

Privacy risks from massive data flows in 5G networks across Africa: Balancing surveillance implications with individual rights in developing economies

Akibu Abiodun Oni *

Department of Management Studies, Lagos State University, PMB 0001, LASU Post Office, Lagos State, Nigeria.

Global Journal of Engineering and Technology Advances, 2025, 23(03), 362-379

Publication history: Received on 25 April 2025; revised on 23 June 2025; accepted on 27 June 2025

Article DOI: <https://doi.org/10.30574/gjeta.2025.23.3.0191>

Abstract

The deployment of fifth-generation (5G) wireless networks across African nations represents a transformative technological advancement that promises unprecedented connectivity, economic growth, and digital innovation. However, this technological revolution simultaneously introduces substantial privacy risks stemming from massive data flows, heightened surveillance capabilities, and inadequate regulatory frameworks in developing economies. This research examines the multifaceted privacy challenges emerging from 5G implementation across Africa, analysing the tension between state surveillance interests and individual privacy rights. The study evaluates the current state of data protection legislation across 54 African countries, revealing significant disparities in regulatory maturity and enforcement capabilities. Through comprehensive analysis of 5G network architecture, data flow mechanisms, and privacy vulnerabilities, this research identifies critical gaps in protection frameworks that expose African citizens to unprecedented surveillance risks. The investigation incorporates quantitative data on 5G rollout statistics, sectoral applications, and economic projections spanning 2025-2030. Findings indicate that while 5G technology offers substantial economic benefits projected at \$712 billion by 2050, the accompanying privacy risks remain largely unaddressed in most African jurisdictions. The research reveals that only 28 countries have enacted comprehensive data protection legislation as of 2025, leaving significant populations vulnerable to privacy violations. The analysis demonstrates that sustainable 5G deployment in Africa requires simultaneous advancement of privacy protection infrastructure to prevent the emergence of surveillance states that undermine democratic principles and individual freedoms.

Keywords: 5G Networks; Privacy Rights; Surveillance; Data Protection; Africa; Developing Economies; Telecommunications; Digital Rights; Network Security

1. Introduction

1.1. Background and Context

With the introduction of fifth-generation network, the telecommunications environment in the world has been profoundly changed. African countries have adopted the 5G as a driver of economic growth and digitalization. Historically, the telecommunications industry in the continent has been under-developed with respect to infrastructure installations and adoption of technologies. Nevertheless, in the last few years, there has been a faster growth in 5G infrastructure investment in several African states. Reports on the industry as collected in 2025 indicate that there are 54 million 5G connections in Africa, which is 3.8 percent of the total number of mobile users (Sutherland, 2018). This number is small in comparison with the world rates, but it is the start of significant technological change. The African Union and regional economic communities have listed the use of 5G as the key element of infrastructure to attain development goals in the continent expressed in Agenda 2063. Commercial 5G services have begun with

* Corresponding author: Akibu Abiodun Oni.

telecommunications operators in such countries as South Africa, Egypt, Nigeria, Kenya, and Tanzania, and network coverage is quickly growing in urban areas.

The economic effects of the implementation of 5G in Africa are enormous and extensive. The industry estimates expect the 5G technology to add 10 billion dollars to African economies by the year 2030, and the figure is projected to grow to 712 billion dollars by the year 2050 (Sutherland, 2018). These economic advantages come out of the improved productivity in several spheres such as agriculture, healthcare, manufacturing, transportation, and the safety of people. The technology has facilitated creative uses like accuracy farming, telemedicine, intelligent production systems, autonomous companies, and technologies of intelligent civil safety systems. Fixed wireless access services are currently available in 25 telecommunications operators with their monthly revenue ranging between 26 and 90 dollars per user (Sutherland, 2018). Growth in the technology sector due to implementation of 5G is estimated to be 185 billion by the year 2025 with an addition of 230 billion by the year 2030.

Nevertheless, the immediate introduction of 5G networks in African countries is taking place in the conditions of the presence of underdeveloped regulatory frameworks, inadequate privacy safeguards, and dictatorial tendencies in a variety of jurisdictions. There are also technological possibilities presented by the 5G architecture that create unparalleled opportunities of mass surveillance, data gathering, and privacy invasion (Adeyeye and Mungai, 2024). The mobile networks 5G are unlike the previous generations because they can handle huge amounts of data, accommodate millions of connected devices at a time within a square kilometer, and allow tracking users and objects with centimetre-level accuracy. Figure 2 illustrates the overall architecture of 5G networks as represented in the perspective of public safety by the National Institute of Standards and Technology, where there is direct device-to-device communication, multi-hop communication, multi-vehicle communication, sensor network, ultra-dense small cells, beamforming functionalities, and vehicular communication as combined to become one network infrastructure (Khan, Kumar, Jayakody, and Liyanage, 2019).

1.2. Research Problem and Significance

The main research problem discussed in the study is the conflict between technology and privacy in the African context. Although 5G has significant economic and social advantages, its implementation in jurisdictions that have poor privacy regulations poses great dangers to personal liberty and democratic administrative procedures. The research problem is presented in various dimensions such as the technical weaknesses, lack of regulations, surveillance, as well as insufficient enforcement processes. The issue of the African governments is how to increase the economic benefits of the 5G deployment but at the same time ensure citizens against privacy violations and abuses of surveillance (Ouma, Wamukoya, and Muthee, 2025). This is an especially pressing problem in emerging economies where resources to execute regulatory control are scarce and the governance frameworks might be focused more on the security than on the rights of an individual.

The existing academic literature focuses a great deal on the 5G security issues in the context of the developed countries but offers little discussion on the privacy issues in relation to the African developing economies (Ijaz, 2024; Khan et al., 2019). The primary attention of the research that is available deals with technical insecurity vulnerability such as authentication vulnerabilities, limitations, and possibilities of exploitation of protocols. Nevertheless, the socio-political aspects of 5G Privacy threat in the settings with weak rule of law, limited judicial independence, and authoritarian tendencies of government are under-researched. This study fills this gap by considering the interplay of 5G implementation with certain African political, legal, and social circumstances to generate unique privacy problems. In analysing privacy risks, the investigation considers such factors as colonial legacies, post-independence governance structures, resource constraints, capacity limitations, and regional diversity.

1.3. Objectives and Research Questions

This study relies on multiple interconnected goals to gain an advantageous insight into privacy hazards in African 5G networks in a very comprehensive way. The main task is to report and review the existing situation of 5G rollout in the African nations, infrastructure building, legislation, and barriers to rollout. The second goal will look at the legislative environment of protecting data in the continent, and how the legislations have been inconsistent, revealing gaps concerning the same. The study will also seek to determine privacy hazards brought about by 5G network structure and operational features in African settings. The other important goal is to examine the implications of surveillance by the deployment of 5G technology in jurisdictions that practice different governance systems and have dissimilar rights protection. Lastly, the study aims to come up with moderate policy superiorities that safeguard privacy without excluding positive 5G applications in emerging economies.

The investigation is guided by several research questions that structure the analytical framework.

- What privacy risks are inherent in 5G network architecture, and how do these risks manifest in African deployment contexts?
- What is the current state of data protection legislation across African countries, and how adequate are existing frameworks for addressing 5G privacy challenges?
- How do African governments utilize 5G networks for surveillance purposes, and what legal frameworks govern such surveillance activities?
- What balance can be achieved between legitimate security interests and individual privacy rights in African 5G deployments?
- What policy interventions, technical safeguards, and regulatory mechanisms can effectively protect privacy while enabling beneficial 5G applications?

