

Comparative Human Rights Analysis of Government Surveillance and Data Privacy in Nigeria, India and South Africa

Adio, Mobola, LL.M, Ph.D. (in View),
Faculty of Law, Lead City University Ibadan, Oyo State, Nigeria.
Email: mobola.adio@gmail.com

Yewande Fatoki, PhD.
Senior Lecturer, Faculty of Law, Lead City University
Ibadan, Oyo State, Nigeria. Email: fatoki.yewande@lcu.edu.ng

ABSTRACT

This paper presents a comparative analysis of the human rights implications of government surveillance and data privacy laws in three leading developing democracies: Nigeria, India, and South Africa, which have all enacted extensive surveillance legislation and major constitutional challenges to the legality of state surveillance powers. The proliferation of digital communications networks throughout the Global South has increased the potential for mass surveillance capabilities on the part of government, leading to significant tension between the demands of state security and constitutional guarantees of individual privacy. Based on constitutional law, primary legislation, judicial precedent, and peer-reviewed academic research, the paper explores the legal structures governing surveillance in each country, analyses the human rights flaws in these structures, and evaluates the effectiveness of constitutional safeguards against those flaws. The paper concludes that although each of the three States has codified the right to privacy in its constitution and data protection laws, it is precisely such measures which create systems of surveillance to violate the very privacy protections they claim to guarantee. The article concludes with recommendations grounded in international human rights standards for the structural reform of surveillance governance in each jurisdiction.

Keywords: Government Surveillance, Data Privacy, human rights, legal pluralism, Comparative Constitutional Law

1.1 INTRODUCTION

The issue of state surveillance and privacy rights has assumed an ever more prominent role in discussions of human rights in modern times. As Lyon (2007) pointed out, the practice of surveillance is no longer restricted only to the regimes of authoritarian countries but has come to be practised widely in both democratic and developing nations to protect national security and combat terrorism and crime. The growth of communications technologies in the age of information has allowed for the creation of many kinds of surveillance activities on the part of governments in both liberal democracies and less-developed countries (Singler and Babalola, 2025). It follows that the laws which regulate state power in surveillance activities are highly significant within any regime of human rights protection.

In this regard, this paper will investigate the following frameworks in the three most populated and institutional democracies of the Global South; namely Nigeria, India, and South Africa. Each of these states demonstrates a unique combination of the surveillance-privacy dilemma. As the Federal Republic of Nigeria, the constitution of which was adopted in 1999, implemented the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and even introduced the Nigeria Data Protection Act 2023, this state's surveillance system has been widely criticized for lack of sufficient judicial control and excessive executive powers (Section 37 of the Constitution of the Federal Republic of Nigeria 1999; Section 38-39 of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015; Section 1-3 of the Nigeria Data Protection Act 2023). However, India, being the largest democracy in the world, managed to reach a great constitutional milestone in 2017 by establishing, through the verdict of a nine-judge Supreme Court Bench, that the right to privacy is a fundamental right based on Articles 14, 19, and 21 of the Constitution. Nevertheless, the Indian surveillance regime, which operates according to Section 69 of the Information Technology Act 2000, remains deficient (Article 19(1)(a) and 21 of the Constitution of India, 1950; Section 68 of the Information Technology Act 2000; Justice K S Puttaswamy (Retd) v Union of India, 2017).

In South Africa, where its 1996 Constitution is considered to be among the most protective of privacy rights anywhere in the world, an important achievement came about in 2021 when the Constitutional Court of South Africa struck down five aspects of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), but the necessary legislative reform is still not fully accomplished yet. (Section 14 of the Constitution of the Republic of South Africa, 1996; RICA, 2002; AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional

Services and Others, 2021). The three jurisdictions are selected for comparative analysis because they share a common structural challenge balancing the security imperatives of large, complex states against the privacy rights of their citizens while presenting meaningfully different constitutional designs, judicial cultures, and institutional capacities for oversight. Their comparison illuminates, from three distinct vantage points, the systemic features of surveillance governance that tend to generate human rights deficits, and the constitutional and institutional conditions under which effective oversight is more or less likely to be achieved.

