivation for adopting digital policing in Kenya is closely associated with efforts to combat corruption (Mutung'u, 2021); streamline police record keeping and improve real-time communication between law enforcement agencies and the public (Kemboy & Zakayo, 2024). For instance, the introduction of the digital Occurrence Book (OB) in 2020 was aimed at replacing the manually recorded crime reports, which were easily altered, manipulated, or lost (Makong, 2023; Mutung'u, 2021). Rogue police officers took advantage of the manual records to remove cases from the OB in exchange for bribes from the accused persons (Makong, 2023; Mangi & Kandiri, 2024; Mutung'u, 2021). Notably, the digitisation of the OB has enabled police officers to efficiently record, retrieve, and track cases, which has reduced incidents of lost files and increased accountability.

In the same regard, the digitisation of the police clearance certificates, commonly referred to as the Good Conduct Certificate in 2023, was also another significant milestone towards streamlining police record-keeping in Kenya (Makong, 2023). The document was initially obtained by an individual visiting police stations and undergoing lengthy processing times (Kemboy & Zakayo, 2024; Makong, 2023). The integration of the digital platform, therefore, enabled applicants to apply and track their certificates online via the e-Citizen portal (Makong, 2023; Mangi & Kandiri, 2024; Mutung'u, 2021). The digitised process has not only increased efficiency; it has also significantly reduced corruption since the applicant no longer has to bribe officials to help them speed up the process (Kemboy & Zakayo, 2024).

The cashless payment of traffic fines was another digital policing measure that was aimed at curtailing corruption. Previously, motorists caught violating traffic laws were incentivised to pay bribes to traffic officers as a way to avoid lengthy legal procedures, which included queueing in designated banking halls to pay fines (Kemboy & Zakayo, 2024; Mangi & Kandiri, 2024). The rollout of the online platform for paying traffic fines in 2023 significantly reduced the opportunity for traffic police officers to demand bribes, thereby ensuring increased transparency in law enforcement (Kemboy & Zakayo, 2024; Makong, 2023).

Besides, efforts are underway to roll out the Crime and Incident Reporting System (CIRS) in April 2025. The CIRS is a digital platform that is developed to streamline reporting, documentation, and responses to crime incidents across Kenya (Kimani, 2025; Mwende, 2025). The system is aimed at replacing the manual reporting systems, which were fraught with delays, susceptible to manipulation, and inaccessible to many citizens (Digitali Webbs Services, 2024; Mwende, 2025). The salient feature of the platform is its online and mobile accessibility, which enables citizens to report crime wherever they are without having to visit a police station (Digitali Webbs Services, 2024; Kimani, 2025; Mwende, 2025).

Previously, visiting a police station to file a report was the requirement for reporting crime, which was often cumbersome and discouraged victims of minor offences (Mwende, 2025). This is aimed at enabling law enforcement officers to receive and track crime data in real-time and respond accordingly (Kimani, 2025). The reports made through the system are instantaneously logged into the National Police Service (NPS) centralised database, which will reduce incidents of altered or missing files. The law enforcement officers can also report from whichever location and coordinate across police units to address the reported crime (Digitali Webbs Services, 2024; Kimani, 2025; Mwende, 2025).

The CIRS system is essential for reducing corruption by eliminating opportunities for manipulating crime reports or delaying investigations due to bribery or personal interests by law enforcement officers (Mwende, 2025). The platform automates the reporting process, ensuring that every report is time-stamped and stored securely, which prevents unauthorised alterations (Digitali Webbs Services, 2024; Mwende, 2025). Besides, the complainants can track the progress of their cases online, which reduces the likelihood of those cases being mishandled or ignored (Kimani, 2025; Mwende, 2025). The CIRS, therefore, leverages technology to enhance efficiency, transparency and public trust in law enforcement.

The adoption of these digital tools in policing has called for law enforcement agencies to work in collaboration with various public and private stakeholders. For one, using these tools has required a formidable policy framework whose formulation and implementation have involved the input of the Ministry of Interior and the Communications Authority of Kenya (CAK) (Mangi & Kandiri, 2024). The Kenya ICT Authority has also provided invaluable technical support that has facilitated the integration of digital platforms within government systems, including in policing in particular (Kimani, 2025; Mangi & Kandiri, 2024). Private sector companies such as Safaricom have facilitated mobile-based policing solutions like crime reporting platforms (Fussey & Sandhu, 2022b; Mangi & Kandiri, 2024). There are also international partners such as the United States Agency for International Development (USAID), Interpol, and the United Nations Office on Drugs and Crime (UNODC) who have supported digital policing initiatives by providing training, funding, and technological solutions (Mangi & Kandiri, 2024).

In consideration of the attendant legal and ethical challenges that come with digital policing, various legal frameworks have been put in place to guide law enforcement agencies in the use of the digital tools at their disposal. For instance, the Kenya Information and Communications Act (KICA), 1998, provides a critical legal framework through which electronic communication is regulated (Amadou et al., 2019; Anjarwalla & Sugow, 2022). More importantly, the act also regulates cyber activities and the role law enforcement agencies play in ensuring cyber security. KICA has provisions for ensuring lawful surveillance, enforcement against cyber-related offences and interception of communication (Amadou et al., 2019; Walubengo & Mutemi, 2018). Notably, digital policing activities such as monitoring online criminal behaviour fall under the scope of KICA since law enforcement agencies are required to collaborate with Telecom service providers in the country to track digital footprints (Anjarwalla & Sugow, 2022).

Besides, KICA outlines the guidelines under which lawful intersection of communication can be conducted, which is a critical aspect of digital policing. This is particularly critical in cases related to terrorism, cybercrime, and national security threats, and supports the investigation into digital crimes such as online fraud, identity theft, and hacking (Amadou et al., 2019; Walubengo & Mutemi, 2018). KICA has also established penalties for digital offences, which reinforce the legal backing for police action against cybercrime (Anjarwalla & Sugow, 2022). For example, KICA has criminalised the transmission of false information and authorised access to computer systems and electronic fraud, which provides a basis for law enforcement to act against such digital offences (Anjarwalla & Sugow, 2022).

The Computer Misuse and Cybercrimes Act (CMCA) 2018 is another essential legal instrument that supports digital policing in the way it defines cybercrime (Anjarwalla & Sugow, 2022; Sugow et al., 2021), outlines penalties (Sugow et al., 2021; Walubengo & Mutemi, 2018), and authorises law enforcement agencies to investigate and prosecute offences committed via digital platforms (Anjarwalla & Sugow, 2022; Sugow et al., 2021). A salient provision of the act involves the criminalisation of cyber offences such as cyberstalking, hacking, phishing, unauthorised access to computer systems, and identity theft (Sugow et al., 2021; Walubengo & Mutemi, 2018). The Act, therefore, enables law enforcement agencies to detect and investigate crimes and bring the perpetrators to account for their offences (Amadou et al., 2019).

