

Research Article

Examining the Significance of the Phelemero Digital Platform Concept of Community Policing on Use of Technology for Investigation of Crime in Malawi

David Kumwenda^{1, 2, *} , Thokozani Andrew Chazema¹ , Dorah Kaunda² 

¹Transformative Community Development Agrisciences, Mzuzu University, Mzuzu, Malawi

²Lilian Precious Dorah Phelemero Consultancy, Mzuzu, Malawi

Abstract

By 2029 Africa anticipates to have about 1, 1 billion projected internet users. Technology integrates Africans on formal informal and non-formal initiated digital surveillance projects for socialization and interaction promoting collaboration and coordination rallying wide participatory successful transaction. The storage replication and dissemination of data in online transactions, data is often processed and stored in unsecured online storage areas, leading to the leaking of both personally identifiable information and data promoting cybercrimes. Protection of data is integral to the digital economy, ensuring ethical use. This study examines the significance of the Phelemero Digital Platform concept of community policing on advanced technology use for prevention and detection of crime in Malawi through literature survey and local observation. Findings reveal that the Phelemero Digital platform concept of community policing shows multiplicity technology perceptions (a) store, replicate, and disseminate information (b) facilitate citizens' integrate formal informal and non-formal on initiated digital surveillance projects (c) anticipated challenges on the use of technology for security (d) enhanced citizens' engagement to digital monitoring and surveillance (e) provide improved channels of communication, alternative ways to gain transparency, revolutionize transform and amplify the customary bureaucratic procedures providing real-time evidence analysis (f) Portrays willingness to digital Literacy empowerment (g) Shows the spirit of citizen participation (h) Shows technology integration can facilitate collaborative leadership (i) Overcoming Traditional Policing Challenges (j) Reveals Contextual Relevance in Malawi. Right of privacy in use of advanced technology for national security is guided by Section 21 (c) of Malawi Constitution through enforcement of Malawi Data Protection Act which promotes (1) Protection of Citizens' Privacy & Rights (2) Fair, Transparent, and Accountable Data Handling (3) Legal & Institutional Oversight (4) Promoting Trust and Confidence (5) Supporting Digital Economy & International Alignment (6) Human Rights Dimension and (7) Mitigating Risks of Data Breaches & Abuse. The Possible Challenges of enforcing the Malawi Data Protection Act are (i) awareness and capacity (ii) resources for Enforcement (iii) balancing with other rights and needs (iv) and cross-border data flows. Value contribution to body of knowledge is that the Phelemero Digital platform concept of community policing gives the interpretation that technology has capacity to integrate citizen at formal informal and non-formal initiated digital surveillance projects defeating the cynical withdrawal due to formal customary bureaucratic procedures as outlined in Participatory Democracy and Social Disorganization Theories. Technology promotes wide citizen participation promoting transparency and accountability in public matters hence reducing corruption.

*Corresponding author: davidkumwenda441@yahoo.com (David Kumwenda)

Received: 17 October 2025; **Accepted:** 29 October 2025; **Published:** 9 December 2025



Copyright: © The Author(s), 2025. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

Keywords

Digital Platform Concept of Community Policing, Integration, Formal Informal and Non-formal, Privacy, Transformative and Revolutionary Channels of Communication

1. Introduction

The use of technology has gained humans with versatile digital platform for formal informal and non-formal socialization and interaction that have helped people to claim for various rights including right to safety [15]. Technology has promoted strong integration reducing people's cynical withdrawal thereby encouraging citizens' rally for responsible actions to collaborate and coordinate with law enforcement agents with an aim to manage neighbourhood security [11, 12]. Digital platform of community policing has improved wide participatory transaction [15]. This article examines the

significance of the Phelemero Digital Platform concept of community policing on the use of advanced technology for prevention and detection of crime in Malawi.

The article answers three questions (1) What is the Phelemero Digital Platform concept of community policing (2) What is the significance of the Phelemero Digital Platform concept of community policing. (3) How can the right of privacy be dealt with in using technology for national security.