1.2 Literature Review

Government surveillance and data privacy have been key themes within discussions surrounding human rights due to the fast advancement of digital technology and the capability of governments to gather, store, analyze and interpret personal information. Surveillance can be defined as an act of surveillance of persons, groups of people, or communication carried out by the government to serve a purpose like security of the nation, crime prevention, law enforcement and public safety or for gathering intelligence (Aloamaka, 2025). According to Mahmoud, Yusuf and Olohunbebe (2025), data privacy pertains to protecting personal information against unauthorised access, use, and/or distribution and entails the control that people should be able to exercise over their personal information. Government surveillance and data privacy have been controversial themes in many discussions since surveillance usually entails the gathering and analysis of personal data.

Chika and Tochukwu (2020), Modilim et al. (2024) and Odugbemi (2026) widely recognize privacy as a basic right which is essential for human dignity, self-determination, and democracy. It follows that any form of violation of one's private matters is considered by international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights as a breach of privacy, family life, home, and correspondence, which is forbidden. Privacy in this case should not be regarded as a mere personal choice since it is seen as a condition for freedom of expression, freedom of association, freedom of religion, and politics. Indeed, Singler and Babalola (2025) believe that people will feel free to exercise their right to freely communicate with others and to discuss different topics in public without fear because of their privacy.

There are different viewpoints among scholars regarding governmental surveillance. Uwadinma (2025) and Mahmoud, Yusuf and Olohunbebe (2025) claim that there is a need for governments to defend their citizens from various types of crime, including terrorist acts, cybercrime, organized crime, human trafficking, corruption, etc. They maintain that the evolution of technology has changed the face

of security threats and the government needs the necessary technologies to investigate and counter these threats. In their opinion, the use of surveillance is justified in ensuring the administration of governance and security, especially given the age of digital communication and transnational crime organisations. According to Odugbemi (2026), surveillance cannot be considered a violation of human rights as long as it follows legal procedures and has appropriate protective measures.

On the other hand, Unnam (2015) claim that surveillance threatens human rights and democracy. They hold that surveillance could easily turn into a tool of controlling and suppressing individuals and could easily turn into an instrument for the misuse of state power where proper checks fail. Social theorists inspired by the ideas of Foucault (1991) see surveillance as a method of social control where people feel compelled to conform themselves because they are under surveillance. This phenomenon is often described as the “chilling effect,” whereby individuals refrain from exercising their rights to free expression, association, or political participation out of fear of monitoring or retaliation (Jemilohun, 2015). Adeoti (2023) therefore cautions that excessive surveillance may undermine the very democratic values that governments seek to protect.

However, the literature also notes problems associated with mass surveillance. Mass surveillance entails collecting massive amounts of data about a population rather than surveilling a particular individual accused of some crime. Human rights activists are critical of mass surveillance based on the fact that it infringes the rights of innocents and fails to meet the requirements of necessity and proportionality (Okoro et al., 2026). However, Sabo and S Utulu (2023) claim that massive data collection poses high risks of information abuse, unauthorised access, discrimination, profiling, and function creep a scenario where information collected for one reason is applied to other purposes not envisaged before. All these issues may have negative implications for confidence in governmental institutions and democracy.

Regarding data privacy, Singler and Babalola (2025) posit that people must have reasonable control over their data. Westin (1967) claims that privacy means being able to control whether and in what manner personal data is shared with others. The issue of privacy has gained importance due to the current technological environment. For instance, it is easier for governments and corporations to collect huge amounts of information about their citizens owing to biometric surveillance technologies, digital identity programs, social media, telecommunication network infrastructure, and AI technologies (Singler and Babalola, 2025). Hence, a growing number of academic sources suggest developing full-fledged laws concerning personal information collection, processing, storage, and exchange.

Another recurrent feature in the reviewed sources is the requirement to balance the right of privacy with legitimate state interests. Virtually all scholars admit that privacy should not be seen as an absolute right, which can be infringed upon in certain cases. Nevertheless, they stress that such infringements should be subject to certain criteria. Modilim et al. (2024) and Odugbemi (2026) point out principles of human rights and constitutional law as legality, necessity, proportionality, transparency, and accountability. According to Okpara and EC Okpara (2025), surveillance operations should be authorised under specific rules set forth in easily accessible laws. The Necessity Principle states that surveillance operations should achieve a legitimate objective and be necessary. Proportionality means that the level of invasion of one's privacy should correlate to the threat. The last two aforementioned principles require transparency in surveillance and data management frameworks and accountability in case of abuse.