1.4. Scope and Limitations

This study includes an extensive analysis of the privacy concerns of the 5G implementation in the African continent. Its geographical coverage is the entire 54 African countries, depending on the depth of analysis according to the available data and the level of 5G deployment. Attention is paid to countries that have made the most efforts to deploy 5G in the continent such as South Africa, Egypt, Nigeria, Kenya, and Tanzania. The time frame is mainly between 2020 and 2025, which is the first stage of the rollout of 5G and the future is expected to be 2030 depending on the industry forecast. Thematic space includes technical, legal, political, and social aspects of privacy in 5G networks, and considers an interdisciplinary approach that incorporates the views of telecommunications engineering, law, political science, and human rights.

Several limitations constrain this research and warrant acknowledgment.

- First, the rapid pace of 5G deployment means that data and statistics may become outdated quickly, limiting the temporal validity of specific findings.
- Second, limited transparency regarding surveillance practices in many African countries constrains empirical investigation of actual government monitoring activities.
- Third, proprietary nature of telecommunications infrastructure and network operations limits access to technical details that would enable more granular privacy risk assessment.
- Fourth, significant variation across African countries in governance systems, legal frameworks, and development levels complicates continental-level generalizations.
- Fifth, the nascent state of 5G deployment in many African countries means that some privacy risks remain theoretical rather than empirically documented.

2. Evolution of Mobile Networks and 5G Technology Architecture

2.1. Historical Development of Mobile Network Generations

The Mobile telecommunications evolution has a history of about forty years starting with the first-generation analog systems in the 1980s. The above evolution can be visually represented (Figure 1) to show the chronological maturation of the technologies that started with 1G to 5G systems and the devices and some of the main technical specifications of the respective generations. First-generation networks, which were implemented in the 1980s as demonstrated in Figure 1, were based on the analog method of transmission, and only enabled simple voice communication networks at a transmission rate of about 2 kilobits per second (Wajdi et al., 2024). The geographical coverage of 1G networks was only limited to the urban regions in the developed world, with little coverage in the African countries.

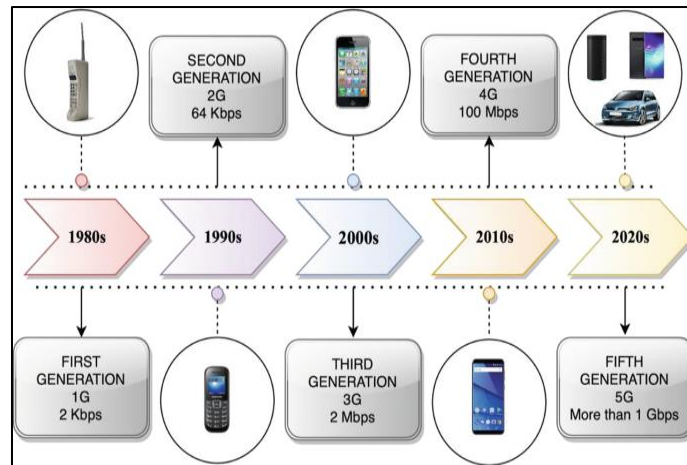


Figure 1 Evolution of mobile network generations

2.2. Technical Architecture of 5G Networks

Fifth-generation wireless technology is a paradigm shift in the network structure and not a simple enhancement on the systems used in 4G. The 5G network has a technical architecture that has several ground-breaking aspects, which made it different as compared to the older generations. Figure 2 shows the holistic structure of 5G networks as reported in the public safety views by the National Institute of Standards and Technology and represents the cumbersome incorporation of various communication modalities and network components (Khan et al., 2019). Figure 2 architecture is a direct device-to-device communications that allow devices to communicate without the need to go through base stations, multi-hop communications that involve data passing through several intermediate nodes, multi-vehicular communications serve connected and autonomous vehicles, large-scale sensor network integration to Internet of Things applications, ultra-dense cell networks with small cells spread across coverage domains, and beamforming functions that direct signals to the intended recipients (Khan et al., 2019).

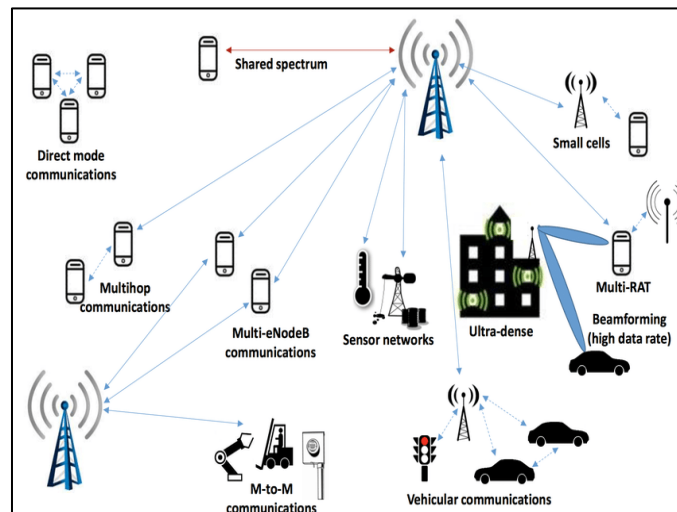


Figure 2 5G network architecture as illustrated in Public Safety Perspective: A 5G Worldview by National Institute for Standards and Technology

Radio access network 5G architecture uses the developments in antenna technologies such as massive multiple-input multiple-output antenna with hundreds of antenna elements. These arrays of antennas make it possible to use beamforming techniques to send radio signal straight to the destination instead of being omnidirectional. This form of targeted transmission is more efficient in the use of the spectrum, improves the data rates, and minimises the interference, at the same time allowing a more accurate location tracking of the devices and users (European Parliamentary Research Service, 2022). The 5G new radio interface can be used on various frequency bands as sub-6 gigahertz to cover extensive areas and millimeter wave frequency bands between 24 and 100 gigahertz to support ultra-high-speed transmission in high-density urban areas. The millimeter wave Spectrum is an enormous band width that

allows transmission speeds of multi-gigabits and has a low propagation range and penetration of obstacles. In turn, the use of millimeter waves presupposes the high density of small cells spaced by 100 to 200 meters in cities as depicted in Figure 2.

The fundamental design of the 5G systems is based on the principles of cloud-native network architecture that is quite unlike in earlier generations. In contrast to 4G networks which are constructed based on specific hardware appliances, 5G core networks apply network functions as software applications that execute on commodity computing infrastructure (Ijaz, 2024). This is a software-defined networking model that allows dynamically allocating resources, deploying services fast and flexibly managing networks. Network function virtualization enables operators to create, scale and move network functions based on demand trends and service demands. Service-based architecture presents network capabilities using application programming interfaces and allows third-party developers to develop novel services using network functions.

2.3. 5G Network Capabilities and Performance Metrics

Fifth-generation networks have provided the network performance improvements in a variety of dimensions relative to the technologies that came before. The highest data rates that 5G systems can support are 20 gigabits per second on the downlink and 10 gigabits per second on the uplink, which is 20 times higher than the 4G LTE-Advanced systems (Wajdi et al., 2024). Such theoretical peak rates permit the usage of 8K video streaming, virtual reality, augmented reality, and cloud gaming. More to the point, to most users, the average user experience on 5G networks range in 5G networks of over 100 megabits per second down and 50 megabits per second up, is a consistent high-performance network throughout the coverage area. The spectral efficiency of the 5G systems is 30 bits/sec/Hz downlink and 15 bits/sec/Hz uplink, three times the spectral efficiency of 4G networks.