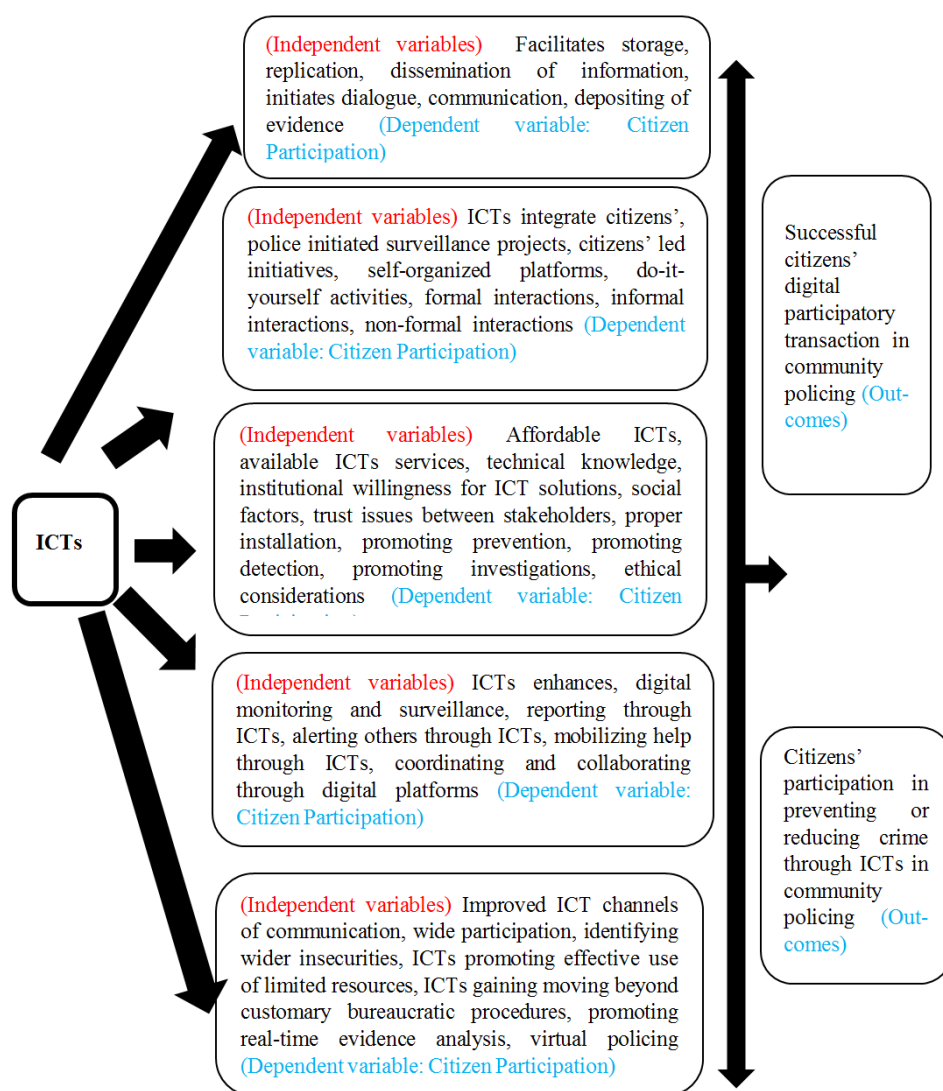


Figure 1. Phelemero Model of digital platform of community policing.

2. The Phelemero Digital Platform Concept of Community Policing

Kumwenda (2025) analysed five published papers from a research *“Investigating citizens’ participation through information communication technology in community policing in Muloza, Malawi”* to come up with an ontology-driven conceptual modelling (ODCM) in the subject of ICT-community policing [28]. The analysis followed the process of thematic analysis which came up with the Phelemero Digital Platform concept of community policing thereby increasing knowledge paradigm and improving the epistemological rigour of the conceptual model in research [9, 21]. The Phelemero Digital platform concept of community policing being ontology-driven conceptual modelling is a higher quality models compared to models that follow the traditional conceptual modeling (TCM) technique [28], and is advantageous for more challenging and advanced facets of ICT community policing because it is able to depict multiplicity digital platform use and interpretation for community policing thereby increasing ICT-community policing knowledge paradigm [27].

Below is the Phelemero digital platform concept of community policing:

Figure 1 above is the Phelemero Digital Platform concept of community policing which assumes that the availability of ICTs will help citizens store, replicate and disseminate information. This will facilitate citizens to initiate dialogue, communication and deposit evidence.

Furthermore, the ICTs will facilitate citizens’ to integrate into police initiated surveillance projects, citizens’ led digital initiatives, self-organized platforms and do-it-yourself activities to manage security in the neighbourhoods. The citizens will be able to interact in both formal, informal and non-formal procedures.

These above transactions will be made possible if ICTs are available, affordable. The citizens’ must also have technical knowledge on how to use, there must also be institutional willingness to sustain the projects. Moreover, social factors that include, context, distribution, ethical compliances as well as environmental consideration must be well managed.

If the above conditions are met ICTs will enhance citizens’ engagement to digital monitoring and surveillance that may promote sharing of information, reporting of rights violations, alerting neighbours of threats, mobilizing coordination and collaborating virtually to manage neighbourhood security.

All the above will also depend on ICTs being able to provide improved channels of communication, ICTs that will provide alternative ways to gain transparency, ICTs that will offset for lack of resources, ICTs that will revolutionize transform and amplify the customary bureaucratic procedures providing real-time evidence analysis and promoting virtual policing.

Such a digital platform conceptual model of community

policing will gain citizens successful digital participatory transaction that promotes citizens to claim the right to security, social cohesion, collective efficacy and community guardianship thereby supporting Peel’s “modern policing” principles of involving citizens to prevent or reduce crime.

3. Significance of Phelemero Digital Platform Concept

The Phelemero digital platform concept of community policing in this paper reveals that technology has potential to bring revolutionary and transformative initiative on leveraging Information and Communication Technology (ICT) to enhance public safety, citizen engagement, and law enforcement efficiency. Rooted in the principles of community policing, the platform empowers citizens to actively participate in security matters, fostering a collaborative approach to crime prevention and resolution. Key Significance of the Phelemero Digital Platform of community policing are as follows:

3.1. Shows Enhanced Storage Replication and Dissemination of Information

The Phelemero Digital platform concept of community policing shows that technology has larger capacity to store replicate and disseminate information. Literature on advanced use of technology reveal that research results by Catarina et al. [2] point out that the use of technology facilitates taking digital images, recording and sharing videos, writing messages and interacting using voice notes promotes virtual coding and processing of data. Study results by Catarina et al. [2] and Khan & Rizvi, [10] underscore the point that the virtual coding and processing of data promotes the process of Datafication.

The implication is that when images, videos, messages and voice notes have been digitized into technology the data will be (1) Stored (2) replicated and (3) disseminated giving police authority to detect, investigate crimes. Therefore, advanced technology can help police manage public security efficiently and effectively. However, this article calls for more research on how police may effectively and efficiently use the stored, disseminated and replicated data for investigations in Malawi.

Much as Catarina et al, [3] supports the notion that the capacity of technology to store, replicate and disseminate information can help improved health care and law enforcement administration. Although literature shows that technology helped detecting movements of clients through Contact tracing applications in Health care, and suspects were detected through (FRT) to verify identities, remotely and in real-time in security. This paper suggests scholars to conduct more research to examine how technology such as mounted CCTV cameras connected to data base may help detect crime

in CBDs of Lilongwe, Blantyre, Mzuzu and Zomba in Malawi cities. The findings may help to create robust ICT tracking systems that may enable the possibility to track individuals by collecting direct or indirect information on how suspects move through the world [3].

As much as Catarina et al. [2] and Khan & Rizvi [10] argue that advanced technology are tools that can potentially assist public authorities in law enforcement, leveraging both surveillance and dataveillance. The article argues that although The Phelemero Digital platform concept of community policing shows that technology facilitates storage replication and dissemination of information, scholars need to do more research in Malawi to validate the argument. Similarly, although Yasmine et al. [30] contend the assertion that people perceive advanced technology protecting them and offering a range of security benefits, the article suggests more research to validate the claim in Malawi.

Although literature supports the assumptions by the Phelemero Digital Platform concept of community policing that codification and datafication promotes storage replication and dissemination of information. Thereby allowing both digital surveillance and dataveillance allowing people to deposit as well as share evidence on right violations. There is need for more civic education to the masses starting from secondary schools students to university students as well as practitioners on the assumptions of the concept for progressive adoption and adaptation.