The CMCA authorises law enforcement agencies to collect, analyse, and preserve electronic evidence, which is essential for addressing cyber-related crimes. The Act provides for real-time interception of communication on the grounds of national security (Sugow et al., 2021), which facilitates proactive policing efforts, especially when it comes to monitoring terrorist activities or tracking financial fraud perpetrated online (Amadou et al., 2019; Anjarwalla & Sugow, 2022; Sugow et al., 2021). More importantly, the Act protects digital users by criminalising online defamation, cyber harassment, and cyberbullying (Walubengo & Mutemi, 2018). It also addresses misinformation and fake news, which are rampant in digital spaces, by specifying penalties for individuals found guilty of spreading false information that may disrupt Public Order or incite violence (Sugow et al., 2021; Walubengo & Mutemi, 2018). In this way, the Act enables law enforcement offices or agencies to use technology in their quest to prevent, detect and respond to cybercrime.

The Data Protection Act (DPA) 2019 is another important legal framework that is shaping digital policing in Kenya. DPA regulates the collection, processing, and sharing of personal data (Nyaga et al., 2023) and is therefore relevant for ensuring law enforcement activities are conducted with respect to the right to privacy and data security of individuals (Mukiri-Smith & Leenes, 2024; Nyaga et al., 2023). The Act advocates for the protection of personal data through lawful, fair, and transparent processing (Sugow et al., 2021). This implies that law enforcement officers are obligated to collect digital evidence in compliance with the Act by ensuring that they handle such data appropriately and safeguard it from misuse (Nyaga et al., 2023). They, therefore, must justify the necessity of accessing communication records or digital transactions of individuals, and upon authorisation, they must protect such data from unauthorised access or use (Nyaga et al., 2023; Sugow et al., 2021).

The DPA restricts law enforcement agencies from collecting personal data unlawfully using means such as mass surveillance, unless they have proper legal backing, which will then exempt them from being held accountable (Nyaga et al., 2023). This provision is critical in preventing potential abuses of power and reinforcing digital policing initiatives (Mukiri-Smith & Leenes, 2024; Nyaga et al., 2023). Additionally, DPA is premised on the concept of data minimisation and purpose limitation, which implies that law enforcement authorities can only collect data for a particular investigation and cannot use such data for any other unrelated purpose (Anjarwalla & Sugow, 2022; Nyaga et al., 2023; Sugow et al., 2021). This provision seeks to ensure that the law enforcement authorities do not infringe upon the rights of citizens by collecting irrelevant or excessive personal information.

Opportunities of Digital Policing in Kenya

The adoption of digital tools has presented significant opportunities for policing in Kenya in terms of improved efficiency, accountability, and community engagement. Some of the key policing areas that have benefited from the use of these digital tools include crime detection and prevention; crime reporting and response; compliance, accountability and transparency; data-driven policing; and community policing.

Crime Detection and Prevention

A key advantage of digital policing in Kenya is its capacity to detect and prevent criminality effectively using tools such as surveillance cameras, biometric databases, and crime mapping (Cheruiyot & Wainaina, 2021; Kirui et al., 2024). Notably, the National Police Service has collaborated with the CAK to install closed-circuit television (CCTV) surveillance cameras in major urban areas such as Nairobi and Mombasa, particularly in crime-prone zones (Cheruiyot & Wainaina, 2021; Kirui, 2024; Kirui et al., 2024). The CCTV footage in downtown Nairobi has been instrumental in identifying pickpockets, tracking down stolen vehicles, and assisting in investigations (Cheruiyot & Wainaina, 2021; Kirui et al., 2024). These cameras have proved invaluable in providing real-time monitoring, thus aiding law enforcement officers in deterring criminal activities and conducting investigations by providing crucial evidence.

Kenyan security agencies use mobile data to track and arrest crime suspects. For instance, police officers tracked and apprehended a suspect, Hudson Musamali Isalamba, in a record two days. Mr. Hudson had stolen a mini Ceska pistol, an iPad, and KSh100,000 from a technician who was inspecting the National Police Service street cameras on Ring Road in Parklands (Mukinda, 2020).

Article DOI: https://doi.org/10.37284/eajle.8.1.2970

The tracking in this case is made possible considering that the agencies have access to mobile phone users' data such as call records and location information, which they use to track the location of suspected criminals and apprehend them(Cheruiyot & Wainaina, 2021; Shabibi & Lautebatch, 2024; Tanui & Barmao, 2016). The agencies access the data via Neural Technologies, a British software company whose data management system is integrated into the internal infrastructure of Safaricom(Kandie & Handa, 2024; Shabibi & Lautebatch, 2024). The Neural Technologies system allows police officers real-time access to the call data of customers. The officers, however, have to process the data through the Law Enforcement Liaison Office at Safaricom headquarters (Kandie & Handa, 2024; Shabibi & Lautebatch, 2024; Sila & Mutuku, 2024).

The police have also used GIS technology to map crime hotspots and allocate police patrols more effectively (Kandie & Handa, 2024; Kenya News Agency, 2019; Sila & Mutuku, 2024). They identify high-risk areas and deploy officers accordingly, taking into account the data on reported crimes (Sila & Mutuku, 2024). For instance, in estates where gang activities and thefts have been prevalent, such as Eastleigh and Kayole, the GIS technology has helped track crime trends and engage with residents (Shabibi & Lautebatch, 2024; Sila & Mutuku, 2024).

Arguably, the integration of drones in urban policing has marked a significant shift toward using advanced technology for more effective crime prevention and crowd control (Kenya News Agency, 2019; Manana & Otieno, 2022). Police have also deployed drones to monitor large gatherings, protest activities, and criminal hideouts (Manana & Otieno, 2022; Wasonga & Ombiro, 2019). For instance, in 2019, the security agencies in Nairobi deployed drones to enhance crime surveillance targeting crime-prone areas such as Eastleigh and the Central Business District (CBD). Using drones, they monitored crime-prone neighborhoods, tracked suspect movements, and provided real-time intelligence to law enforcement (Kenya News Agency, 2019; Wasonga & Ombiro, 2019).