3. Current State of 5G Deployment Across Africa

3.1. Regional Rollout Statistics and Growth Projections

The roll out of 5G networks in the African continent has gained pace in significant ways since its first commercial rollouts in 2020. Figure 6 is a detailed summary of the statistics and outlook of 5G implementations in Africa between 2025 and 2030 based on the 2022-2025 industry reports as quoted by Sutherland (2018). There are around 54 million 5G connections in Africa in total, with over 54 million shown at the end of 2025, as illustrated in the current state section of Figure 6, which is a 3.8 percent proportion of the total mobile users in the region. Figure 6 also shows that 5G services are already deployed in 29 countries in Africa, and 14 other countries are also intending to roll out 5G services soon. The data presented in Figure 6 depicts that 5G spectrum has been allocated to telecommunications operators by 28 countries by 2025 (Sutherland, 2018).

3.2. Leading Countries in 5G Implementation

Several African countries have become continent leaders in 5G implementations in terms of network coverage, subscriber uptake, and sophistication in the 5G services. Egypt has the highest level of the 5G market in Africa and has more than 5 million 5G connections as of 2025 as shown in the regional leaders' section of Figure 6, and this is thanks to its massive investment in infrastructure by various operators (Sutherland, 2018). The nation assigned 5G spectrum on various bands such as the 3.5 gigahertz and 26 gigahertz frequencies which allow a wide area of coverage and high-capacity services in the city. Egyptian operators have rolled out 5G networks in major cities such as Cairo, Alexandria and Giza, and plan to expand the network to national scale by 2027. South Africa, which is shown in Figure 6 as the top Sub-Saharan development market, is the next top 5G market with extensive network coverage in larger metropolitan regions (Sutherland, 2019).

Among the large 5G markets in Africa as shown in Figure 6, Nigeria is the largest potential 5G market in Africa in terms of population size and number of mobile subscribers of more than 200 million (Sutherland, 2018). In 2022, Nigeria's operators began 5G services and after the spectrum auctions brought significant revenue to the government. By the year 2025, Nigeria has recorded approximately 3 million 5G connections that will be concentrated in Lagos, Abuja, and Port Harcourt. Infrastructure issues affecting the country are irregular electricity supply, security issues in certain areas and lack of fibre optic backhaul to facilitate network growth. However, the economic relevance of Nigeria and the high number of young people make it a key market to African 5G development. The two countries mentioned in Figure 6 as technology-based economies, Kenya and Tanzania, stand as the pioneers in 5G implementation in the East African region, and both nations begin commercial services in 2023 (Sutherland, 2018).

3.3. Sectoral Applications and Economic Impact

The economic potential of 5G implementation in Africa is reflected in the variety of applications in sectors and productivity. Figure 7 shows the distribution of economic value creation by the 5G technology of the 5G enabled digital world based on the analysis of global deployment pattern adjusted to the African realities (European Parliamentary Research Service, 2022). The 5G applications to the energy and utility sector contribute the most economic value to the economy 19 percent, as shown in Figure 7. With smart grids, electricity generation and distribution can be monitored and controlled in real-time to minimize losses and enhance reliability in power systems which are constantly characterized by lack of capacity and poor management. The advantages of massive sensors implemented on 5G connections allow water utilities to use the leak system and remotely read the meter, as well as optimize the distribution network.

4. Data Protection Legislative Landscape in Africa

4.1. Regional Overview of Data Protection Laws

The law-making framework in protecting data privacy and protection in Africa is highly heterogeneous with countries in significantly different levels of legislation and enforcement. By 2025, 28 African nations will have passed extensive data protection laws, and 26 nations do not have specific privacy laws (Clifford Chance, 2025). Figure 3 offers the geographical illustration of African nations that have legislation on data protection, so the year of the enactment or drafting of the respective statute in the region is presented on the continent (Data Protection Africa, 2024). Countries where comprehensive data protection laws are enforced include South Africa that was enacted in 2013, Mauritius in 2017, Burkina Faso in 2013, Senegal in 2008, Tunisia in 2004, Morocco in 2009, Egypt in 2020, Kenya in 2019, Uganda in 2019, Rwanda in 2021, Ghana in 2012, Nigeria in 2020. Figure 3 uses color encoding to identify those countries that do not have enacted laws on protection as shown in gray color, countries that have enacted laws in protection shown in blue color, countries that enacted laws in protection shown in orange color, countries that enacted laws in protection but still have not yet implemented them as shown in light orange color, and countries that have enacted laws in protection but has not implemented the laws as shown in light blue.

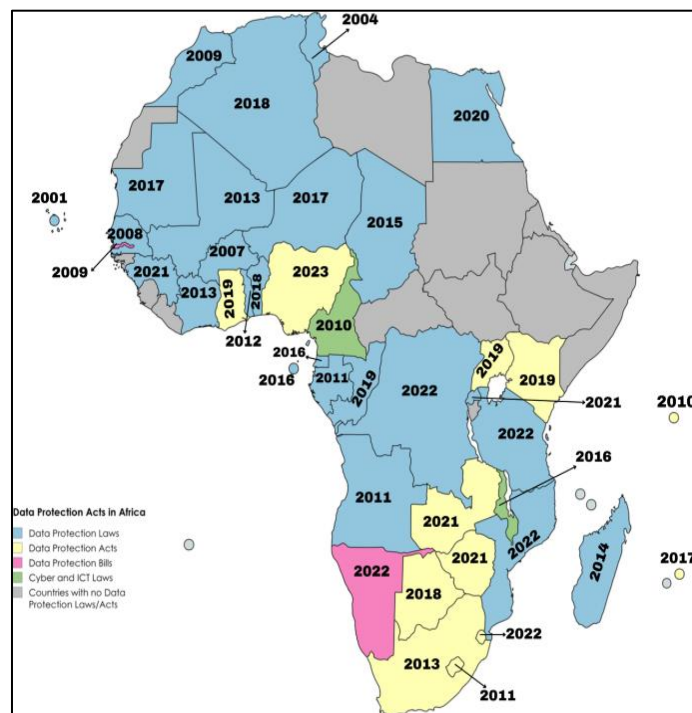


Figure 3 Representation of African countries with data protection legislation/statutes and year enacted or drafted

The substantive provisions of African data protection laws typically address several core elements.

4.2. Temporal Analysis of Legislative Development

The historical development of the data protection laws in Africa shows specific stages of evolution affected by the local efforts and foreign trends. Figure 3 captures the timeline of law enforcement in the continent and shows that the adoption of laws has been rapid in the last 20 years (Data Protection Africa, 2024). The first laws in Africa on data protection were developed in 2000s, with Tunisia passing legislation in 2004, Senegal in 2008, and Morocco in 2009 (See Figure 3). Complementary temporal analysis contained in Figure 4 represents the status of laws on national data protection in Africa between 2000 and September 2020 with the color scheme indicating the timeframe of implementation (U.S. International Trade Commission, 2020). These innovative laws were influenced by the French law and the regulations of the European Union on data protection. The second wave of legislation was observed between 2011 and 2015, which can be seen on both Figure 3 and Figure 4 as several countries adopted data protection frameworks, which include Cape Verde (2011), Burkina Faso, Angola, Lesotho in 2011, South Africa in 2013, Madagascar in 2014 and Gabon in 2011 (Data Protection Africa, 2024).