3.2. Depicts Real-time Integration and Wide Participation

The Phelemero Digital Platform concept of community policing shows that technology has the potential to integrate citizens from all sectors of society ranging from individual to groups and global socialization and interaction. This kind of integration can take place in many forms starting at formal, informal and non-formal levels thereby promoting prompt wide socialization and interaction. Technology facilitates real-time integration of authorities, citizens to solve community related issues.

- 1) By practical observations, public security administration has always deliberately come up with technology initiatives that facilitate citizens to join the police initiated surveillance and dataveillance projects for the purposes of preventing and detecting crime. Although this kind of initiative is more oriented to allow Citizens and police integrate on Police initiated surveillance projects for the purposes of preventing and tracking criminal activities, but it is mostly to be described as Formal integration [10, 15]. This article suggests more research on applicability of the Phelemero Digital Platform concept related to such formal initiated surveillance and dataveillance in Malawi.
- 2) Apart from formal Police initiated surveillance and dataveillance projects to monitor security in society,

divergent thinkers in exercising the right to security and expression have preferred to interact by themselves on community related issues. In supporting principles of community oriented policing, where people take charge of their security affairs prompt Citizens to come up with initiatives promoting digital monitoring and surveillance forming WhatsApp groups Facebook charts etc. for easy community mobilization to resolve certain observed issues [12]. Although this kind of socialization and interaction promotes wide citizen participation on citizen led initiated surveillance projects but still the deliberations on these digital forums are Informal and non-formal integration in nature [10, 14]. This article argues that this kind of socialization and interactions are parallel oversight to manage checks and balances on power abuse by public security authority. The study argues more studies on what kind of informal and non-formal integrations the Phelemero Digital Platform concept offer does to Malawians.

- 3) Practical example could be during the 2025 Malawi General election results tallying process, it has been observed that technology facilitated informal and non-formal integration of citizens, various private Television Broadcasting stations, Radio Broadcasting stations, Political Party tally centres to rally citizens groups and organizations to share analysed results from polling stations all over the country through digital storage dissemination and replication in comparison with Malawi electoral official tallying and verification of results apart from official declaring the winner as mandated MEC. By analysing the Phelemero Digital Platform concept is shows that technology allowed wide participation in the tallying of election results improving transparency and accountability thereby reducing an element of corruption. The Phelemero Digital Platform concept signal that people are watching and there is need to be cautious on following procedures to maintain transparency and accountability to allow credibility of results.
- 4) Evidence shows that technology has the capacity to improve social cohesion, collective efficacy and community guardianship. All these years when technology was at the novice stage or rather when there was marginalization on the service availability and affordability to use of advanced technology, physical social integration relied on people of similar interests. Although evidence shows advanced technology has allowed people of all statuses and nationalities including every age in a society to be part of the community through digital integration, this article argue more research to validate how the Phelemero Digital Platform concept ignites citizens on improving social cohesion, collective efficacy and community guardianship through digital integration.

Although evidence through literature review validates

theory that technology is able to facilitate strong socialization and interaction on informal and non-formal manners allowing individuals, groups as well as community manage strong digital integration without demographic boundaries. Sociologically, evidence depicts that technology has modernized simplified transformed and revolutionized global socialization and interactions defying national boundaries, age, statuses through Tik-Tok, WhatsApp, and Facebook. Practically, the observation is that a Malawian is able to see how Captain Ibrahim Traore is influencing his country and this sends messages to any foreign intentions to safeguard their intended offensive intervention against a sovereignty of Burkina faso.

3.3. Portrays Willingness to Digital Literacy Empowerment

The Phelemero Digital platform concept of community policing is able to reveal the challenges that affect the use of technology in the prevention and detection of crime. Although literature from some studies such as Catarina et al. [2] reveal that there is need for collaborative leadership through digital platform to integrate various data base stakeholders for enhancing national security in Malawi to defeat challenges of technology. Other scholars claims that use of technology faces numerous challenges and amongst them are distribution and affordability for security like;

- 1) Inequality distribution of digital services [2].
- 2) Biased deployment of CCTV Cameras [2].
- 3) Avoiding the point of letting every person in public place becoming a suspect over planted FRTs [2].

However, the Phelemero Digital Platform concept of community policing gives the motivation that technology has larger significance in facilitating digital interactions and socialization in the modern life. The concept gains public authorities the willingness to align institutions to adopt to the use of technology. Thereby, inspiring citizens to start learning on how best and ethical to utilize technology. Literature from studies conducted by William et al. [29] reveal that there must be an awareness to authorities and the people that digital service availability influences people to participate in digital interactions and socializations. Similarly, results from research conducted by Smit et al. [25] reveal that digital service affordability promotes people's spirit of utilizing the technologies for digital interactions and socialization. On the contrary, research findings from studies conducted by Oliveira & Garcia [18] conclude that lack of knowledge about digital service availability and affordability thwarts people's spirit of using the available and affordable technologies.

Promoting the willingness to digital literacy empowerment influences stakeholders to have the ambition of investing in buying need to have technology and not nice to have technology [19]. Digital literacy empowerment helps fight the challenges of distribution and marginalization by tackling

through understanding the factors that affect the use of technology for the prevention and detection of crime [13].

3.4. Shows the Spirit of Citizen Participation

The Phelemero Digital platform concept of community policing shows that there is direct communication between citizens and law enforcement, enabling real-time reporting of crimes, sharing of security concerns, and submission of evidence such as photos and videos. This digital interface encourages broader community involvement, including marginalized groups, in the policing process. Studies indicate that such platforms can increase transparency, accountability, and trust between the police and the community [11-14].

3.5. Depicts Revolution and Transformation of Improved Channels of Communication

The Phelemero Digital Platform concept of community policing shows that ICTs facilitates integration that depicts transformed and revolutionized channels of communication through use of software and hardware of advanced technology.

While finding by Khan & Rizvi [10] indicate that technology has really transformed and revolutionized communication for prevention and detection of crime through the use of biometrics to improve security. Khan & Rizvi [10] continue to argue that the use of Biometrics in technology is frequently used by a safety company to identify, authenticate and regulate access purposes. However, in Malawi there is no evidence of how useful is use of biometrics to trace suspect person in criminal cases based upon their thumbprint, voice/face identification and medical necessity for a criminal investigation amidst claims that technology hardware and applications can be made compatible to identify unrecognized corpses and also detecting possible crimes [10].