This aerial surveillance significantly improved the capacity of the officers to respond more swiftly to criminal activities. They also leveraged the technology to acquire a bird's-eye view of large crowds or protests, and thus manage public order and prevent potential violence (Wasonga & Ombiro, 2019). In April 2021, the police deployed drones in Nakuru and Kajiado counties to nab those violating COVID-19 lockdown measures, which were critical for enforcing public health directives. The same measures were adopted in Rift Valley after police realised individuals were taking alternative routes to evade roadblocks, often using boda-boda (motorcycle taxis). The police, therefore, deployed high-density cameras to monitor movements to identify and apprehend those circumventing established checkpoints (Matara & Kariuki, 2021).

Drone technology has also proved critical in tracking and responding to banditry in the Northern parts of the country, where this crime is rampant. In Laikipia County, drones have been used to monitor conflicts between herders and farmers, track illegal firearms, and the movement patterns of criminal groups (Manana & Otieno, 2022). Security agencies introduced drone technology in Elgeyo Marakwet County in December 2022 as a tool for curbing regional banditry. This was piloted at the Tot Police Station to monitor the vast and challenging terrain and reduce the advantage that cattle rustlers have enjoyed over the security agencies for a long time. The drones provide real-time footage to a command centre and enable the officers to track and arrest suspects, even in the most remote areas (Kurgat, 2022).

Crime Reporting and Response

Digital policing has improved the capacity of citizens to report crime promptly and receive timely responses from the police. The use of mobile applications, toll-free emergency numbers, and social media platforms have enabled police to respond to security threats more efficiently (Cheruiyot & Wainaina, 2021; Gichohi et al., 2023; Shabibi & Lautebatch, 2024; Sila & Mutuku, 2024). For instance, the Kenyan government initiated a KSh430 million project in 2012 to install 51 surveillance cameras in Nairobi's Central Business District (CBD) to bolster security. The project, dubbed the Integrated Urban Surveillance System (IUSS), was awarded to the Chinese state-owned firm, Nanjing Les Information Technologies (Business Daily, 2020a).

The cameras were designed with facial recognition capabilities and could capture vehicle registration numbers and drivers' faces and transmit them to a central control room. This investment in technology was informed by data from the Kenya Police, which indicated that Nairobi had experienced a 40 percent increase in crime the previous year, with national crime rates rising by 7 percent. Some of the most common offences revealed in the data included robberies, break-ins, theft by servants, criminal damage, economic crimes, corruption, and offences involving police officers (Business Daily, 2020a).

In 2017, the Kenya National Crime Research Centre (NCRC) launched a mobile application designed to enhance crime reporting and evidence gathering (Akama, 2025). The app is available on Android, iOS, and Windows platforms (and accessible from the Play Store and the Apple Store) and allows citizens to securely share crime data, including photos and videos about incidents in their communities (Akama, 2025; Gichohi et al., 2023). The confidentiality assured through the use of the app facilitates a direct channel for the public to report crimes (Akama, 2025). Besides, law enforcement agencies seek to use the collected data aids to come up with informed, research-backed solutions to combat crime and improve community safety (Akama, 2025; Business Daily, 2020).

The Mulika Mwizi (Expose a Thief) App enables citizens to report criminal activities anonymously, wherever they may be located in the country (Gichana, 2023; Mulika Kenya, 2025). Also referred to as Mulika Kenya, the App uses 988 (SMS code) through which individuals report crime incidents to security agencies, either as victims or witnesses of crimes (Gichana, 2023). The key in the message begins with the name of their country, and then they provide the details of the criminal incident. Once sent, the message is received by five security entities, including the County Commissioner, County Police Commander, County Administration Police Commander, County Criminal Investigation Officer, and National Intelligence Service. The system, therefore, ensures that reports reach relevant authorities promptly, even as it protects the identity of the informant (Gichana, 2023; Mulika Kenya, 2025). This has incentivised citizens to participate in crime prevention and made it increasingly easier for police to collect data on crime and respond promptly to incidents (Mulika Kenya, 2025).

Compliance, Accountability, and Transparency

Law enforcement officers have also resorted to technological tools for ensuring compliance with the law in various facets. In August 2018, the National Transport and Safety Authority (NTSA) acquired advanced equipment for the traffic police department, which included specialised digital scanners, communication devices, and speed guns with night vision capabilities, among others. This comprehensive toolkit was aimed at bolstering the enforcement of traffic regulations and mitigating road accidents associated with speeding and impaired driving. For instance, using handheld digital scanners connected to NTSA's database, the traffic police could verify motor inspection records, authenticity of driver's licenses, and vehicle insurance details (Kariuki, 2020).

The proposed use of digital policing tools such as body-worn cameras, automated record management systems, and online complaint platforms has sought to improve transparency and reduce corruption within the police force (Harrison et al., 2022; Montasari et al., 2023). The Kenyan government has piloted the use of body cameras in a bid to curb police misconduct. The cameras provide an objective record of police interactions with the public, thereby reducing incidents of abuse of power and unlawful arrests (Guyo, 2024). According to Davies and Krame (2023), body-worn cameras (BWCs) have contributed to a significant reduction in the prevalence of use-of-force incidents and a decrease in complaints by citizens against the police. They noted that BWC translated into more measured and appropriate responses in police-citizen encounters. The use of BWC by the Rialto Police Department in California significantly reduced police use-of-force incidents and citizen complaints (Ariel et al., 2014). Besides, the use of the technology by the London Metropolitan Police reduced citizen complaints against police by 93 percent and also enhanced police-community relations (University of Cambridge, 2016).

Data-Driven Policing

Data-driven policing involves using data analysis, technology, and predictive algorithms to enhance crime prevention (Afzal and Panagiotopoulos, 2024), resource allocation, and decision-making (David et al., 2022; Lee et al., 2024). This technology involves collecting and analysing crime statistics (Afzal and Panagiotopoulos, 2024; Tschernutter and Feuerriegel, 2025), social trends (Tschernutter and Feuerriegel, 2025), and geographic information to identify crime patterns, high-risk areas, and potential offenders (Lee et al., 2024). Tschernutter and Feuerriegel, (2025) argue that police can deploy resources more efficiently by leveraging tools such as predictive analytics, artificial intelligence, and real-time surveillance. The tools can also be effective in reducing response times (Afzal and Panagiotopoulos, 2024) and developing proactive strategies (Afzal and Panagiotopoulos, 2024; Lee et al., 2024). According to David et al., (2022), data-driven policing improves public safety, accountability, and transparency even as it minimises chances for perpetuating bias.