The requirement for independent oversight is another recurrent feature in the reviewed materials. The most frequently suggested approaches include judicial oversight, parliamentary control, independent regulatory agencies, and data protection authorities. (Okpara and Okpara, 2025). Scholars also emphasise the importance of effective remedies that enable individuals to challenge unlawful surveillance and seek redress for violations of privacy rights. The literature ultimately highlights that there is no consensus regarding whether surveillance without restrictions or privacy without compromise is ideal. The best way forward is to have a proper balance where surveillance is employed as a means of addressing genuine security needs on one hand but the rights of individuals are also guaranteed at the same time (Unnam, 2015) For this reason, the most recommended approach by scholars is for governments to enact appropriate laws governing the use of information, provide proper checks and balances, and uphold international human rights standards.

1.3 The International Human Rights Framework Governing Surveillance

The right to privacy is considered one of the core human rights guaranteed by Article 17 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Nigeria, India, and South Africa. General Comment No 16 to the ICCPR, produced by the UN Human Rights Committee, states that Article 17 protects a person from the arbitrary or unlawful interference with his or her correspondence and other forms of communications (ICCPR, 1966). The committee specifies that states should specify in the laws particular instances of interference in private communications allowed by the law. The UN Human Rights Committee considers

that "arbitrariness" should include elements of both unlawfulness and lack of necessity and proportionality (UN, 1988)

In 2013, the UN General Assembly passed Resolution 68/167 "The Right to Privacy in the Digital Age," according to which the same set of rights, which a person has in the offline world, should be available to him or her in the digital age (UN General Assembly Resolution 68/167). UN High Commissioner for Human Rights stated after reviewing the issue that bulk or mass surveillance programs, or communication intercepts carried out without specific grounds, are "likely to be disproportionate and interfere with the right to privacy (UN High Commissioner for Human Rights, 2013).

The Necessary and Proportionate Principles, which were formulated by a group of civil society organisations and adopted by human rights mechanisms of the United Nations, lay down thirteen principles for applying surveillance powers in a human rights-compliant manner, including the principles of legality, legitimate purpose, necessity, sufficiency, proportionality, judicial oversight, notice to the user, transparency, and oversight. Although such principles are not legally binding, they are the most detailed manifestation of international consensus about the human rights principles relevant to state communications surveillance, and form the normative basis against which the three domestic systems considered in this article are tested.

Regionally, the Declaration of Principles of Freedom of Expression and Access to Information in Africa, which is adopted by the African Commission on Human and Peoples' Rights, provides that in Principle 39 all surveillance activities should be carried out in accordance with the principles of legality, necessity, and proportionality and should be subject to judicial oversight and public transparency (Principle 39, ACHPR, 2019). For South Africa, jurisprudence of the European Court of Human Rights under Article 8 of the European Convention on Human Rights is also relevant in analogies, especially based on the comparative constitutional jurisprudence of the Constitutional Court. The Grand Chamber judgment in *Big Brother Watch and Others v United Kingdom* (2021), where it was held that mass interception regimes should meet the criteria of prior judicial authorization, notification after surveillance, and independent monitoring, is a directly relevant analogical precedent for South Africa.

In terms of international law, the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) obligates the member-States to "guarantee the right to privacy in the electronic communications domain" and to adopt necessary legislative measures ensuring lawful processing of personal data. Nigeria and South Africa have made efforts to incorporate the

framework in their national legislation (Babalola, 2022). For India, which is not an African country, the ICCPR framework and Indian constitutional jurisprudence would be applicable. The overlap between international and regional legal standards and core principles of legality, necessity, proportionality, and judicial control forms the basis of the normative comparison conducted in the following sections.

1.4 Government Surveillance and Data Privacy in Nigeria

The legal framework under which government surveillance and data privacy in Nigeria operate creates an apparent contradiction. On the one hand, privacy under the Constitution is guaranteed in wide terms; yet on the other, there are numerous ways of infringing this guarantee in the interest of national security and crime prevention in particular. The above issue is very topical today. Pursuant to Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended), the right to privacy and freedom from infringement of this right with regard to a person, his or her home, correspondence, telephone communications, and telegraphic communications shall be inviolable. It is important to note that privacy of communication is specifically provided for and may embrace even modern communication (such as email or instant messaging). At the same time, the constitutional right in question is not an absolute one; like any other fundamental human right, it can be limited provided that the limitation can be seen as reasonable and justifiable in a democracy with regard to, for example, national security, public safety, or crime prevention and detection (Aloamaka, 2025).