Khan & Rizvi [10] further point out that the broad demands on community safety nudged the expansion of the use of biometric face recognition databases and systems, which is explicitly and convincingly justifies in terms of efficiency in fulfilling a specific security and safety purpose. The rising investment in face recognition technology is required to propel the business over the passage of time. Embracing modern technology and innovation is always encouraging and necessary in the social and national security of the country. This article contends the above assertion by agreeing that the Phelemero Digital Platform concept reveal that digital platform has the potential to empower, transform citizens to take charge of their security.

Catarina et al. [2] argue that although the Phelemero Digital Platform concept promises a lot but use advanced technology by law enforcers must always meet ethical legal standards to avoid abuse of power when using advanced technology on the public.

3.6. Shows Integration Can Facilitate Collaborative Leadership

Apart from integration issues facilitated by technology Kumwenda et al. [11] argues more on technology helping to improve storing replication and dissemination of information in policing. Furthermore, Kumwenda [15] contends that technology has the power to integrate individuals, public institutions as well as government departments to citizen led surveillance projects, police initiated surveillance projects to improve prevention and detection of crime in community policing in Malawi. The Phelemero Digital platform concept of community policing depicts that technology has potential to facilitate integration that may improve collaborative leadership from various departments that may be team players for ICT-community policing for national security. Gausi [6] and Ngwenya [22] in Malawi laments the absence of an overarching national information policy on information services resulting into lack of collaborative leadership on national security. In turn, these issues have affected economic development of Malawi.

The Phelemero Digital platform concept of community policing depicts that the versatility of technology spearheads collaborative leadership as well as creating an overarching digital database in digital community policing that may boost national security. Khan & Rizvi [10] support the notion of integration for collaborative leadership and creating an overarching digital database for national security by reporting that integrating with different existing database of criminals and technology like CCTV footage may help further analyzing accurate analysis and information exchange in the interest of criminal investigations. For example, In China CCTV Cameras through biometrics face recognition helps identify accused of minor offences including Jay walking or humiliating people in public (walking in pajamas). After arrival of FRT in India, criminal investigations have become convenient for LEA.

Ismail et al. [8] report that community driven surveillance enhances report accuracy and collective responsibility, resulting in enhanced drug-related arrests. Advanced technology facilitates real-time communication between public and law enforcement and may promote safety and accountability. Simbeye & Kumari [24] reveal that integration through advanced technology promotes collaborative leadership that is managed through digital forums that increase collaborative problem solving.

Ismail et al. [8] claim integration of various public service departments will provides collaborative leadership with capacity for real-time datafication surveillance and dataveillance improving digital monitoring for preventing and detecting crime in community policing. Khan & Rizvi [10] argue that innovative mobile based & web based programs can be useful in preventing and verification of documents in speedy mode. Mapping technology of facial recognition vigil assist prison administration for crowd management and ap-

propriate compliance of social distancing norms among prisoners. Also helps preventing and detecting any kind of illegitimate practices occurred among prisons. Useful in identifying crime professionals and victims of human trafficking. Missing persons. And different kinds of organized crimes.

Evidence from literature review suggest that integrating multidisciplinary database connected to vigil facial recognition technology in public places in Malawi, may greatly assist border posts detect transactions of money laundering, receiving stolen property and false asset declaration. Where there is element of conspiracy and inadequacy of different direct evidence or eye witness to specific crime [2]. With above development and advantages over use of integrated database for national security Catarina et al. [2] questions on how much power can be handed to AI systems, but also how can we ensure that the power given to the public authorities over individuals will be used exclusively in their best interest.

Despite research based evidence in Malawi about collaborative leadership through digital integration, the article argues the Phelemero Digital platform concept of community policing displays the potential of using advanced technology to integrating databases from key institutions like NRB (National Registration Bureau), MRA (Malawi Revenue Authority), MPS (Malawi Police Service), RTD (Road Traffic Directorate), Immigration, hospitals, MEC (Malawi Electoral Commission), Ministry of Education, TNM, and Airtel Malawi would provide a rich, interconnected data ecosystem that could dramatically enhance AI-driven investigations in Malawi [2]. The integration of all the mentioned departments will support the notion of digital monitoring by means of datafication surveillance and dataveillance which among other things will benefit law enforcement agents to benefit tracking stolen devices, investigating breaches of law, and overall national security [2].

The paper contends that digital integration promotes electronic data storage replication and dissemination thereby promoting data coding dataveillance and Surveillance. Therefore, integrating NRB, MEC, Immigration, and mobile provider databases: *Stolen Phones/Computers*: AI can trace ownership via SIM card registration (linked to NRB), usage patterns, and GPS data. Even if the device is resold, its reactivation can trigger alerts. *Fake Identities*: AI can cross-reference national IDs, passports, and SIM card data to flag identity inconsistencies or fraud. *Suspect Movement*: Immigration and RTD data can be used to track suspect movement across borders or via vehicle ownership/registration [2, 10, 15].

- 1) By linking mobile operators (TNM, Airtel) with law enforcement and immigration: AI can geolocate stolen devices or suspects based on cell tower triangulation or GPS. Communication patterns (metadata, not necessarily content) can help trace criminal networks. SIM swapping, multiple IMEIs, and suspicious re-registrations are flagged automatically [2, 10, 15].