In Kenya, law enforcement agencies have leveraged big data and analytics to modernise policing. The technology is invaluable in analysing trends and effective allocation of resources for addressing or preventing crime (Xu et al., 2020). The Kenyan law enforcement agencies have thus adopted predictive policing, which uses historical data to understand criminal activities and inform preemptive measures to be undertaken (Luvembe & Mutai, 2019). This has involved the integration of Geographic Information System (GIS) technology into policing (Noor et al., 2020; Xu et al., 2020). Crime mapping has enabled law enforcement agencies to visualise crime hotspots and strategically deploy officers (Xu et al., 2020). The proactive approach has significantly reduced incidents of violent crimes, carjacking, and robbery in areas such as Eastlands in Nairobi.

According to Odhiambo (2024), law enforcement agencies can also use AI to analyze extensive data from road networks, and particularly historical accident data, weather conditions, road infrastructure, and traffic patterns in major cities such as Nairobi, Nakuru, and Mombasa to historical accident data, weather conditions, road infrastructure, and traffic patterns in major cities such as Nairobi, Nakuru, and Mombasa. The predictive capabilities of AI can enable agencies to implement preventive measures such as increased policing, road maintenance, or traffic control on high-risk roads (Luvembe & Mutai, 2019; Saruni, 2025).

Additionally, AI-enhanced systems can be instrumental in optimising emergency response times due to the capacity for predicting accident locations and severity as informed by incoming data from sources such as emergency calls, traffic cameras, and vehicle sensors (Luvembe & Mutai, 2019). AI can also analyse driver behaviour such as aggressive driving, drowsiness, and/or speeding based on the data collected through in-car sensors and external cameras, therefore, providing real-time feedback to drivers or directing interventions to prevent accidents (Luvembe & Mutai, 2019; Odhiambo, 2024).

Furthermore, AI algorithms can also identify potential hazards like potholes, sharp curves, or inadequate lighting by assessing road infrastructure data, thereby, allowing for prioritised maintenance and the design of safer roads. This optimisation is necessary for attaining efficiency in resource allocation and, therefore, saving lives potentially (Luvembe & Mutai, 2019; Saruni, 2025). Notably, the installation of CCTV cameras on Thika Superhighway and Mombasa Road has had a limited impact on reducing road carnage. However, integrating AI-powered driver assistance systems alongside highway CCTV cameras could enhance their effectiveness by capturing adaptive cruise control, lane departure warnings, and automatic emergency braking (Luvembe & Mutai, 2019; Odhiambo, 2024). This would, in turn, translate into alerting drivers to potential dangers and undertaking corrective actions if need be (Odhiambo, 2024).

Fighting Terrorism

Law enforcement agencies use advanced surveillance systems such as closed-circuit television (CCTV) networks and drone technologies to conduct real-time monitoring of public spaces and critical infrastructures (Cheruiyot & Wainaina, 2021; Shabibi & Lautebatch, 2024). These surveillance systems facilitate the early detection of suspicious activities and enable agencies to promptly intervene accordingly (Miruka, 2023). Data analytics tools process vast amounts of information to identify patterns and anomalies associated with terrorist behaviours (Cheruiyot & Wainaina, 2021; Kandie & Handa, 2024).

Notably, ICT tools are crucial for intercepting and analysing communications among terrorist networks (Miruka, 2023). Law enforcement agencies monitor emails, phone calls, and online chats to uncover plots and identify key operatives (Kandie & Handa, 2024; Manana & Otieno, 2022). However, Cheruiyot & Wainaina, (2021) caution that this practice often necessitates a delicate balance between national security interests on one hand and individual privacy rights on the other hand.

Technology is also a formidable proactive tool for law enforcement officers with regard to terrorism. This is critical to note that terrorist organisations often use the internet to spread propaganda and recruit members (Saruni, 2025). Therefore, the use of ICT facilitates to monitoring of extremist content and the promotion of counter-narratives goes a long way in dissuading individuals from radical ideologies (Miruka, 2023). In particular, initiatives such as the Global Internet Forum to Counter Terrorism (GIFCT) are a collaborative effort among tech companies to curtail the dissemination of terrorist content online (Saruni, 2025). Such platforms have enabled law enforcement agencies to exchange intelligence and coordinate responses, which is essential for addressing the transnational nature of terrorism (Saruni, 2025).

Additionally, agencies have leveraged ICT to track financial transactions linked to terrorist funding. The agencies analyse banking data and electronic fund transfers to identify and disrupt financial networks that bankroll terrorist activities (Saruni, 2025).

Community Policing

Community policing is a proactive approach that prioritises collaboration between law enforcement agencies and the public to enhance safety, prevent crime, and build trust (Cheruiyot & Wainaina, 2021; Kisio & Wa Teresia, 2024; Nanjala, 2022). The police in Kenya have increasingly adopted technology to strengthen their community policing initiatives. For instance, police have embraced technology in community policing through digital crime reporting platforms such as the Fichua Kwa DCI mobile app (Manana & Otieno, 2022; Shabibi & Lautebatch, 2024) and SMS-based reporting systems that allow citizens to anonymously report suspicious incidents or crimes in their neighbourhoods (Kisio & Wa Teresia, 2024; Manana & Otieno, 2022; Nyaga et al., 2023). In this way, the police can quickly gather intelligence from the community and respond quickly to criminal incidents, which has translated into improved trust between law enforcement and residents (Kandie & Handa, 2024; Manana & Otieno, 2022; Shabibi & Lautebatch, 2024). The toll-free emergency numbers, such as 999, 112, and 911, have also provided direct channels for citizens to report incidents without having to physically visit a police station (Cheruiyot & Wainaina, 2021; Nanjala, 2022).

Besides, many local police stations across Kenya have established WhatsApp groups that connect officers with residents in specific neighbourhoods (Kemboy & Zakayo, 2024). According to Nanjala, (2022), these groups serve as digital platforms for real-time communication through which residents share security concerns (Kemboy & Zakayo, 2024), report suspicious activities (Nanjala, 2022), and receive alerts from the police (Kemboy & Zakayo, 2024; Manana & Otieno, 2022). Community policing groups on WhatsApp in parts of Nairobi, such as Buruburu and Kasarani, have helped the police track down stolen vehicles. They have also helped police to identify suspected criminals and respond quickly to distress calls (Kemboy & Zakayo, 2024; Nanjala, 2022). These platforms have, in that sense, created a sense of collective responsibility for security, making communities more involved in crime prevention.