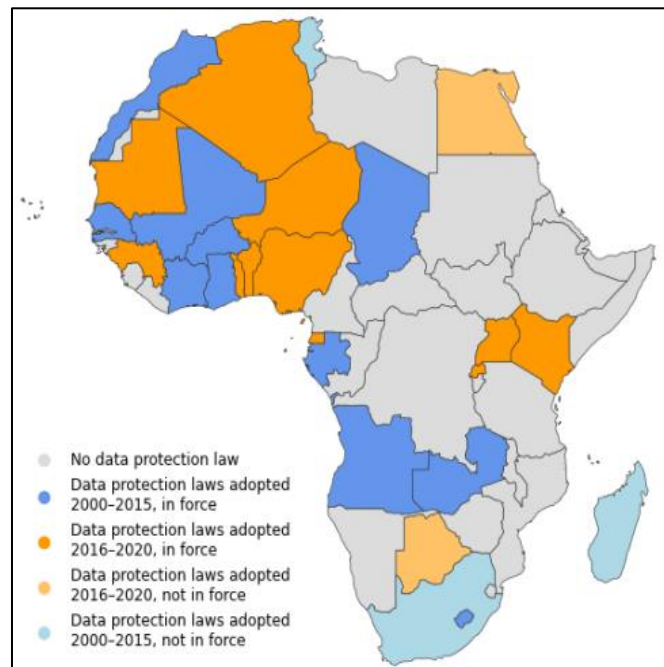


Figure 4 Status of national data protection laws in Africa, 2000–September 2020

4.3. Comparative Assessment of Regulatory Frameworks

Comparison of African data protection models demonstrates that there is a set of similarities and considerable differences between them in terms of regulations. Table 1 introduces comparative evaluation of data protection laws in the chosen African states, focusing on such significant aspects as the completeness of the legislation, the establishment of the supervisory body, the enforcement system, the restriction of the cross-border transfers, and harmonization with the international guidelines. The most detailed Systems can be found in such countries as South Africa, Mauritius, Tunisia, and Kenya, where there are functioning supervisory authorities, elaborated implementing regulations, and operational enforcement programs (Clifford Chance, 2025). The Protection of Personal Information Act of South Africa establishes an Information Regulator whose powers are exceedingly high, and which includes investigation, enforcement of the laws, and setting of penalties.

$$\text{Privacy Protection Index} = \alpha \cdot L + \beta \cdot E + \gamma \cdot A + \delta \cdot C$$

where:

- L represents legislative completeness on a 0 to 1 scale
- E represents enforcement effectiveness on a 0 to 1 scale
- A represents supervisory authority capacity on a 0 to 1 scale
- C represents compliance culture on a 0 to 1 scale
- $\alpha, \beta, \gamma, \delta$ are weighting factors with $\alpha + \beta + \gamma + \delta = 1$

Table 1 Comparative Assessment of Data Protection Frameworks in Selected African Countries

Country	Legislation Status	Supervisory Authority	Enforcement Activity	International Alignment	5G Readiness
South Africa	Comprehensive (2013, enforced 2021)	Established, adequately funded	Active enforcement, penalties imposed	High alignment with GDPR	High
Nigeria	Comprehensive (2023)	Established (NDPC)	Limited enforcement record	Moderate alignment	Medium
Kenya	Comprehensive (2019)	Established (ODPC)	Moderate enforcement	High alignment	Medium
Egypt	Comprehensive (2020)	Established	Limited public enforcement	Moderate alignment	High
Ghana	Comprehensive (2012)	Established	Minimal enforcement	Low to moderate alignment	Low
Uganda	Comprehensive (2019)	Established	Minimal enforcement	Moderate alignment	Low
Tunisia	Comprehensive (2004, updated 2017)	Established, functioning	Moderate enforcement	High alignment	Medium
Mauritius	Comprehensive (2017)	Established	Limited enforcement	High alignment	Medium
Tanzania	Recently enacted (2022)	Being established	No enforcement yet	Moderate alignment	Low
Morocco	Comprehensive (2009)	Established (CNDP)	Moderate enforcement	Moderate alignment	Medium

Data sources: Compiled from TechHive Advisory (2025), Clifford Chance (2025), Aitchison and Ayodeji (2025) and supplementary regulatory analysis 2024-2025

Africa has numerous states that have enacted data protection laws but these efforts have been compromised by high costs of implementation. Inadequate supervisory authorities that do not have enough staff, technical skills, and financial resources to execute mandates are common weaknesses (Aitchison and Ayodeji, 2025). There are those supervisory authorities, which are merely on paper and they lack functional operations, office space, and appointed commissioners. The mechanisms of enforcement are still very weak in most jurisdictions, with little investigations carried out, little penalties being given and little compliance checking. The general knowledge on data protection rights is still low, and citizens do not demand its implementation as reported by Ouma et al. (2025). Compliance in the private sector is a major issue; most large multinational corporations have privacy programs in place whereas small domestic companies do not bother with the requirements. In most cases, government agencies often can get away with asserting exemptions to the protection of their data due to the national security or public interest considerations, constraining the scope of actual protection. Most African laws have cross-border limitations on data transfer that are not enforced seriously, and it is a common practice to have an outbound flow of data across the border with proper provision of no adequacy and no suitable data protection measures.

5. Privacy Risks in 5G Networks

5.1. Massive Data Collection and Flow Mechanisms

The amount of personal data generated and processed by the fifth-generation networks is qualitatively different than the prior generations, leading to qualitatively different threats to privacy (European Parliamentary Research Service, 2022; Khan et al., 2019). The architecture of the 5G systems illustrated in Figure 2 facilitates the constant data assembly in various dimensions. Figure 2 gives a complex architecture of the network elements that collect and process device identity information such as International Mobile Equipment Identity numbers, International Mobile Subscriber Identity numbers, device hardware fingerprints, etc. The location data will be more precise than ever before, with 5G networks being able to calculate device positions over meters or even centimetres using advanced positioning methods

that combine multiple signals generated by the ultra-dense cell deployments and beamforming made possible using Figure 2. Location records which are time stamped leave detailed histories of movement which reveal daily habits, social connections, workplaces, dwelling patterns, and destinations. The metadata of traffic such as communication partners, duration, frequency, and volumes of communication data reveal social networks and patterns of communication even in situations where the data is encrypted.

The data collection does not only limit itself to the conventional telecommunications data, but spans across application-layer data that is produced by the connected services and devices. The devices of Internet of things installed in huge numbers within the 5G networks as represented in the sensor networks section of Figure 2 continuously relay sensor data, status data, and behavioural data (Pirbhulal et al., 2024). Smart home appliances communicate occupancy, temperature, appliance, and entertainment. Smart health wearables transfer such physiological data as the heart rate, activity, sleep, and location. Vehicular communications in Figure 2 report position, speed, routes, destinations, driving behaviors, and vehicle diagnostics. The sensors used in industry are used to check the production processes, the performance of equipment, the environment, and the activities of workers. By combining the data that is found in these various sources, a holistic profiling of the person can be realized and intimate information about personal life, routines, tastes, relations, and ideas that few persons would be willing to tell, but analysed by Ouma et al. (2025).

$$D_{total} = \sum_{i=1}^n (D_{network}^i + D_{application}^i + D_{IoT}^i)$$

where:

- D_{total} represents total data collected per user
- $D_{network}^i$ represents network signaling and metadata
- $D_{application}^i$ represents application-layer data
- D_{IoT}^i represents Internet of Things device data
- n represents number of connected devices per user