One of the key issues in relation to Nigeria is the lack of detailed judicial interpretation of the exact extent of the right to privacy as protected under the Constitution of the country. While courts in such countries as India have developed clear constitutional standards with regard to privacy and surveillance, the Nigerian judiciary tends to approach issues in connection with privacy rather cautiously, and deference to executive assertions of national security has not helped develop a clear body of privacy jurisprudence (Singler and Babalola, 2025). As a result, constitutional guarantees often prove to be more theoretical than actual.

The main laws that regulate the issue of surveillance include the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Terrorism (Prevention) Act 2011, and the Nigeria Data Protection Act 2023. Taken together, they attempt to find the balance between security objectives and the right to privacy. It should be pointed out, however, that in most cases, the balance is in favour of the State. Under the Cybercrimes Act of 2015, law enforcement authorities are allowed to intercept electronic communication under certain conditions. Judicial approval is usually necessary, although it can pose a problem. With regard to evidence requirements,

limitation periods for issuing interception orders, time limits for data retention, and procedures for destroying any information gathered from suspects who do not eventually commit any offence, the legislation is silent. This means there could be variations in the implementation process and increased probability of arbitrariness in implementing surveillance laws.

The second piece of legislation that provides a wider scope for surveillance activities than the Regulation of Investigatory Powers Act (RIPA) is the Terrorism (Prevention) Act (Regulation of Investigatory Powers Act 2000 (UK); Section 14, 15, 28, 29-31 of the Terrorism (Prevention) Act 2011, Nigeria). In cases deemed urgent, surveillance can be carried out by government agencies without getting approval from the court, where delays could compromise ongoing investigations. It has been condemned by human rights scholars and civil society organisations on the grounds that they provide the opportunity for government agencies to use their discretion in determining the need for surveillance. Independent judicial scrutiny is vital in upholding surveillance from a human rights perspective since it ensures legality, necessity, and proportionality.

Moreover, there have been worries regarding the acquisition and use of highly advanced surveillance technologies by government bodies. The reports revealed that there have been greater government investments in advanced technologies that would enable surveillance on digital communications, even on encrypted ones. The rise in the surveillance power of technology has raised some concerns about the effectiveness of the laws governing this surveillance activity (Okpara and Okpara, 2025). According to Mahmoud, Yusuf and Olohunbebe (2025), while the technology is advancing quite fast, the laws and oversight mechanisms that can govern its use have failed to keep up with such advancements.

The introduction of the Nigeria Data Protection Act 2023 was a significant step taken in ensuring personal data protection in the country. It provides for an elaborate framework that governs the processing, transfer, storage, and even collection of any personal data within the territory of Nigeria (Unnam, 2015; Uwadinma, 2025). Moreover, it has set up the Nigeria Data Protection Commission that would be responsible for overseeing any issue pertaining to personal data protection. Furthermore, it also ensures that individuals enjoy some rights concerning their personal data (Odugbemi, 2026)

In spite of all the developments, there are wide exceptions made for activities related to national security, defence, public safety, and law enforcement under the Act. The exceptions make some forms of processing lawful even without consent in case such actions are required for the achievement of government interests (Modilim et al., 2024). While exceptions like these are standard for most of the existing data

protection legislation around the world, the main problem is that they are sometimes too broad and do not have adequate oversight processes. According to Unnam (2015) and Uwadinma (2025), such loopholes in the Act may weaken data protection provisions and allow surveillance measures to be conducted without being subject to any of the safeguards provided by the Act.

It should be noted that institutional independence continues to matter significantly. Even though the Nigeria Data Protection Commission is supposed to act as an independent supervisory body, it has been claimed that its autonomy might be jeopardised by the appointment process and other factors (Babalola, 2022). Data protection regulation would be effective only if supervisory authorities are able to carry out their functions independently from executive interference. From a human rights viewpoint, surveillance by the government can have legitimate objectives, like fighting terrorism, cybercrime, national security, and public order. But international human rights law mandates that any surveillance practice must meet requirements of legality, necessity, proportionality, and accountability (Hoofnagle, Sloat and Borgesius, 2019; Erickson, 2019; Chika and Tochukwu, 2020; Odugbemi, 2026). That means surveillance must be authorised by law, used where absolutely necessary, kept proportionate to the legitimate aim sought, and properly supervised.