The Kenya Police Service and the Directorate of Criminal Investigations (DCI) actively use social media platforms such as Twitter, Facebook, and Telegram to engage with the public (Kemboy & Zakayo, 2024; Manana & Otieno, 2022). These agencies issue security advisories, expose wanted criminals, and educate the public on crime prevention measures using these social media platforms. The DCI, for example, has a Twitter account where they frequently post updates about ongoing investigations. They also post about missing persons and fraud schemes, thereby, encouraging the public to provide leads and report suspicious activities (Kemboy & Zakayo, 2024). This has made it easier for the agency to receive community-generated intelligence, translating into successful arrests and crime prevention. Besides, it enhances community policing efforts by allowing the police to take preemptive action before violence erupts (Manana & Otieno, 2022).

Legal and Ethical Issues in Digital Policing in Kenya

Right to Privacy and Data Protection

In Kenya, the right to privacy is a fundamental human right captured in Article 31 of the Constitution. This right guarantees every individual against the unlawful interference of their personal information, home, or communications (Khamala, 2024; Laibuta, 2023). The right is a key consideration for law enforcement agencies using digital policing tools and techniques such as surveillance, biometric identification, and digital tracking to enhance security and crime prevention (KIPPRA, 2024; Laibuta, 2023). Notably, these digital tools pose a significant risk to personal privacy, especially when not properly regulated. In particular, the wide-scale installation of CCTV cameras in urban areas, particularly in Nairobi and Mombasa, has brought with it concerns about privacy breaches (KIPPRA, 2024).

Notably, these privacy issues are premised on questions such as who has access to the footage; how long the data is stored; and whether it is used within the parameters stipulated by the law (Khamala, 2024). These concerns have been based on emerging cases in which surveillance footage has been leaked or used for purposes beyond law enforcement, such as monitoring political opponents (Khamala, 2024; KIPPRA, 2024). There are also reports of police using spyware to access private communications and track the movement of individuals without obtaining the necessary court orders (KIPPRA, 2024; Laibuta, 2023). Such actions have undermined the constitutional rights of the affected individuals and also eroded public trust in the deployment of digital policing tools.

The direct access to mobile phone users' sensitive personal data from mobile service providers has also raised significant privacy concerns. Notably, Safaricom has been blamed for the possible misuse/sharing of customer data in the wake of the June 24th Gen Z protests across the country, which have facilitated abductions and extrajudicial killings by government operatives. The excessive access to personal data by law enforcement officers is a violation of the privacy rights of individuals (Laibuta, 2023; Shabibi & Lautebatch, 2024).

Admissibility of Digital Evidence in Courts of Law

Law enforcement agencies have had to increasingly depend on digital evidence to investigate and prosecute cybercriminals, especially as digital crimes become more sophisticated. However, a major challenge associated with digital evidence is the form of authenticity and integrity of the evidence (Ofwa, 2025; Raburu & Dinga, 2020). Notably, digital data can be easily manipulated, deleted, or altered, which makes it challenging for one to prove its originality in a court of law (Raburu & Dinga, 2020; Rutenberg et al., 2021). The admissibility of digital evidence is premised on strict chain-of-custody procedures that ascertain that the evidence is collected legally, stored securely, and presented without tampering (Raburu & Dinga, 2020; Rutenberg et al., 2021). However, many law enforcement officers lack adequate knowledge and skills in cyber forensics, which often results in the mishandling of critical evidence (Ofwa, 2025; Raburu & Dinga, 2020). This has further caused court cases to lack merit because of the digital evidence that law enforcement officers have presented against the accused persons.

For instance, in *Republic v Mark Lloyd Steveson (2016)*, the High Court refused to admit digital evidence presented by the prosecutor questioning the integrity and proper handling of the electronic data presented (Raburu & Dinga, 2020). The court argued that law enforcement agencies need to adhere strictly to digital forensics protocols to ensure the authenticity and reliability of electronic evidence (Rutenberg et al., 2021). In Ondieki v Maeda (Petition E153 of 2022), the High Court addressed the installation of CCTV cameras in a residential area and argued that that infringed on the privacy rights of residents (Raburu & Dinga, 2020; Rutenberg et al., 2021). The court ruled that the installation of CCTV systems must comply with constitutional privacy protections and the Data Protection Act, and argued that the rights of individuals should not be violated through unlawful surveillance practices (Ofwa, 2025; Raburu & Dinga, 2020).

Effectiveness of Digital Policing Tools

The use of body-worn cameras (BDW) is a welcome addition to the technological toolkit for digital policing in Kenya (Guyo, 2024). However, recent studies have indicated mixed results in terms of its effectiveness in ensuring professionalism in law enforcement. For instance, Lum et al., (2020) found mixed results regarding the impact of BWCs on police conduct, use of force, and citizen compliance. On one hand, BWC reduced complaints against police officers and encouraged professional behaviour, whereas citizens were less likely to escalate confrontation or resist arrest upon knowing that they were being recorded. The study, however, established that the exclusive use of BWC did not guarantee improved policing outcomes. Their effective use was, however, contingent upon other factors such as departmental policies, officer training and development, and the enforcement of protocols for camera usage. In another study, Harrison et al., (2022) also concurred that whereas BWCs could be effective tools for advancing transparency and accountability amongst law enforcement officers, their optimisation is based on factors such as how they are utilised, monitored and the context within which they are implemented.

Besides, whereas facial recognition technology has been adopted by security officers, for instance, to identify traffic offenders in Kenya, its effectiveness generally has been questioned in association with the significant biases that it presents. For instance, in the US, studies have shown that facial recognition algorithms often present significantly higher error rates, particularly when it comes to identifying individuals from minority groups as compared to white citizens (Hill et al., 2022; Johnson et al., 2024; Moraes et al., 2021). This bias has often resulted in discrimination, wrongful arrests (Johnson et al., 2024; Lynch, 2024), and a loss of public trust in law enforcement (Johnson et al., 2024; Moraes et al., 2021). This implies that the Kenyan security authorities need to guard against such biases in the deployment of digital tools, which is highly likely to result in discrimination against minority groups who are often profiled for particular crimes such as terrorism.

Digital policing also demands that security agencies develop and maintain digital repositories of the evidence that they collect regarding detected or reported criminality (Brayne, 2018; Neiva et al., 2023). These repositories, or rather databases, archive vast amounts of sensitive information, which includes personal data, criminal records, surveillance footage, and facial recognition data (Brayne, 2018; Wilson-Kovacs & Wilcox, 2023). Due to the richness of the data they hold, the repositories have become targets of hackers, who present risks to privacy, public safety, and national security. Notably, cyberattacks on law enforcement systems could translate into data breaches, identity theft, and the manipulation of criminal records (Wilson-Kovacs & Wilcox, 2023).