- 2) MRA, banks, and vehicle registration (RTD) can be cross-referenced: AI can detect illicit wealth accumulation or property purchases inconsistent with declared income (money laundering, tax evasion). Links stolen goods to the wider criminal economy (e.g., device smuggling rings) [2, 10, 15].
- 3) With access to education, hospital, and police data: AI can profile repeat offenders (mental health records, prior criminal cases, disciplinary issues). Predict high-risk zones or individuals based on data fusion (e.g., youth dropouts from Ministry of Education + high-crime areas). AI can map social graphs and identify gang affiliations, cross-border networks, or terrorism risks [2, 10, 15].
- 4) Via MEC, Immigration, and NRB: Prevent electoral fraud by verifying voter ID, death records (to prevent ghost voting), and dual registration. AI flags anomalies like underage registration, repeated votes, or biometric mismatches [2, 10, 15].
- 5) Police investigations become faster and more accurate — AI can generate suspect lists, vehicle traces, and asset maps in minutes. Helps automate investigation leads, e.g., if a stolen laptop pings a TNM tower with a new user linked to NRB data [2, 10, 15].
- 6) Everything from device IMEIs to education credentials can be validated through digital records. AI can detect fake academic records or employment fraud (e.g., forged university degrees or fake hospital work history) [2, 10, 15].
- 7) AI systems can monitor for unusual behaviors (like bulk SIM registrations, erratic movement at borders, black-listed IMEIs being reused) [2, 10, 15].

Integrating these databases enables a holistic, AI-powered investigative framework that boosts efficiency, accuracy, and speed in solving phone theft cases, while also reinforcing the role of community policing in Malawi's digital age [15].

Yasmine et al. [30] report that the hybrid approach not only improves sentiment classification accuracy but also effectively processes large volumes of data in real-time. CCTV systems and AI automate the analysis of video footage, identifying suspicious behaviors and predicting areas at higher risk of crime. AI has further enhanced these capabilities, enabling more sophisticated models and analyze complex datasets, including real-time CCTV footage, demographic data and environmental factors. The article suggests more practical research on the topic of collaborative digital integration and how this may improve national security in Malawi.

3.7. Overcoming Traditional Policing Challenges

The platform addresses challenges such as limited physical presence of law enforcement in remote areas by providing a virtual space for reporting and communication. This is

particularly important in regions with scarce resources, as it allows for continuous engagement and monitoring.

3.8. Contextual Relevance in Malawi

In Malawi, where community policing has been a cornerstone of law enforcement since 1997, the Phelemero Digital Platform concept represents a modern evolution of this approach. It aligns with existing initiatives like Community Policing Forums and Neighbourhood Watch Groups, enhancing their effectiveness through digital means. The integration of ICT into community policing not only modernizes the approach but also addresses the unique challenges faced in rural and underserved areas.

In brief, the Phelemero digital platform conceptual model of community policing is a pivotal development in Malawi's community policing strategy. By harnessing the power of ICT, it bridges the gap between citizens and law enforcement, fostering a collaborative environment for addressing security concerns. This initiative not only enhances public safety but also contributes to the broader goals of social cohesion, resource optimization, and community empowerment. Furthermore, it is helping to show that collaborative digital integration may help to fill knowledge gaps in following areas (1) Cross-Sector Data Interoperability: No detailed explorations of linking databases across departments. (2) Collaborative Frameworks: Few studies outline how different institutions could share data, insights, or workflows in coordinated ways. (3) Technology Infrastructure: Beyond mobile apps, there's limited discussion on integrated backend systems and governance structures. (4) Impact Evaluation: Further research could measure how true multi-departmental data integration influences crime rates, response times, and community trust.

4. Dealing with the Right of Privacy in the Use of Technology

While the Phelemero Digital Platform concept shows that use of technology has helped to improve citizen's integration at formal, informal and non-formal levels influencing participatory democracy reducing the challenge of cynical withdrawal of people from claiming of their rights [15]. The promotion on use of technology must not overlook at challenges of privacy [2]. Catarina et al. [2] reveal that adopting AI-powered surveillance systems expose population to an increased risk of power imbalance, based on the enabling of access to privileged information, on individuals' private lives collected within and feeding systems to provide intel to the public authorities, while the output information may be extremely relevant to predict, prevent and neutralize societal threats, it pushes the boundaries of personal privacy and bestows an immense amount of power on public authorities over individuals, which may lead to the undermining of democratic values and individual rights and liberties.

4.1. Malawi Data Protection Act

Section 21(c) of Malawi Constitution; *“Every person shall have the right to personal privacy, which shall include the right not to be subject to – (c) interference with private communications, including mail and all forms of telecommunications”*. In the management of the above right in Malawi, the Data Protection Act was enacted in 2024, assented to on 1 February 2024, and came into force shortly afterwards. It provides a legal framework for protection of personal data (for natural persons), regulating how it’s collected, processed, stored, shared, and moved. It designates the Malawi Communications Regulatory Authority (MACRA) as the Data Protection Authority (DPA), giving it oversight responsibility.

- 1) *Part 1*: Looks at preliminary of the Act and this explains the Application of the Data Protection Act.
- 2) *Part 2*: Looks at the administration that includes; designation of data protection authority, functions of the authority, and power of the authority, advisory committees.
- 3) *Part 3*: Looks at principles relating to the processing of personal data and it includes; personal data to be processed lawfully, fairly, etc., purpose limitation, data minimization, data accuracy, storage limitation, data integrity and data confidentiality, principles for determining the validity of consent, provision of information to a data subject, provision of information to a data subject, processing of sensitive personal data, processing personal data of children and other legally incapacitated persons, and processing of personal data relating to criminal offences, convictions etc.
- 4) *Part 4*: Looks at the rights of a data subject and this include; right to access personal data, right to data portability, right to rectification of personal data, right to erasure of personal data, right to restriction of processing personal data, right to object, and automated decision making, derogations.
- 5) *Part 5*: Looks at duties of a data controller and a data processor and they include; adherence to data protection principles, technical and organizational measures, record of personal data processing activities, data protection impact assessment, joint data controller, regulation of the relationship between data controller and data processors, designation of data protection officer, and duties of data protection officer.
- 6) *Part 6*: Looks at data security that include; security of personal data, and notification of personal data breach to data subjects.
- 7) *Part 7*: Looks at cross border transfers of personal data and this include; cross-border transfer of personal data, adequacy of protection of personal data, and binding corporate rules, and certification mechanisms.
- 8) *Part 8*: Looks at registration of data controllers of major importance and data processors of major importance and

this include; registration of data controllers of significant importance and data processors of significant importance.

- 9) *Part 9*: Looks at complaints and this include; complaints, suspension or cancellation of registration, exemptions, and compliance orders.
- 10) *Part 10*: Looks at miscellaneous and this includes; appeal against decisions of the authority, civil remedies, obstruction interference with the authority, breach of confidentiality, offences committed by legal persons, firms etc., vicarious liability, regulations, and transitional provision.