In Nigeria, while some improvements have been made in recognising privacy as a constitutional right and developing an appropriate regime of data protection, there are still issues around overly broad statutory powers, overly broad exceptions on national security, limited judicial review, and lack of proper oversight mechanisms. As technology becomes more advanced in allowing for greater surveillance powers, there will be an increasing need to provide stronger legal safeguards against abuses of power.

1.5 Government Surveillance and Data Privacy in India

There is greater elaboration of the constitutional basis of privacy rights in India as compared to similar other nations because of the groundbreaking ruling of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India Judgment (2017). Before the judgment, it was still not clear whether privacy was a fundamental right within the scope of the Indian Constitution or not because there were conflicting decisions by courts before the Puttaswamy case. The confusion ended in 2017 when the nine-judge bench unanimously ruled that the right to privacy is a fundamental right in itself that falls under Article 21 of the Constitution, although the same right derives its protection from Article 14 and Article 19 of the Constitution. The Court defined privacy in very broad terms, not limiting it merely to the right to private property but including aspects of decision-making autonomy,

privacy of person and information (Pooja, 2023). An important point for discussion regarding privacy in relation to the use of new technologies is the potential threat that could be posed to the enjoyment of liberty and democracy due to the collection and analysis of personal data by governments (Bhandari and Lahiri, 2020; Kakkar et al., 2023). Consequently, the Court established that any limitation on privacy must satisfy the requirements of legality, legitimate state purpose, and proportionality. This constitutional standard reflects international human rights principles and has become the primary benchmark for evaluating surveillance measures in India.

The recognition of privacy, on the other hand, coexists alongside a far-reaching statutory framework for surveillance, which precedes the decision in Puttaswamy. Indeed, even prior to 2017, the Supreme Court was addressing issues related to privacy in *People's Union for Civil Liberties v Union of India* (1997) wherein the validity of telephone interception pursuant to the Indian Telegraph Act was called into question. While the court failed to recognise privacy as a fundamental right in this case, it laid down procedural rules for regulating the power of surveillance possessed by the executive. Such rules include, among others, the requirement for written authority, restrictions on the period for which an order for intercepting the messages may be valid, the grounds upon which such orders may be made, and review by special committees (Sonkar, 2026; Sidharth, 2024). However, these rules have been criticised as being inherently executive in character, inasmuch as they did not provide for judicial authorisation of surveillance prior to its initiation.

The relevant section of legislation in India governing digital surveillance is section 69 of the Information Technology Act (2000). The provision permits the central or state government to intercept, monitor, or decrypt any information transmitted through computer resources in case such an act is considered necessary in relation to national security, sovereignty, public order, friendly relations with foreign states, and the prevention and investigation of offences (Bhattacharya, 2026). Despite the fact that these purposes are acknowledged under international human rights laws as legitimate purposes, there is considerable apprehension about the scope of the statutory provisions. Mishra (2026) point out that the justification clause is sufficiently broad so that the government would have a wide margin of discretion in determining the need for interception, thus relaxing the requirement of restriction being justified by necessity.

One of the most serious flaws in section 69 of the IT Act 2000 is the failure to provide prior judicial authorisation for interception. In contrast with legal regimes that require prior judicial authorization for implementation, the Indian regime entrusts decision-making power solely in the hands of executive authorities (Arun, 2025; Athar et al., 2025). The issue at stake is whether such a setup can ensure

institutional independence since the branch which undertakes the surveillance exercise has considerable power over the process of authorising the act and its subsequent supervision. The process of surveillance oversight set out by the legislation places considerable reliance on surveillance review boards which consist of members of the executive. Many scholars argue that such a system does not ensure the level of external scrutiny required by the principle of proportionality in Puttaswamy (Sonkar, 2026). Another issue that may lead to the lack of external scrutiny and accountability is the absence of any obligatory provision which would compel the authorities to inform the affected parties about the surveillance being undertaken.

The issues mentioned above gained prominence during the controversy associated with the use of the Pegasus spyware against individuals who were journalists, activists of various sorts and members of the political opposition in India. The accusations pointed to the use of high-tech means of surveillance against individuals pursuing their democratic activities in a legitimate manner. While the Supreme Court of India created a special technical committee to look into the allegations, the lack of transparency remains an issue (Bhandari and Lahiri, 2020; Kakkar et al., 2023; Sidharth, 2024 and Sonkar, 2026). The controversy illustrated the practical consequences of a system in which surveillance operations may occur with limited independent oversight and where affected individuals may never become aware that their communications or devices were targeted.