CONCLUSION

Kenya has increasingly adopted technology in all facets of life, and with this, criminals have also leveraged digital tools to advance their nefarious agendas. This demands that law enforcement agencies take up digital tools to counter criminality in all its forms. Digital policing integrates technology, digital tools, and data analytics to enhance law enforcement efficiency, prevent crime, and support public safety. Digital policing involves the use of digital tools, including AI-powered predictive analytics, digital surveillance, cybercrime investigations, digital forensics, surveillance technologies, and mobile policing applications. This has, therefore, required law enforcement agencies to invest in surveillance tools, including body-worn cameras, facial recognition, and IoT devices to improve transparency and situational awareness. They have also leveraged social media monitoring and mobile policing applications to streamline communication and intelligence gathering.

In Kenya, for instance, digital policing reforms have sought to combat corruption and enhance police accountability. This has involved the rollout of initiatives such as the digital Occurrence Book, online police clearance certificates, and cashless traffic fine payments, which have not only engendered efficiency but also reduced bribery and public complaints about security officer conduct. The establishment of the Crime and Incident Reporting System (CIRS) aims to facilitate real-time crime reporting and tracking, and increase transparency and accessibility in the enforcement of law and order.

Despite these numerous advantages that come with digital policing, the methodology also presents significant legal and ethical challenges, with specific regard to privacy and data protection. For instance, cases of leaked surveillance footage and unauthorised tracking undermine constitutional provisions regarding citizen privacy and public trust in law enforcement. Besides, the admissibility of digital evidence in court remains another key issue. Notably, digital data is prone to manipulation and therefore requires strict chain-of-custody protocols.

However, inadequate training in cyber forensics amongst law enforcement officers often leads to the mishandling of evidence, which in turn, waters down prosecution efforts. This is evident considering cases in which courts have ruled against improperly handled digital evidence and urged adherence to forensic standards and privacy laws. Additionally, whereas digital tools such as body-worn cameras (BWCs) are adopted in Kenya to enhance police accountability, their effectiveness will not be automatic. Therefore, law enforcement agencies will have to check on proper policies, training, and enforcement to support the use of BWCs. In sum, without stringent regulation and oversight, digital policing invariably becomes a significant risk against constitutional rights rather than a tool or methodology for improving law enforcement outcomes in Kenya.

Recommendations

Based on the legal and ethical issues raised, this discourse recommends the harnessing of existing legal frameworks, such as the Data Protection Act (2019), to ensure that law enforcement agencies are accountable for how they collect, store, and use digital data. Proper mechanisms should be put in place to ensure that security agencies access and use personal data without violating privacy rights. In this regard, the Office of the Data Protection Commissioner (ODPC) must conduct regular audits; sanction non-compliance and impose fines; and ensure security agencies adhere to the due process when handling personal data. More importantly, law enforcement agencies need to implement privacy-preserving methodologies or technologies such as data anonymisation, encryption, and restricted access controls to minimise risks associated with data handling.

The government should also establish clear policies regarding the use of facial recognition systems, which are enabled by artificial intelligence (AI) and machine learning. Such regulations should require rigorous testing before the deployment of facial recognition technologies to ascertain their accuracy and reliability. This is important considering that biased and incorrect facial recognition could translate into wrongful arrests, misidentifications, and violations of the rights of individuals.

There is also a need to establish an independent oversight body made up of legal experts, technologists, and civil rights advocates to regularly audit AI-based policing tools. The body should be charged with ensuring that the deployed AI policing systems are used in a transparent, explainable, and subject to public scrutiny. They should also ensure that the systems do not reinforce racial, gender, or socioeconomic biases. The oversight function of the body should, therefore, contribute to eliminating chances for flawed AI models to be used, which could entrench discriminatory policing practices.

Besides, Law enforcement agencies in Kenya should develop and implement specialised training programs for law enforcement officers on digital forensics. The training should also equip them with skills in digital evidence collection and preservation. This should include competencies in developing standardised chain-of-custody protocols to ensure the integrity and authenticity of digital evidence in court. The training should also cover the need for collaboration between law enforcement, the judiciary, and forensic experts in terms of the role that each entity plays in the criminal justice system as a way of bolstering the reliability of digital evidence. This will go a long way in improving the admissibility of digital evidence in the prosecution of cases.

Additionally, the subsequent rollout of the BWC should be accompanied by strict enforcement of policies that stipulate how the cameras should be used, including mandatory activation during interactions with civilians. This requires the establishment and implementation of monitoring mechanisms and protocols to prevent officers from tampering with or selectively using BWC footage. More importantly, law enforcement officers need to be provided with adequate training regarding the ethical and procedural use of BWCs.

REFERENCES

Afzal, M., & Panagiotopoulos, P. and. (2024). Data in Policing: An Integrative Review. *International Journal of Public Administration*, 1– 20. https://doi.org/10.1080/01900692.2024.2360586

Akama, M. N. J. (2025). Management of Strategic Change at National Crime Research Centre in Kenya. *International Journal of Arts and Humanities*, *13*(2), 47–58.

Amadou, N. S., Maino, M. R., Massara, M. A., Saiz, H. P., & Sharma, P. (2019). *FinTech in Sub-Saharan African Countries: A Game Changer?* International Monetary Fund.

Anjarwalla, K., & Sugow, A. (2022, June 17). Road to 9/8: Risks Posed by Digitisation of Electoral Processes - The Elephant. *The Elephant*.

https://www.theelephant.info/opinion/2022/06/17/road-to-9-8-risks-posed-by-digitisation-of-electoral-processes/

Arrigo, B. A., & Sellers, B. G. (2021). *The Pre-Crime Society: Crime, Culture and Control in the Ultramodern Age*. Policy Press.

Asser, J., Waiganjo, E., & Njeru, A. (2025). (PDF) Influence of Technology Adoption Interventions on Performance of Selected Commercial State Corporations in Kenya. *Multidisciplinary Journal of Technical University of Mombasa*, *2*(1). https://doi.org/10.48039/mjtum.v2i1.49

Brayne, S. (2018). The Criminal Law and Law Enforcement Implications of Big Data. *Annual Review of Law and Social Science*, *14*, 293–308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839

Campbell, E. (2024). Techno-digital policing: Time, temporalities, timescapes. *Time & Society*, 0961463X241273817. https://doi.org/10.1177/0961463X241273817

Cheruiyot, G. K., & Wainaina, L. (2021). Effect Of Crime Deterrence Strategies On The Control Of Juvenile Gang Crime In Mombasa County, Kenya. *International Academic Journal of Social Sciences and Education*, *2*(2).