4.2. Key Significances of Data Protection Act

4.2.1. Protection of Citizens’ Privacy & Rights

It ensures that individuals (data subjects) have rights over their personal data—rights such as accessing, correcting, or deleting their data, being informed how their data is used, and objecting to certain processing. This helps prevent abuses (unauthorized use, exposure, discrimination, etc.). Sensitive personal data (e.g. health, religion, ethnicity, biometric data, and political opinions) receives extra protection. Processing such data usually requires explicit consent [23, 26].

4.2.2. Fair, Transparent, and Accountable Data Handling

The Act introduces principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, integrity and confidentiality. Data controllers and processors are obliged to implement technical and organisational measures to protect data (e.g. security, preventing unauthorized access or leaks) [23, 26].

4.2.3. Legal & Institutional Oversight

Establishment of a Data Protection Authority gives Malawi a body to monitor compliance, enforce the law, handle complaints and data breaches. It also is responsible for issuing guidelines, raising awareness, and engaging stakeholders. The Act also prescribes penalties for non-compliance and demands registration of certain data controllers/processors, especially those of “significant importance” (i.e. handling large volumes or sensitive data) [23, 26].

4.2.4. Promoting Trust and Confidence

For citizens, knowing that there is a legal regime protecting their personal data builds trust in using digital services (banks, healthcare, e-government, mobile services etc.). For private sector, having clarity about duties and legal expectations helps design their systems better, avoid legal risk, reduce potential reputational harm from data breaches [23, 26].

4.2.5. Supporting Digital Economy & International Alignment

Helps create an enabling environment for digital innovation, e-commerce, and other tech-based services. Protection of personal data is increasingly a condition for cross-border business and data transfers. Aligning with international norms (GDPR-like or other global data protection standards) helps Malawi trade, attract investment, and collaborate more confidently with external partners who require such protections [23, 26].

4.2.6. Human Rights Dimension

The right to privacy is recognised as a fundamental human right. The Act expressly treats data protection not just as technical/security matter but as a human rights issue [23, 26].

4.2.7. Mitigating Risks of Data Breaches & Abuse

In an era with frequent cyberattacks, identity theft, misuse of data for fraud, or manipulation of personal information, having formal legal standards helps reduce vulnerabilities. The law obliges entities to notify authorities (and potentially affected persons) in case of breaches, so mitigation can happen [23, 26].

4.3. Possible Challenges of Data Protection Act

While it's very positive overall, there are some challenges or things to watch out for:

4.3.1. Awareness & Capacity

Because the law is new, many entities (private and public) may not yet fully understand their obligations. Training and awareness campaigns are necessary.

Kumwenda [15] argue that there is need for researchers to do more research on mitigating factors over misuse and abuse of information communication technology and Artificial Intelligence. For example, citizens must be sensitized about the Data Protection Act as well as offences that may be committed when using information communication technology under the Malawi electronic transaction Act 2016, such as section 78, administering domain name without authority. Section 83, search warrants by courts. Section 84, unauthorized access, interception or interference with data. Section 85, child pornography. Section 86, prohibition of cyber harassment. Section 87, prohibition of offensive communication and many more as guided by section 21 of Malawi Constitution.

4.3.2. Resources for Enforcement

The DPA needs sufficient resources (skilled staff, technical capability, budget) to effectively monitor compliance, investigate breaches, apply penalties.

4.3.3. Balancing with Other Rights & Needs

For example, between privacy and legitimate public interests (security, public health, law enforcement). There will need to be clear rules or exemptions.

4.3.4. Cross-border Data Flows

As data increasingly moves across national boundaries, ensuring safe cross-border transfers is complex. Malawi's law will need to provide mechanisms for that.

Findings in a study by Bronstein [1] in the Republic of South Africa argue that the absence of collaborative governance mechanisms in the Data Protection Act (POPIA) constitutes a missed opportunity to build a culture of enhanced data protection in South Africa. The Information Regulator has the task of giving many exemptions and prior approvals under the Act. The newly constituted Information Regulator will find itself exposed as it faces a particularly difficult mandate.

Similarly, results by Netshakhuma [17] in the Republic of South Africa showed that most of the participants were not aware of the POPIA, lack of collaboration between the legal practitioners, records managers and archivist. Internal control systems with Information Communication Technology (ICT) need to be in place to provide information integrity and the value of international integrity with regard to the international students and staff. The Social implications is that if The POPIA is not properly implemented, can contribute to the violation of information integrity of the international students with regard to research and cultural exchange programme. Furthermore, it can affect SA trade relations with the European countries as it is a requirement for non-European countries to comply with the European Union General Data Protection Regulations (GDPR).

Similarly, findings match with results in a study by Chimboza and Smith [3] in The Republic of South Africa that lack of technical measures to combat the abuse of personal information, limited awareness of the implications of POPIA compliance on organisations, and organisations' resource constraints are some factors that exacerbate the complexity of the regulatory environment. Through interviews in seven organisations, including tourism, banking, retail, healthcare, fintech, and technology, the study found that POPIA compliance affects organisations at the people, process, and technological levels.

Research findings by Raji et al. [20] reveal that in Africa comparing the enforcement approaches among different African countries, the findings can shape future regional policy and data protection practices.

Study findings in Kenya by Juma & Faturoti [7] and Deo Shao et al. [4] indicate that Kenya has achieved measurable progress in data protection enforcement whereas Nigeria is still grappling with foundational issues. Despite these contrasts, both countries show alignment with global data protection norms such as the GDPR, offering a foundation for growth. The paper recommends targeted strategies to

reinforce enforcement, including increasing institutional autonomy, expanding public education efforts, and building stronger technical capacity. Similarly, Modilim et al. [16] in Nigeria, findings reveal that while the NDPA significantly strengthens Nigeria's data protection regime through the establishment of the independent Nigeria Data Protection Commission (NDPC), expanded data subject rights, and formalized cross-border data transfer protocols, substantial challenges remain in regulatory independence, judicial efficiency, and emerging technology governance. The article concludes by proposing forward-looking policy recommendations to enhance Nigeria's digital privacy framework, particularly in addressing AI governance, cyber-security integration, and global data flow adequacy requirements to position Nigeria as a regional leader in data governance.