India has complemented its legal Regime for surveillance with the Digital Personal Data Protection Act 2023, aimed at developing a comprehensive data protection Regime. The Act is the first of its kind for regulating matters pertaining to the collection, processing, storage, and utilisation of personal data (Arun, 2023; Modilim et al., 2024). Rights of individuals have been provided under the Act in the form of access, correction, erasure, and redressal of grievances. At the same time, various obligations have been imposed on data fiduciaries with respect to processing personal data lawfully and managing it responsibly (Bhandari and Lahiri, 2020; Sonkar, 2026). With such a law on the books, India seems to have made great progress in protecting informational privacy.

Despite all that, the efficacy of the Digital Personal Data Protection Act in regulating government surveillance practices has come under serious scrutiny. According to this act, the central government possesses wide powers in issuing exemptions from its requirements in regard to national security, sovereignty, public order, and other related issues (Modilim et al., 2024; Sonkar, 2026; Sidharth, 2024). The problem with these exceptions is that they severely weaken the effectiveness of the law in providing adequate protections because much of the most invasive data

collection and surveillance takes place through state agencies. Where there are exceptions to certain important protections, the law will be considerably weakened in its potential ability to serve as a mechanism for checking government excesses (Bhandari and Sane, 2018; Rana, 2026; Odugbemi, 2026). This means that the legal system remains characterised by the presence of a constitutionally guaranteed right to privacy on one hand and an extensive statutory regime of surveillance on the other. This debate is still continuing in contemporary times and revolves around issues pertaining to human rights and national security, questioning the compatibility of Indian surveillance laws with constitutional principles laid down in Puttaswamy and international human rights norms.

1.6 Government Surveillance and Data Privacy in South Africa

South Africa possesses one of the most comprehensive constitutional privacy frameworks in the world, due to a high level of respect for the dignity, personal autonomy, and freedom of individuals. The legal basis for protecting privacy can be found in Section 14 of the Constitution of the Republic of South Africa 1996, which provides that everyone has the right to privacy, which includes the right not to have his or her person or property searched, and not to have possessions seized, and not to have privacy of communication infringed (Gupta and Chima, 2019; Modilim et al, 2024; Chika and Tochukwu, 2020). Contrary to certain other constitutional articles, which may be written under the assumption that communication takes place only through traditional methods, Section 14 is written in a broad manner that includes modern forms of communication and electronic processing of information. Furthermore, in accordance with Section 36, the limitations of fundamental rights must be reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom (The Constitution of the Republic of South Africa 1996).

The jurisprudence of privacy law in South Africa can be considered a product of an integration of comparative constitutional traditions and the indigenous constitutional value of Ubuntu in South Africa (Sidharth, 2024). Cachalia and Klaaren (2023) have noted that South Africa's concept of privacy draws from the German concept of informational self-determination, the common-law concept of privacy in the United Kingdom, and the concept of ubuntu, which focuses on human dignity and personhood in South Africa. As such, privacy in South Africa cannot be considered simply an absence of intrusion but must also be considered as a positive state of being that allows individuals to grow and flourish. The judicial understanding of the concept of privacy has always been that it should encompass the individual's ability to control personal information and decide when, how, and

under what circumstances information regarding one's life may be revealed to others (Katzav, 2022; Coetzee, 2024; Ilori and Killander, 2025)

Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) is the primary legislative framework controlling state surveillance activities in South Africa. The statute was passed to control the situations when communications could be legally intercepted. Contrary to the surveillance laws implemented in various other nations, RICA mandates judicial intervention before interceptions can take place and identifies the designated judge who hears interception applications (Swales, 2022). Such an element of the surveillance law was introduced into the statute in order to prevent abuses associated with the exercise of interception powers and to ensure that interceptions could take place only in cases of necessity. Still, certain issues arose about the sufficiency of safeguards introduced by the Act and the extent of surveillance conducted by the State authorities (Staunton and Stadler, 2019; Swales, 2022).