Davis, J., Purves, D., Gilbert, J., & Sturm, S. (2022). Five ethical challenges facing data-driven policing. *AI and Ethics*, *2*(1), 185–198. https://doi.org/10.1007/s43681-021-00105-9

Digitali Webbs Services. (2024, November 13). *Crime and Incident Reporting with the Kenya Police: What You Need to Know*. https://digitali.co.ke/crime-and-incident-reporting-with-the-kenya-police-what-you-need-to-know/

Ekanem, S. (2024). Top 5 African countries with the highest number of mobile phones | Pulse Nigeria. *Pulse*. https://www.pulse.ng/articles/business/domestic/african-countries-with-the-highest-number-of-mobile-phones-2024092616481852536

Fussey, P., & Sandhu, A. (2022a). Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, *26*(1), 3–22. https://doi.org/10.1177/1362480620967020

Fussey, P., & Sandhu, A. (2022b). Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, *26*(1), 3–22. https://doi.org/10.1177/1362480620967020

Galis, V., Gundhus, H. O. I., & Vradis, A. (2025). *Critical Perspectives on Predictive Policing: Anticipating Proof?* Edward Elgar Publishing.

Gichana, A. (2023, March 8). The mobile apps spicing up girl-child’s life. *Nation*. https://nation.africa/kenya/news/gender/the-mobile-apps-spicing-up-girl-child-s-life-4150716

Gichohi, J. W., Murimi, D. S., & Owino, D. G. E. (2023). Extent To Which Geospatial Techniques Have Been Integrated In Police Response Strategies For Crime Prevention In Nairobi City County, Kenya. *Reviewed Journal of Social Science & Humanities*, *4*(1), 50–61.

Guyo, K. D. (2024, November 17). Bodycams vital for police reforms. *Nation*. https://nation.africa/kenya/blogs-opinion/opinion/bodycams-vital-for-police-reforms-4827196

Harrison, K., L’Hoiry, X., & Santorso, S. (2022). Exploring the impact of body-worn video on the everyday behaviours of police officers. *The Police Journal*, *95*(2), 363–377. https://doi.org/10.1177/0032258X211000834

Hill, D., O’Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*. https://doi.org/10.1177/14613557221089558

Johnson, T. L., Johnson, N. N., Topalli, V., McCurdy, D., & Wallace, A. (2024). Police facial recognition applications and violent crime control in U.S. cities. *Cities*, *155*, 105472. https://doi.org/10.1016/j.cities.2024.105472

Kandie, D. S., & Handa, S. (2024). Mobile Phone Technology Adoption By The Police As A Counter Terrorism Measure In Nairobi City County, Kenya. *Reviewed Journal of Social Science & Humanities*, *5*(1), Article 1. https://doi.org/10.61426/rjssh.v5i1.199

Kaufmann, M., & Lomell, H. M. (2025). *De Gruyter Handbook of Digital Criminology*. Walter de Gruyter GmbH & Co KG.

Kemboy, L. K., & Zakayo, C. N. (2024). Police Use Of Social Media And Public Trust In Nairobi City County, Kenya. *Reviewed Journal of Social Science & Humanities*, *5*(1), Article 1. https://doi.org/10.61426/rjssh.v5i1.252

Kenya News Agency. (2019, September 8). *Technology instrumental in the fight against crime and drugs, says Regional Commissioner – Kenya News Agency*. https://www.kenyanews.go.ke/technology-instrumental-in-the-fight-against-crime-and-drugs-says-regional-commissioner/

Khamala, C. A. (2024). Digital surveillance and big data: Balancing the rights to privacy and security in Kenya. *African Journal on Privacy and Data Protection*, *1*(1). https://doi.org/10.29053/ajpdp.v1i1.0009

Kimani, B. (2025, January 14). *Gov't to digitise police services by April 2025*. Citizen Digital. https://www.citizen.digital/news/govt-to-digitise-police-services-by-april-2025-n355831

KIPPRA. (2024). *Strengthening Data Protection in Kenya: Opportunities and the Way Forward – KIPPRA*. https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/

Kirui, G. (2024). Enhancing Police Operations: The Impact of CCTV in Monitoring, Incident Response, and Crime Investigation in Nairobi City County, Kenya. *International Journal of Scientific Research and Management*, *12*(5). https://doi.org/10.18535/ijsrm/v12i05.sh01

Kirui, G., Muiya, B., Ochieng, D., & Waithaka, S. (2024). (PDF) Impact of CCTV on Police Operations Outcomes in Nairobi City County, Kenya. *East African Journal of Information Technology*, *7*(1). https://doi.org/10.37284/eajit.7.1.1995

Kisio, B., & Wa Teresia, N. (2024). Ethical Implications of Advanced Surveillance Technologies on Law Enforcement: A Case Study of National Police Service in County of Nairobi, Kenya. *East African Journal of Information Technology*, *7*(1), Article 1. https://doi.org/10.37284/eajit.7.1.1722

Kurgat, P. (2022, December 30). Elgeyo Marakwet County Launches Drones to Combat InsecurityKenyans.co.ke. *Kenyan.Co.KE*. https://www.kenyans.co.ke/news/83587-elgeyo-marakwet-county-launches-drones-combat-insecurity

Laibuta, M. (2023). *Adequacy of Data Protection Regulation in Kenya* (SSRN Scholarly Paper No. 4724788). Social Science Research Network. https://doi.org/10.2139/ssrn.4724788

Lum, C., Koper, C. S., Wilson, D. B., Stoltz, M., Goodier, M., Eggins, E., Higginson, A., & Mazerolle, L. (2020). Body-worn cameras' effects on police officers and citizen behavior: A systematic review. *Campbell Systematic Reviews*, *16*(3), e1112. https://doi.org/10.1002/cl2.1112

Luvembe, A. M., & Mutai, H. (2019). Big Data Framework for Kenya's County Governments. *Journal of Computer and Communications*, *9*(1).