Study findings by Ochang et al. [5] show that institutions that make or create data and monitor governance laws beyond data protection, that can generate evidence-based research for data governance and that can facilitate Findable, Accessible, Interoperable, Reusable (FAIR) data are lacking in Africa. They also demonstrated that whereas data protection regulations are gaining traction in Africa, most established institutions created to monitor compliance and enforcement are yet to operate independently of government control. This lack of independence grossly affects effectiveness at different levels. Furthermore, the findings show that both private and public data-driven entities that should apply data governance principles to their processing workflows are yet to establish data governance roles within their organisations.

5. Conclusion

In conclusion, current study findings on Phelemero Digital platform concept of community policing underscores the fact that future developments may include the creation of “Smart cities”, where integrated ICT systems help law enforcement and citizens manage community policing activities that may range from managing, detecting and preventing crime through the use of sensors and connected infrastructure. Such systems would provide real-time data to officers, improving the coordination of emergency responses. The value contribution of the Phelemero Digital platform concept of community policing is that it reveals the versatility of technology whereby technology has the capacity to integrate citizens at formal informal and non-formal levels on various virtual platforms ranging from police led initiated surveillance projects, citizen led initiated surveillance projects as well as do-it-yourself activities that promote storage replication and dissemination of information that allows wide participation facilitating global digital socialization and interaction allowing people claim for their rights. In this case technology allows building social cohesion, collective efficacy and community guardianship promoting transparency and accountability thereby helping to reduce corruption. The Phelemero

Digital platform concept shows that technology has power to rally citizens to participate in claiming for their security rights moving away from cynical withdraw as speculated by Participatory Democracy theory. Furthermore, technology has power to integrate people on formal informal and non-formal participatory transactions drifting away from assumptions and criticisms of the Social disorganization Theory that emphasized on formal aspects of official interactions. The Phelemero Digital platform concept of community policing supports the notion that technology provides improved channels of communication that gain transparency and accountability promoting wide participation that helps to reduce corruption.

Abbreviations

ACENUB	African Centre of Excellence in Neglected and Underutilized Biodiversity
DPA	Data Protection Authority
GDPR	General Data Protection Regulations
LPDP	Lilian Precious Dorah and Phelemero
Consultancy	Consultancy
MACRA	Malawi Communications Regulatory Authority
MEC	Malawi Electoral Commission
M of E	Ministry of Education
MPS	Malawi Revenue Authority
MRA	Malawi Police Service
NDPC	Nigeria Data Protection Commission
NRB	National Registration Bureau
ODCM	Ontology-driven conceptual modelling
POPIA	Protection of Personal Information Act
RTD	Road Traffic Directorate
TCM	Traditional Conceptual Modelling
TNM	Telecom Network Malawi

Acknowledgments

The author thanks all the co-authors for their time to contribute to the article and all the cited authors for their contribution to the body of knowledge in the subject.

Author Contributions

David Kumwenda: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Writing – original draft, Writing – review & editing

Thokozani Andrew Chazema: Validation, Writing – review & editing

Data Availability Statement

This literature review did not use data.

Conflicts of Interest

The authors have no conflict of interest.

References

- [1] Bronstein V (2022) "Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the *Protection of Personal Information Act*" *PER / PELJ* 2022(25) - <http://dx.doi.org/10.17159/1727-3781/2022/v25i0a11661>
- [2] Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan, Christoph Lütge (2022) AI-powered public surveillance systems: why we (might) need them and how we want them. <https://doi.org/10.1016/j.techsoc.2022.102137>
- [3] Chimboza, Tendani and Smith, Erin, (2024) "How Does Compliance with the Protection of Personal Information Act (POPI Act) Affect Organisations in South Africa?" (2024). African Conference on Information Systems and Technology. 19. <https://digitalcommons.kennesaw.edu.acist.2024.presentations.19>
- [4] Deo Shao, Fredrick Ishengoma, Anastasija Nikiforova and Mrisho Swetu (2025) Comparative analysis of data protection regulations in East African countries. *DIGITAL POLICY, REGULATION AND GOVERNANCE* VOL. 27 NO. 4 2025, pp. 486-501, Emerald Publishing Limited, <https://www.researchgate.net.38>
- [5] Eke, D., P. Ochang, A. Adimula, F. Borokini, S. Akintoye, R. Oloyede, L. Sorborikor, M. Adeyeye, B. Wale-Oshinowo, T. Ogundele. 2022. Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs. Centre for the Study of African Economies (CSEA). <https://cseaafrica.org.images.posts.PDF>
- [6] Hambani Gausi (2012). The effects of the brittle national information policy framework on information services in Malawi. Submitted in fulfillment of the requirements of the Master's Degree in Library and Information Science (MLIS), Department of Library and Information Science, Faculty of Social Sciences and Humanities, University of Fort Hare. <https://scispace.com.papers.ef>
- [7] Isaac Juma & Bukola Faturoti (23 May 2025): Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice, *International Review of Law, Computers & Technology*, <https://doi.org/10.1080.13600869.2025.2506918>
- [8] Ismail, Felecia, Azizah, A. K., & Rahmawati, D., (2025) Integrating Smart Monitoring Systems in Urban Drug Abuse Prevention: A Case Study in Jakarta. *West Science Social and Humanities Studies* Vol. 03, No. 04, April 2025, pp. 490-500. <https://doi.org/10.58812/Wsshs.v3i04.1819>
- [9] Jaakkola, E., 2020, 'Designing conceptual articles: four approaches', *AMS Review* (2020) 10: 18–26, viewed 30 Dec 2023, <https://doi.org/10.1007.s13162-020-00161-0>
- [10] Khan, Z. A., & Rizvi, A., (2021) AI based facial recognition technology and criminal justice: issues and challenges. *Turkish Journal of Computer and Mathematics Education* Vol. 12 No. 14 (2021), 3384-3392. <https://doi.org/10.17762/turcomat.v12i14.10923>
- [11] Kumwenda, D., Tembo, M., Mphande, C., Benard, S., Nalivata, C., Nundwe, V., Chazema, T. A., Ngilazi, H. & Kalinga, M., (2023 A) "Digital Community-Policing Application at Muloza Border of Malawi and Mozambique in Mulanje", *ijmst*, vol. 10, no. 2, pp. 3138-3147, Aug. 2023. <https://doi.org/10.15379.ijmst.v10i2.3069>
- [12] Kumwenda, D., Tembo, M., Mphande, C., Nundwe, V., and Chazema, T. A., (2023 B). "Digital Mystery: Enhanced Active Citizens' Participation Through Information Communications Technology in Community Policing", *ijmst*, vol. 10, no. 2, pp. 4062-4073, Aug. 2023. <https://doi.org/10.15379.ijmst.v10i2.3309>
- [13] Kumwenda, D., Tembo, M., Ahmad, Z., Mphande, C., Kaunda, D., et al. (2024). Future Role of Digital Platform of Community Policing in Malawi. *American Journal of Networks and Communications*, 13(2), 84-96. <https://doi.org/10.11648.j.ajnc.20241302.11>
- [14] Kumwenda, D., (2025). Examining the Versatility and Misuse of Information Communication Technology in Community Policing in Malawi. *International Journal of Information and Communication Sciences* 2025, Vol. 10, No. 1, pp. 13-22. <https://doi.org/10.11648.j.ijics.20251001.12>
- [15] Kumwenda, D. P., (2025). (Draft Thesis) *Investigating citizens' participation through information communication technology in community policing in Muloza, Malawi*. A thesis submitted to the Faculty of Environmental Sciences, Department of Agri-sciences in fulfillment of the requirements for the award of Doctor of Philosophy Transformative and Community Development. Mzuzu: Mzuzu University.
- [16] Modilim, S. N., Bolarinwa, I., Omidiora, M. T. and Tawo, O., (2024). Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment. *International Journal of Law Management & Humanities* Volume 7 | Issue 6 2024, Page 2481 – 2495. <https://doi.org/10.10000.IJLMH.119827>
- [17] Netshakhuma, N. S., (2019). Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). *Global Knowledge, Memory and Communication* Vol. 69 No. 1/2, 2020 pp. 58-74. © Emerald Publishing Limited 2514-9342 <https://doi.org/10.1108/GKMC-02-2019-0026>
- [18] Oliveira, C. and Garcia, A. C. B. (2019) 'Citizens' electronic participation: a systematic review of their challenges and how to overcome them', *Int. J. Web Based Communities*, Vol. 15, No. 2, pp. 123–150. <https://doi.org/10.1504/IJWBC.2019.10020619>
- [19] Purdy, D. W., (2013). Community Policing Theoretical Problems and Operational Issues. In Verma, A., Das, D. K., & Abraham, D. M., (Ed). *Global Community Policing. Problems and Challenges*. New York: Taylor & Francis Group, pp. 41-62. https://www.routledge.com.Verma-Das-Abraham_book