Such issues found their culmination in the decision of the Constitutional Court in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (2021). It was one of the most prominent judicial reviews on the matter of surveillance powers. The Court found that RICA had certain deficiencies from the constitutional perspective. However, it found that the Act does not provide any provision to notify people after they have been under surveillance; thus, they cannot make a challenge against the violation of the interception process and get legal remedies. It also argued that the judge authorised to permit interception was not institutionally independent enough for impartial surveillance, which led to further worries (*AmaBhungane case*, 2021; Sonkar, 2026). Additionally, there were no guarantees regarding *ex parte* interceptions, storage of material interceptions and destruction thereof and communication confidentiality between the legal practitioners and media workers (Bhandari and Lahiri, 2020; Sidharth, 2024).

The decision of the Constitutional Court was important for several reasons. First, it was about the legitimacy of bulk surveillance. In particular, it was decided that South African legislation does not allow bulk surveillance based on general national security considerations. Thus, no legal basis exists for indiscriminate mass interception. The principle of constitutionality of surveillance was established, whereby surveillance needs to be justified, authorised, and proportionate. Thus, the Constitution prohibits bulk interceptions for security purposes as disproportionate measures. The decision has been widely regarded as a major victory for privacy rights and democratic accountability because it subjected surveillance legislation to

rigorous constitutional scrutiny and emphasised the need for effective safeguards against abuse (Swales, 2021)

In addition to constitutional guarantees and judicial review, South Africa has also established a data protection regime through the adoption of the Protection of Personal Information Act 4 of 2013. Coming into full effect in 2021, POPIA provides extensive regulations pertaining to the collection, processing, storage, and disclosure of personal information by both public and private entities. The Act is premised on eight basic principles relating to accountability, lawful processing, purpose specification, transparency, quality of data, security measures, and participation of the data subject (Leipsig, 2025). By providing clear rights and obligations, POPIA aims to promote informational privacy in an increasingly digital world.

An important aspect of POPIA is the establishment of the Information Regulator, which is tasked with overseeing compliance, carrying out investigations, conducting audits, enforcing compliance notices, and punishing violators. The independence of the Information Regulator makes the South African data protection regime unique in the sense that many countries rely on regulatory agencies that are heavily influenced by the executive branch of government. Although POPIA contains exemptions relating to national security, law enforcement, and public safety, these exemptions are generally narrower than those found in comparable legislation in several other jurisdictions and remain subject to oversight mechanisms (Singh and Power, 2019). The Information Regulator has demonstrated a willingness to enforce the Act against both public and private entities, thereby reinforcing confidence in the effectiveness of the regulatory framework.

While these accomplishments may appear substantial, the governance regime surrounding South Africa's use of surveillance still faces difficulties. In Ama Bhungane (2021), the Constitutional Court deferred its declaration of invalidity to give Parliament a chance to fix the constitutional violations contained in RICA through amendments. As a result, the legislative process has been slow, leaving room for concern about the effectiveness of South Africa's regulations regarding surveillance (Ilori and Killander, 2025). While the delay leaves open the question of the efficacy of surveillance regulation, and the extent to which constitutional principles can be actualized without legislative reform, South Africa nevertheless has a much stronger legal tradition around surveillance than most countries (Ilori, 2021). This is because, unlike many other nations, South Africa's constitutional safeguards, combined with its judicial oversight system, the lack of bulk data collection, and data protection authority, make it one of the best legal traditions in the world.

1.7 Comparative Synthesis: Common Deficits and Jurisdictional Distinctions

The comparative analysis of Nigeria, India, and South Africa reveals that what poses the biggest threat to adequate privacy protection is not the failure to acknowledge privacy rights in their respective constitutions, but rather the presence of broad national security exceptions that grant the executive branch an excessive degree of freedom (Bhandari and Lahiri, 2020). Even though the three jurisdictions have constitutional provisions that acknowledge the existence of privacy rights in the countries and pass the relevant legislation on personal data and surveillance activities, the legal system of all three remains such that it grants the executive a great deal of power in case national security interests, public order, and law enforcement concerns arise (Cachalia and J Klaaren, 2023).