5.2. Enhanced Surveillance Capabilities

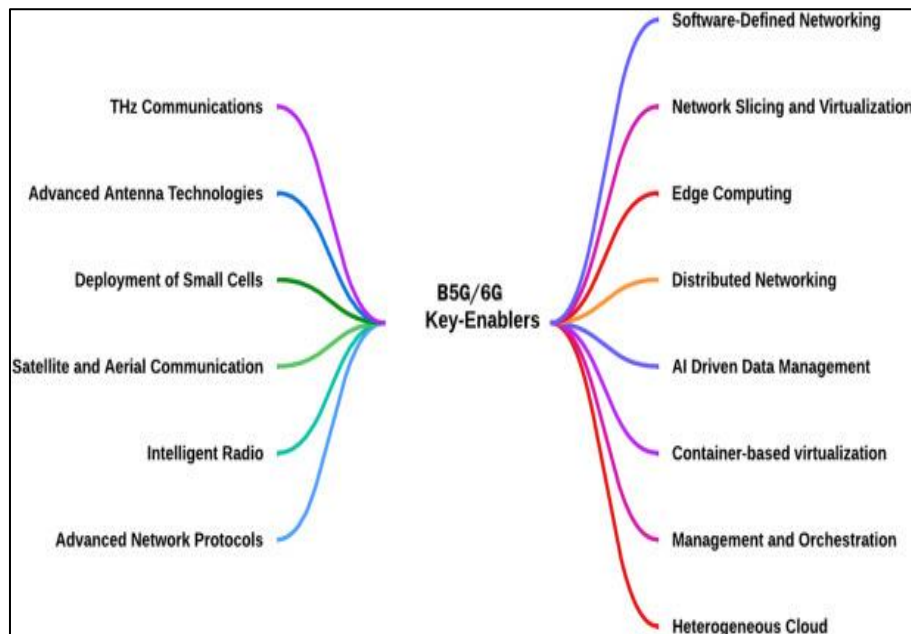


Figure 5 Key enablers of 5G private networks

The surveillance opportunities of 5G networks are enormous in the possibilities of the governments, law enforcement agencies, intelligence services, and commercial organizations (Adeyeye and Mungai, 2024; Digital Rights Alliance Africa,

2025). Network slicing allows to form special virtual networks that are used to perform surveillance, which may have weaker encryption or required backdoors that allow the interception. The 5G core network software-defined architecture in Figure 5 enables the dynamically interpreted addition of lawful intercept functionality and deep-packet inspection capabilities to the network without having to touch physical transmission facilities. Platforms Edge computing platforms represented in Figure 5 and deployed across networks can analyze traffic patterns, conduct content analysis and behavioural analytics in real-time near end users prior to the encryption process.

The artificial intelligence and machine learning functions built into 5G network management systems as illustrated in the artificial intelligence-based data management area of Figure 5 can be used to the advanced surveillance applications (Ali et al., 2024). Pattern recognition algorithms note the user of a device, the pattern of application use, and the behavior of the user even when their identities are obfuscated. The algorithms of social network analysis graphically represent the relationship of people depending on their communication patterns, location correlations, and interests. Predictive analytics is used to predict the future behaviors, motions, and relationships after considering the past. The anomaly detection systems detect deviant actions that may be in a form of threat, dissent, or illegal activities. Facial recognition that is based on 5G-connected surveillance cameras and real-time recognition allows people to be identified and tracked in the open world.

5.3. Security Vulnerabilities and Exploitation Risks

Although 5G systems have been said to provide greater security than 4G networks, the technology has a lot of vulnerabilities that can be used by threat actors to infringe privacy (Khan et al., 2019). Authentication vulnerabilities in original network connection protocols allow identity spoofing and man in the middle attacks. Signalling procedures have protocol vulnerabilities that can be used to track the devices, inject fake information, and disrupt services. The software-based architecture in Figure 5 presents several risks such as susceptible software elements, unsafe interfaces, privilege increment attacks, and malware of the chain of supply, to network operations. Virtualization technologies such as container-based virtualization as illustrated in Figure 5 leave attack surfaces such as vulnerabilities in hypervisors, container escape vulnerabilities, and inter-tenant attacks in multi-tenant cloud settings.

Stingrays are International Mobile Subscriber Identity catchers, which continue to work against 5G despite the supposedly enhanced security (European Parliamentary Research Service, 2022). These devices mimic the appearance of legitimate cell towers and surround the immediate devices and make them connect to them instead of legitimate network infrastructure. In the event of the connection, the IMSI catcher can intercept communications, tracing device position, and injecting malicious traffic. Although specifications of the 5G have safeguards against this type of attack, those safeguards are compromised by implementation flaws, backward compatibility, and vulnerabilities of user devices. Advanced attackers such as intelligence agencies have the capacity to use 5G vulnerability to spy. There are always zero-day vulnerabilities in network equipment and software that are finding their way and can be exploited before they are patched.

$$R_{privacy} = P_{exploit} \times I_{impact} \times \frac{1}{C_{defense}}$$

where:

- $R_{privacy}$ represents overall privacy risk
- $P_{exploit}$ represents probability of vulnerability exploitation
- I_{impact} represents impact severity of privacy breach
- $C_{defense}$ represents defensive capability effectiveness

5.4. Third-Party Access and Commercial Surveillance

In addition to the government surveillance, 5G networks support the business surveillance methods of telecommunications operators, technology firms, advertisers, and data brokers (Hosein, 2011). Network operators gather extensive information regarding the behavior, location, communication, and utilization of applications by the subscribers. Such data forms a good commercial property that operators can sell in different ways such as a form of targeted advertising, location analytics to retailers, and behavioural profiling to marketers. The 5G network analytics systems can make real-time inferences of subscriber conditions such as their locations, activities, interests, and intentions to purchase. Advertisers can be provided with the capability by operators to reach specific audiences due to detailed behavioural profiles without providing any personal information, although this targeting behavior exposes personal information as discussed by Zuboff (2019).

The application developers and service providers who can access the 5G networks via APIs receive user information that they can use to their own commercial benefit (Ali et al., 2024). Mobile apps often demand too much access to gather location data, contacts, communications, and information about the device that do not have any relevance to the functionality of the app. The third-party analytics firms incorporated in applications monitor users in most services, which build detailed profiles of online activities, interests, and associations. Data brokers collect data (telecommunications providers, application providers, websites, and records, public records, and commercial databases) and assemble detailed dossiers of individuals being sold to marketers, employers, insurers, and others.

The intelligence and security agencies are allowed very wide-ranging discretion on how to intercept communications and infiltrate the telecommunications information without any independent control. National security laws often provide blanket authority over surveillance and loosely define what threats are and include little procedure protection.

The telecommunications laws of most African nations have a clause that mandates the operators to enable lawful intercept, keep subscriber logs long enough and respond to demands of the government (Sutherland, 2018). There are countries that require live access to the network infrastructure by the security agencies so that it is possible to monitor the communications being always made. Telecommunications operators are also required by others to install monitoring equipment provided by the government in their networks. Surveillance practices are not transparent and therefore, it is hard to determine the actual monitoring activities.

Table 2 Legal Frameworks Governing State Surveillance in Selected African Countries

Country	Constitutional Privacy Protections	Surveillance Law Framework	Judicial Authorization Required	Independent Oversight Mechanisms	Transparency Reporting
South Africa	Strong constitutional protections	Regulation of Interception of Communications Act	Yes, for interception	Judicial oversight by designated judges	Limited operator transparency
Kenya	Constitutional privacy rights	Security Laws Amendment Act	Ostensibly required but often bypassed	Weak oversight mechanisms	No systematic reporting
Nigeria	Constitutional privacy provisions	Cybercrime Act, NSA Act	Ambiguous requirements	Limited oversight	No transparency reports
Egypt	Limited constitutional protections	Anti-Terrorism Law, Emergency Law	Not required for terrorism suspects	Minimal oversight	No transparency
Uganda	Constitutional rights often superseded	Regulation of Interception Act	Required but loosely enforced	Weak oversight	No reporting
Tanzania	Constitutional provisions	Cybercrimes Act	Ambiguous procedures	Minimal oversight	No transparency
Zimbabwe	Constitutional rights with exceptions	Interception of Communications Act	Required but surveillance exceeds legal bounds	Limited oversight	No reporting
Ghana	Constitutional protections	Electronic Communications Act	Required for criminal investigations	Moderate oversight	Limited reporting
Ethiopia	Limited constitutional protections	Anti-Terrorism Proclamation	Not required for security threats	No independent oversight	No transparency
Morocco	Constitutional privacy provisions	Telecommunications Law	Required but procedures unclear	Limited oversight	No systematic reporting

Data sources: Compiled from Adeyeye and Mungai (2024), Sutherland (2018), Khan et al. (2019) and human rights organization report 2023-2025

5.5. Deployment of Dual-Use Surveillance Technologies

Many African governments have acquired advanced surveillance systems to international sellers that allow them to monitor the online activities and digital communications in detail (Digital Rights Alliance Africa, 2025). These dual-use technologies, which are claimed to be used in the name of law enforcement and national security, are often used against the critics, opposition groups, and the civil society through political surveillance. The internet traffic can be monitored in real time through deep packet inspection systems which can be used to block certain contents and to identify people visiting blocked sites or exchanging valuable information. The telecommunications interception systems offer the ability to intercept voice communication, text messages, and data communications, in most cases without judicial approval or supervision.