Lynch, N. (2024). Facial Recognition Technology in Policing and Security—Case Studies in

Regulation. *Laws*, *13*(3), Article 3. https://doi.org/10.3390/laws13030035

Makong, B. (2023, September 12). Govt moves to expedite issuance of certificates of good conduct. *Capital News*. https://www.capitalfm.co.ke/news/2023/09/govt-moves-to-expedite-issuance-of-certificates-of-good-conduct/

Manana, R. W., & Otieno, N. (2022). Drones Operations in Kenya: Perspectives on Privacy Challenges and Prospects. *Air and Space Law*, *47*(1). https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\AILA\AILA2022005.pdf

Mangi, G. Z., & Kandiri, J. (2024). Technology And Intelligence Led Policing In Nairobi City County, Kenya. *Reviewed Journal of Social Science & Humanities*, *5*(1), Article 1. https://doi.org/10.61426/rjssh.v5i1.219

Matara, E., & Kariuki, A. (2021, April 6). Police to use drones to arrest lockdown violators. *Nation*. https://nation.africa/kenya/counties/nakuru/police-considering-use-drones-arrest-lockdown-violators--3350424

Miruka, G. (August 23). How security agencies can use ICT to fight terrorism. *Nation*. https://nation.africa/kenya/blogs-opinion/blogs/how-security-agencies-can-use-ict-to-fight-terrorism-4345086

Montasari, R., Carpenter, V., & Masys, A. J. (2023). *Digital Transformation in Policing: The Promise, Perils and Solutions*. Springer Nature.

Moraes, T. G., Almeida, E. C., & de Pereira, J. R. L. (2021). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. *AI and Ethics*, *1*(2), 159–172. https://doi.org/10.1007/s43681-020-00014-3

Mukiri-Smith, H., & Leenes, R. (2024). Beyond the 'Brussels Effect'? Kenya's Data Protection Act (DPA) 2019 and the European Union's General Data Protection Regulation (GDPR) 2018 | Request PDF. *ResearchGate*. https://doi.org/10.21552/edpl/2021/4/7

Mulika Kenya. (2025). *Mulika Kenya*. Mulika Kenya. https://mulikakenya.co.ke/

Mutung'u, G. (2021, July 30). Kenya's transition to digital ID not without risks. *Research ICT Africa*. https://researchictafrica.net/2021/07/30/kenya-risks-in-transformation-of-a-national-identification-system-to-digital-id/

Mwende, S. (2025). PS: Starting April, you'll not physically visit police stations to report incidents. *The Star*. https://www.the-star.co.ke/news/realtime/2025-01-14-ps-starting-april-youll-not-physically-visit-police-stations-to-report-incidents

Nanjala, W. B. (2022). *Influence Of Social Media On National Security In Kenya, 2014-2022* [United States International University-Africa]. https://erepo.usiu.ac.ke/bitstream/handle/11732/7712/Wanjala%20Brenda%20Nanjala%20MIR%202022.pdf?sequence=1&isAllowed=y

Neiva, L., Machado, H., & Silva, S. (2023). The views about Big Data among professionals of police forces: A scoping review of empirical studies. *International Journal of Police Science & Management*, *25*(2), 208–220. https://doi.org/10.1177/14613557231166225

Noor, A. S. M., Sanusi, S. S., & Rahim, N. H. A. (2020). A survey of big data and data mining techniques for crime prevention. *COMPUSOFT: An International Journal of Advanced Computer Technology*, *9*(11), Article 11.

Nyaga, B. M., Ondego, J. C., & Joel, M. (2023). *Mediation and Data Protection Law in Kenya: Appraising ADR for Optimal Access to Justice under the DPA 2019* (SSRN Scholarly Paper No. 4424688). Social Science Research Network. https://doi.org/10.2139/ssrn.4424688

Odhiambo, J. (2024, March 25). How Kenya can harness AI power to curb road carnage.

Business Daily. https://www.businessdailyafrica.com/bd/data-hub/how-kenya-can-harness-ai-power-to-curb-road-carnage--4568252

Ofwa, J. (2025). Analysis of Digital Evidence Admissibility in the Administration of Justice in Kenya: An Implication of Sexual Offenses Crime. *International Journal Of Law Management & Humanities*, *7*(5). https://ijlmh.com/wp-content/uploads/Analysis-of-Digital-Evidence-Admissibility-in-the-Administration-of-Justice-in-Kenya.pdf

Pepper, I., & McGrath, R. (2025). *Introduction to Professional Policing: Examining the Evidence Base*. Routledge, Chapman & Hall, Incorporated.

Raburu, G., & Dinga, L. (2020). Legal Issues in Computer Forensics and Digital Evidence Admissibility. *International Journal of Computer Science and Mobile Computing*, *9*(7), 86–89.

Rutenberg, I., Kiptinness, S., & Sugow, A. (2021). Admission of electronic evidence: Contradictions in the Kenyan Evidence Act. *Digital Evidence and Electronic Signature Law Review*, 35– 49. https://doi.org/10.14296/deeslr.v18i0.5280

Saruni, J. L. (2025). Influence of Intelligence Data Utilization in Crime Prevention in Nairobi City County, Kenya | The International Journal of Business & Management. *The International Journal of Business & Management*, *12*(10). https://www.internationaljournalcorner.com/index.php/theijbm/article/view/173947

Shabibi, N., & Lautebatch, C. (2024, October 29). Exclusive: How Kenyan police use mobile phones to track, capture suspects. *Nation*. https://nation.africa/kenya/news/exclusive-how-kenyan-police-use-mobile-phones-to-track-capture-suspects-4804416

Sila, B. M., & Mutuku, M. (2024). (PDF) Determinants of smartphones adoption and use at Kenya Airport Police Unit, Kenya. *International Journal of Research in Business and Social Science*, *12*(5), 486–493. https://doi.org/10.20525/ijrbs.v12i5.2684

Sugow, A., Zalo, M., & Rutenberg, I. (2021). Privacy and Data Protection Practices of Digital Lending Apps in Kenya. *Journal of Intellectual Property and Information Technology Law*, *1*(1), 131–169.

Tanui, D. K., & Barmao, C. K. (2016). Use of ICT in the Detection and Prevention of Crime in Kenya. *Journal of Information Engineering and Applications*, *6*(9), 62–71.

Walubengo, J., & Mutemi, M. (2018). Treatment of Kenya’s internet intermediaries under the Computer Misuse and Cybercrimes Act, 2018. *The African Journal of Information and Communication*, *21*, 1–19. https://doi.org/10.23962/10539/26114

Wasonga, M., & Ombiro, W. (2019, February 1). *Will drones and UAVs unriddle insecurity in Kenya?* CIO Africa. https://cioafrica.co/will-drones-and-uavs-unriddle-insecurity-in-kenya/

Wilson-Kovacs, D., & Wilcox, J. (2023). Managing Policing Demand for Digital Forensics through Risk Assessment and Prioritization in England and Wales. *Policing: A Journal of Policy and Practice*, *17*, paac106. https://doi.org/10.1093/police/paac106

Xu, Z., Cheng, C., & Sugumaran, V. (2020). Big data analytics of crime prevention and control based on image processing upon cloud computing. *Journal of Surveillance, Security and Safety*, *1*(1), 16–33. https://doi.org/10.20517/jsss.2020.04