- [20] Raji, M., Wilder, D., Ugwuoke, V. & Bashir, M., (2025) 'An assessment of the enforcement mechanisms in African data protection laws' (2025) 2 *African Journal on Privacy & Data Protection* 1-40 <https://doi.org/10.29053.ajpdp.v2i1.0002>
- [21] Recker, J., 2010, 'Conceptual Model Evaluation. Towards more Paradigmatic Rigor, viewed 12 Jun 2023, <https://www.researchgate.net/publication.27464397>
- [22] Reuben Paulos Ngwenya (2015) Collaborative leadership among security actors to achieve sustainable national security and prosperity in Malawi: a practical framework prosperity in Malawi: <https://ub-ir.bolton.ac.uk.doctoral>
- [23] Samuel-Okon, A. D., Olateju, O. O., Okon, S. U., Olaniyi, O. O., and Igwenagu, U.T.G.I., (2024). Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence. *Archives of Current Research International* Volume 24, Issue 5, Page 612-629, 2024; Article no. ACRI.118733 <https://doi.org/10.7934/acri/2024/v24i5735>
- [24] Simbeye, C. & Kumari, D., (2024). Reform Initiatives in the Malawi Police Service Strategies to Rebuild Public Trust and Operational Efficiency: A Review. *International Journal of Management Issues and Research*. Volume 13, Issue 1, Jan-Jun 2024, pp. 107-118. <https://doi.org/10.69711/sharda.ijmir.v13i1.2408>
- [25] Smit, A., Swart, J., and Broersma, M., (2024) Bypassing digital literacy: Marginalized citizens' tactics for participation and inclusion in digital societies. *New media & society* 1–19. <https://doi.org/10.1177.14614448231220383.journals>
- [26] Taylor, M., Haggerty, J., Gresty, D., Wren, C., and Berry, T., (2022) Avoiding the misuse of social media by employees, *Network Security*, Volume 2016, Issue 5, 2016, Pages 8-11, [https://doi.org/10.1016.S1353-4858\(16\)30047-2](https://doi.org/10.1016.S1353-4858(16)30047-2)
- [27] Torreano, J. (2021) *How research consultants can encourage students intellectual and ethical development*. In Torreano, J. and O'Kelly, M. (2021) *Training research consultants. Aguide for academic libraries*. New York: Association of College and Research Libraries. <https://scholarworks.gvsu.edu.cgi.viewcontent.PDF>
- [28] Verdonck, M., Gailly, F., Pergl, R., Guizzardi, G., Martins, B., and Pastor, O., 2018, 'Comparing traditional conceptual modeling with ontology-driven conceptual modeling: An empirical study, viewed 30 Dec 2024. <https://doi.org/10.1016/j.is.2018.11.009>
- [29] Williams, K., Markwardt, S., Kearney, S. M., Karp, J. F., Kraemer, K. L., Park, M. J., Freund, P., Watson, A., Schuster, J., and Beckjord, E., (2021). Addressing Implementation Challenges to Digital Care Delivery for Adults With Multiple Chronic Conditions: Stakeholder Feedback in a Randomized Controlled Trial. *JMIR Mhealth Uhealth* 2021 | vol. 9 | iss. 2 | e23498. <https://doi.org/10.2196/27996>
- [30] Yasmine Ezzeddine, Petra Saskia Bayerl & Helen Gibson (2023) Safety, privacy, or both: evaluating citizens' perspectives around artificial intelligence use by police forces, *Policing and Society*, 33: 7, 861-876, <https://doi.org/10.1080.10439463.2023.2211813>