In recent years, the infiltration of surveillance technologies in Africa has been more rapid due to the sales of the Chinese and Israeli surveillance firms, European telecommunications equipment suppliers, and others (Digital Rights Alliance Africa, 2025). The various African nations, such as Zimbabwe, Uganda, and Kenya, that China has been exporting its all-inclusive safe city surveillance systems are all inclusive of integrated systems that incorporate telecommunications interception, the ability to monitor the internet, facial recognition, and predictive policing analytics. Such systems allow dictator regimes to spy on people in their entirety under the guise of improving citizen security and combating terrorism. This level of obscurity of procurement methods, the ability of implemented systems, and real usage of patterns does not allow people to be held to account and to control it.

5.6. Case Studies from Selected African Countries

The deployment of surveillance technologies in Nigeria is an example of alarming tendencies with no legal protection and democratic checks and balances (Spaces for Change, 2024). The nation has acquired massive surveillance devices such as telecoms interception tools, internet surveillance systems, and the use of closed-circuit television systems with face recognition. In 2024, Spaces for Change recorded the spread of dual-use surveillance technologies in Nigeria, noting that this technology presents threats to privacy, freedom of expression, and democratic participation. Their implementation was done without a well-developed legal framework to regulate its use, little or no consultation with the people and the creation of independent regulatory bodies.

Kenya has also increased surveillance by acquiring telecommunications interception equipment, social media surveillance infrastructure, and CCTV networks (Kenya Human Rights Commission, 2017). The Kenya Human Rights Commission reported widespread surveillance of political activists, civil society groups, and the press especially during election periods when the government tries to check the activities of the opposition. Especially widespread use of surveillance technologies was evident in the 2017 elections to monitor political opponents and block dissent. Although Kenya has a relatively developed data protection system, as indicated by Figure 3 as having legislation in place in 2019 and Table 1 as having moderate enforcement, security agencies do not abide by the regulations, as they are provided by the national security exemptions and ineffective oversight mechanisms. Criminal cases against illegal surveillance have met a slight success in limiting the surveillance activities used by the government. The proliferation of the 5G networks in Kenya, which have about 1.5 million subscribers as shown in the regional analysis of Figure 6 currently, implies the ability to provide the network with improved surveillance that is currently not appropriately controlled by the legal systems as examined by Kenya Human Rights Commission (2017).

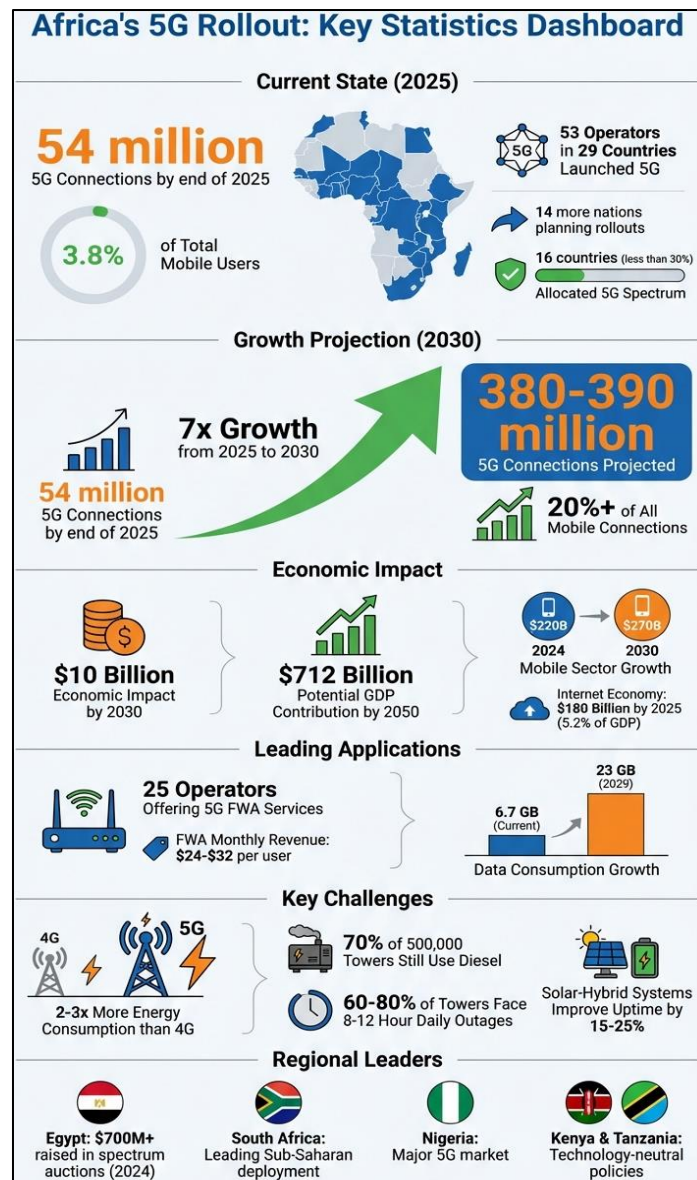


Figure 6 Africa's 5G Rollout: Key Statistics and Projections for 2025-2030. Data compiled from industry reports 2022-2025

6. Balancing Security Interests with Individual Privacy Rights

6.1. Legitimate Security Requirements in Developing Economies

Most of the governments of African countries have real security issues that give justifiable demands to certain surveillance facilities under proper legal limitations (Sutherland, 2018; Hosein, 2011). In various parts of Africa, such as in East Africa and the West African region, terrorist groups such as Al-Shabaab, the Boko Haram and the Islamic State affiliates are continuing to kill thousands of people each year. Prisoner trafficking Organized crime syndicates are involved in drug trafficking, human trafficking, arms smuggling and other transnational crimes that need to be investigated and prosecuted. Cybercrime against financial institutions, government systems, and individuals is a problem that generates significant economic losses and creates a sense of distrust in digital systems.

The dilemma is to come up with surveillance structures, which can facilitate legal security activities and avoid misuse and invasion of privacy rights (Hosein, 2011). Such frameworks must incorporate several elements including:

- Surveillance powers should be granted only through clear legal authorization enacted by legislatures and subject to constitutional review.

- Surveillance should be permitted only when necessary and proportionate to address specific legitimate security threats, not for generalized monitoring of populations.
- Targeted surveillance should require prior judicial authorization based on probable cause or reasonable suspicion, with emergency exceptions narrowly defined.
- Independent oversight mechanisms including judicial review, legislative oversight, and specialized privacy commissioners should monitor surveillance activities and investigate abuses.
- Transparency requirements should mandate periodic public reporting of surveillance statistics, legal authorities invoked, and oversight findings, subject to genuine national security redactions.
- Individuals subjected to surveillance should receive notification after investigations conclude unless ongoing security needs justify continued secrecy.
- Effective remedies including suppression of evidence, civil damages, and criminal sanctions should be available for unlawful surveillance as analysed by Hosein (2011).

Table 3 Proposed Framework for Balancing Security Interests with Privacy Rights in 5G Networks

Principle	Implementation Mechanism	Oversight Requirement	Penalty for Violation
Legality	Parliamentary legislation defining surveillance powers	Constitutional court review of surveillance laws	Suppression of unlawfully obtained evidence
Necessity	Requirement to demonstrate specific security threat	Judicial review of necessity claims	Disciplinary action against officials
Proportionality	Least intrusive means requirement	Privacy impact assessments for surveillance programs	Civil damages for disproportionate surveillance
Judicial Authorization	Prior warrant requirement for targeted surveillance	Specialized surveillance court review	Criminal sanctions for unauthorized surveillance
Independent Oversight	Privacy commissioners with investigative powers	Regular audits of surveillance activities	Public reporting of oversight findings
Transparency	Statistical reporting of surveillance activities	Parliamentary oversight committees	Mandatory disclosure of previously secret programs
Notice	Post-surveillance notification to affected individuals	Review of notification delays	Right to challenge surveillance in court
Redress	Access to courts and complaint mechanisms	Investigation of abuse allegations	Compensation for privacy violations
Data Minimization	Collection limited to necessary information	Review of data retention practices	Mandatory deletion of excess data
Security	Protection of surveillance data from unauthorized access	Audit of data security measures	Sanctions for security failures

Data sources: Synthesized from European Parliamentary Research Service (2022), Hosein (2011), African Union (2014) and international human rights standards

6.2. Privacy-Preserving Technologies and Approaches

Technological solutions can decrease the tension between security demands and privacy protection by allowing the surveillance opportunities that are as limited to the legitimate purpose as possible and avoiding the further violation of privacy (European Parliamentary Research Service, 2022). End to end encryption ensures that no telecommunication operator and network intermediaries have access to the content of communication so that only the parties in the communication can decrypt messages. Heavy encryption may not stop gathering of metadata such as the communication partners, time, and frequency which assists in numerous legitimate investigations without disclosing intimate conversation content. Telecommunications operators can offer lawful intercept functionality with reasonable protection such as judicial authorization condition, audit trail and technical measures that ensure unauthorized access is not possible.

$$U_{social} = B_{security} + B_{services} - C_{privacy} - C_{surveillance}$$

where:

U_{social} represents total social utility

$B_{security}$ represents security benefits

$B_{services}$ represents service benefits from 5G

$C_{privacy}$ represents privacy costs

$C_{surveillance}$ represents surveillance harms

6.3. Regulatory Best Practices and Policy Recommendations

The surveillance within 5G networks should be regulated properly with the detailed policy frameworks that should include the international human rights provisions adjusted to the African settings (Hosein, 2011; African Union, 2014). The changes in legislation must provide clear limits on the reasons that should be allowed to conduct surveillance which can be restricted to investigation of serious crimes and legitimate threat to national security. The wide definitions of national security allowing the surveillance of political opposition, civil society, or unpopular speech should be abandoned in favour of narrow definitions that are based on violence, terrorism, and transnational crime. The procedures of surveillance authorization must involve the judicial issues of warrants on probable cause or reasonable suspicion, and made by independent judges and not by the officials of the security agencies. Exceptions on the use of surveillance without prior authorization in the name of emergency need to be well defined, temporal, and expedited judicial oversight.

There is a need to develop independent oversight mechanisms that have the resources, expertise, and power to conduct effective surveillance exercises (Clifford Chance, 2025; Aitchison and Ayodeji, 2025). The powers of investigations, access to classified information, subpoena authority and independent budgets must be protected by the executive branch against the control of privacy commissioners or specialized surveillance oversight agencies. Surveillance programs should be checked on a regular basis to determine its compliance with the legal standards, the need and proportionality of surveillance, and the security of the information gathered. The transparency needs must require that periodical public reporting should contain the numbers of surveillance authorizations requested and obtained, legal basis invoked, nature of investigated offenses, and demographics of the victimized persons.

6.4. Multi-Stakeholder Engagement Frameworks

Surveillance and privacy in 5G networks can only be effectively governed through the active participation of various stakeholders other than the government such as telecommunications operators, civil society organizations, technical experts, and international organizations (Hosein, 2011). Telecommunications operators are advised to use privacy-by-design principles in the network architecture and operation, reduce data gathering, use high security standards, and resist illegal surveillance demands. The industry associations should develop the codes of conduct to create the best practices in dealing with the government surveillance demands, user privacy protection, and transparency. The civil society groups have been playing significant roles in lobbying protection of privacy, recording of abuses of surveillance, informing the people about their privacy, and suing on cases concerning unlawful monitoring. Technical experts also help in the development of privacy-enhancing techniques depicted in Figure 5, security standards, and policy recommendations based on the present technological strength and constraints as examined by Hosein (2011).

7. Regional and International Perspectives

7.1. Comparative Analysis with Global Privacy Standards

The issue of African privacy in 5G networks is situated in the larger global environment of changing privacy standards and regulatory strategies. The General Data Protection Regulation of the European Union, as the most influential and comprehensive privacy regulation in the world, sets the high standards of data protection and establishes the presence of extraterritoriality to the application on African organizations processing the data of European citizens (Clifford Chance, 2025). The GDPR has integrated such principles as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. It gives substantial rights to the data subjects such as access, rectification, erasure, restriction, portability, and objection. In the case of severe violations of the regulation, the penalty is high in terms of 4% of the annual revenue around the world, which generates high incentives to adhere to it.

Table 4 Comparative Privacy Frameworks: Africa, Europe, United States, and Asia

Region	Regulatory Approach	Core Principles	Enforcement Mechanisms	Surveillance Constraints	Cross-Border Data Flows
European Union	Comprehensive omnibus regulation (GDPR)	Lawfulness, consent, purpose limitation, minimization	Independent supervisory authorities, substantial penalties	Prior judicial authorization required	Adequacy decisions, standard contractual clauses
United States	Sectoral regulation, emerging state laws	Varies by sector, notice and choice predominant	Federal Trade Commission, state attorneys general	Extensive surveillance with oversight	Minimal restrictions, privacy shield framework
African Union	Malabo Convention framework	Principles derived from EU standards	National authorities with varying effectiveness	Highly variable across countries	Adequacy requirements in laws
Asia-Pacific	Diverse national approaches	Varies significantly by country	Mixed effectiveness	Generally permissive	Increasing restrictions
Latin America	Growing comprehensive frameworks	Influenced by European standards	Emerging enforcement capacity	Variable constraints	Increasing restrictions

Data sources: Synthesized from TechHive Advisory (2025), Clifford Chance (2025), African Union (2014) and comparative privacy law scholarship

7.2. Regional Cooperation Mechanisms

The efforts of regional cooperation in Africa are directed at aligning the privacy standards, movement of data across the borders, as well as enhancing the enforcement capacity (African Union, 2014). The Malabo Convention of the African Union offers a structure of continental cooperation, but is limited in its effectiveness due to limited ratification. Economic communities such as Economic Community of West African States, East African Community and Southern Africa Development Community have undertaken the harmonization of data protection with inconsistent results. In 2010, ECOWAS adopted a Supplementary Act on Personal Data Protection which demanded its member states to create national legislation to be compatible. Nonetheless, its implementation is not full and some member states do not have frameworks which comply more than a decade later as reported by Future Privacy Forum (2024).

7.3. Technology Transfer and Capacity Building

In the African 5G rollouts, technology transfer arrangements influence capabilities and privacy results (Sutherland, 2018; Sutherland, 2019). The competitive pricing, vendor financing schemes, and bilateral technology cooperation agreements are manifested in the approach of the Chinese telecommunications equipment vendors such as Huawei and ZTE dominating the African 5G networks. Nonetheless, such partnerships are problematic in terms of surveillance capacity that may be integrated into the network infrastructure as depicted in Figure 2, equipment access by equipment providers or Chinese government, and technology reliance that limits policy freedom in Africa. Other solutions with European and other suppliers can provide more privacy protection at a noticeably increased price and less favourable financing conditions.

8. Conclusion

In conclusion, the introduction of the fifth-generation wireless network in Africa is a ground-breaking technology with significant economic and social potential. Nevertheless, the same digital revolution poses unprecedented privacy threats due to the large volumes of information, increased surveillance capacities, and lack of proper regulatory safeguards in the environment of developing economies. This study has fundamentally analysed privacy issues related to the introduction of 5G in African countries, including the conflicts between the interests of the state surveillance and the rights of people. The analysis recorded status of 5G rollout in the continent with 54 million connections being

recorded to date and with 54 million connections being projected to increase seven-fold by 2030 as shown in Figure 6 and creating an immense economic value in various sectors.

The analysis of the African data protection legislative situation revealed that there are major gaps between the regulatory maturity in the continent as shown in Figure 3 and Figure 4. Although 28 nations have implemented the full privacy framework by as of 2025 as seen in Figure 3 in the different colors, effectiveness has been wide ranged in its implementation depending on the supervisory authority ability, resources to enforce the framework, and the political commitment. Other problems encountered by many countries that have laws to protect data privacy are lack of funds to run the oversight organizations, lack of effective enforcement strategies, poor publicity, and poor compliance by government organizations. The lack of privacy laws in 26 African nations indicated in gray in Figure 3 and Figure 4 exposes large populations to have no policy or law that protects them against commercial or government surveillance. The African Union Malabo Convention and other regional integrations such as Latin America have had minimal success because of the delay in ratifying them and because of implementation barriers.

The survey of the surveillance implications in the African experiences indicated alarming practices such as the use of dual uses technologies, lack of legal mechanisms to limit government surveillance, a poor judicial system to oversee surveillance mechanisms, and monitoring political critics, journalists, and civil society groups. Nigeria, and other case studies reported real abuses of surveillance through the telecommunications networks with no proper accountability or redress to victims. The study has indicated that the trade off between legitimate security demands and privacy security requires detailed frameworks that have clear legal authorization, judicial checks, autonomous accountability infrastructure, and technical controls as shown in Figure 5.

Privacy protection in the 5G networks in Africa must be balanced between competing concerns such as maximizing economic benefits of digital technologies of approximately \$712 billion projected in 2050 as in Figure 6, effective security concerns, rights and democratic governance of individuals, and capacity building of institutions with limited resources. This balance can be maintained by good policy designing, political determination, proper allocation of resources and multi-stakeholder inclusion.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

- [1] Wajdi, M., Rahman, A., & Al-Hashimi, M. (2024). Exploring the technological advancements and security issues of 5G. *World Journal of Advanced Research and Reviews*, 23(2), 812-846.
- [2] Adeyeye, A. O., & Mungai, P. (2024). Public attitudes towards surveillance and privacy of personal communications in 34 African countries. *Computers in Human Behavior Reports*, 15, Article 100489. <https://doi.org/10.1016/j.chbr.2024.100489>
- [3] Digital Rights Alliance Africa. (2025). The surveillance footprint in Africa threatens privacy and data protection.
- [4] Ouma, S., Wamukoya, J., & Muthee, J. (2025). Big data and personal information privacy in developing countries: Insights from Kenya. *Frontiers in Big Data*, 8, Article 1532362.
- [5] Ijaz, M. (2024). 5G security challenges & solutions: A comprehensive review. *International Journal of Research and Technology Innovations*, 24(5), 1-18. <https://ijrti.org/papers/2405076.pdf> [PDF Available]
- [6] Sutherland, E. (2018). Digital privacy in Africa: Cybersecurity, data protection and surveillance (SSRN Working Paper). <https://doi.org/10.2139/ssrn.3201310>
- [7] European Parliamentary Research Service. (2022). Privacy and security aspects of 5G technology (STUD 697205).
- [8] Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions. *IEEE Communications Surveys & Tutorials*, 22(1), 196-248.
- [9] TechHive Advisory. (2025). Roundup on data protection in Africa 2024: Projections for 2025.

- [10] Hosein, G. (2011). Privacy and developing countries. Office of the Privacy Commissioner of Canada.
- [11] Future Privacy Forum. (2024). Global RECs: Towards a continental approach to data protection in Africa.
- [12] Narciandi-Rodríguez, D., Aveleira-Mata, J., Alfonso-Cendón, J., & Benavides, C. (2025). A cybersecurity review in IoT 5G networks. *Internet of Things*, 30, Article 101478. <https://doi.org/10.1016/j.iot.2024.101478>
- [13] Clifford Chance. (2025). Africa guide: Data protection 2025.
- [14] Nigeria Data Protection Commission. (2024). *International journal of data privacy and protection*.
- [15] Pirbhulal, S., Chockalingam, S., Shukla, A., & Abie, H. (2024). IoT cybersecurity in 5G and beyond: A systematic literature review. *International Journal of Information Security*, 23, 2827-2879.
- [16] Aitchison, E., & Ayodeji, A. O. (2025). Enforcing data privacy in Kenya and Nigeria: Towards an African approach to regulatory practice. *Information & Communications Technology Law*, 34(1), 1-28. <https://doi.org/10.1080/13600869.2025.2506918>
- [17] U.S. International Trade Commission. (2020). Data protection laws in Africa: A pan-African survey and policy recommendations.
- [18] Spaces for Change. (2024). Proliferation of dual-use surveillance technologies in Nigeria: Deployment, risks & accountability.
- [19] Africa Privacy Roundup. (2024). Roundup on data protection in Africa – 2024. <https://africaprivacyroundup.com/roundup-on-data-protection-in-africa-2024/>
- [20] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 193-199. <https://doi.org/10.1109/CSCN.2017.8088621>
- [21] Persistent Energy. (2024). Data protection compliance in Africa. <https://persistent.energy/persistent-story/data-protection-compliance-in-africa/>
- [22] Data Protection Africa. (2024). Mapping the progress (and delays) for data protection in Africa. <https://dataprotection.africa/data-protection-in-africa-progress/>
- [23] Kenya Human Rights Commission. (2017). The right to privacy in the age of communications surveillance: Kenya country report. KHRC.
- [24] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2024). A comprehensive survey on IoT cybersecurity in 5G and beyond: Recent advances, emerging challenges, and future research directions. *International Journal of Information Security*, 23, 1625-1681. <https://doi.org/10.1007/s10207-024-00865-5>
- [25] Sutherland, E. (2019). The fourth industrial revolution—The case of South Africa. *Politikon*, 47(2), 233-252. <https://doi.org/10.1080/02589346.2019.1696003>
- [26] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
- [27] Ali, M. N., Abdulghani, H., Ayed, W. B., Hassan, M. M., & Fortino, G. (2024). A comprehensive survey on generative AI solutions in IoT security. *Electronics*, 13(24), Article 4965. <https://doi.org/10.3390/electronics13244965>
- [28] Kamau, P. M., & Wanjohi, A. M. (2019). Challenges of big data governance in Kenya: A case of selected government ministries. *International Journal of Science and Technology Research*, 8(10), 491-500.
- [29] Rayes, A., & Salam, S. (2022). *Internet of Things from hype to reality: The road to digitization* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-030-90158-5>
- [30] African Union. (2014). African Union convention on cyber security and personal data protection (*Malabo Convention*).