Despite differences in the specific legal devices used to exercise such discretion, the results remain similar across the three countries analysed above. For example, Nigeria's Cybercrimes Act and Terrorism Prevention Act grant wide-ranging powers to carry out surveillance actions, including communications interception and personal data access, while at the same time offering no clear procedural safeguards to be adhered to (Modilim et al., 2024). This results in a surveillance regime where executive agencies have significant discretion to operate without corresponding transparency and accountability measures. India, on the other hand, experiences such an issue through the synergy between Section 69 of the Information Technology Act and the numerous exemptions provided in the Digital Personal Data Protection Act. With wide legal grounds to conduct interceptions in combination with the lack of necessity for mandatory judicial approval prior to conducting surveillance operations, the regime creates room for executive agencies to exercise discretion regarding the appropriateness of initiating surveillance (Staunton and Stadler, 2019).

In South Africa, there was an analogous case of the same challenge based on the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act through engaging in surveillance that went beyond the statutory boundaries. Nonetheless, judicial review through the judgment made in the *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (2021) helped reduce this activity within its constitutional boundaries.

One major lesson drawn from this comparison is the fact that, by themselves, constitutional guarantees of privacy may not translate to effective means of combating surveillance practices by the state government. What makes these guarantees effective depends upon the existence of independent institutions which

can ensure enforcement against the executive branch of the government (Odugbemi, 2026).

In the absence of such institutions and where there are broad national security exceptions together with weak oversight measures, constitutional guarantees of privacy tend to be meaningless. As such, constitutional guarantees cannot guarantee privacy protection alone without strong institutional designs and enforcement capacity (Unnam, 2015; Sonkar, 2026; Sidharth, 2024). The three countries present varying degrees of judicial intervention in surveillance governance. South Africa presents a stronger example of judicial oversight in surveillance governance through its Constitutional Court's active enforcement of constitutional limitations on surveillance powers. For instance, in its decision in *AmaBhungane Centre for Investigative Journalism v Minister of Justice* (2021), the court enforced strict proportionality analysis and declared deficiencies in existing laws dealing with surveillance practices before requiring reforms to the surveillance legislation. Clearly, South Africa's constitutional court shows a strong rights-oriented judicial culture with an enforcement mandate of constitutional guarantees.

India occupies a middle position. The landmark judgement by the Supreme Court in *Justice K. S. Puttaswamy (Retd.) v Union of India* (2017) has unequivocally made privacy a fundamental right that has to meet a well-defined test for proportionality. The tests involve legality, legitimacy, and necessity. However, implementation of such judicial doctrines has been sporadic, with examples including the criticisms surrounding the Pegasus controversy and the alleged lack of judicial oversight in those cases. In effect, even though the doctrine itself is powerful, its implementation is inconsistent.

Nevertheless, judicial oversight in the Nigerian case still stands out as the least advanced amongst the three countries. Even though Section 37 of the Constitution of the Federal Republic of Nigeria recognises the right to privacy, there is a lack of landmark judicial pronouncements such as the Puttaswamy decision in India or the AmaBhungane decision in South Africa that clarify the extent of surveillance allowed within the constitutional framework (Modilim et al, 2024; Chika and Tochukwu, 2020). As such, the review standard for evaluating surveillance is weak, giving room for considerable discretion on the part of the executive.

On the institutional front, data protection institutions exist in all three countries, although with varying levels of effectiveness. The Information Regulator of South Africa is seen to be more independent than others, as well as being proactive in investigating both government and corporate actions regarding data protection and issuing enforcement directives. This gives greater strength to

accountability mechanisms and enhances the realization of privacy rights through the same. In the case of Nigeria and India, issues arise with regard to the structural independence of the respective Data Protection Commissions and Boards. India is a case where the Board lacks the power of oversight due to the discretionary nature of the government's powers under the Digital Personal Data Protection Act, where any surveillance may be covered by an extremely wide national security exception (Modilim et al, 2024; Chika and Tochukwu, 2020; Odugbemi, 2026).

One weakness found in all three nations is the lack of transparency and notification provisions. Many instances of surveillance go unnoticed because individuals who are monitored do not even know about it. For challenging any illegal surveillance, knowledge regarding the surveillance is vital. South Africa has a possible remedy in the form of the AmaBhungane judgment, whereby the Constitutional Court of South Africa highlighted the importance of post-surveillance notification as necessary for effective judicial review of surveillance. While there are no such provisions in Nigeria and India, privacy can only be improved in these nations by having more oversight institutions, less extensive national security exceptions, and more transparency provisions.

1.8 Conclusion

It has been shown that there is a constant balance maintained in relation to government surveillance in Nigeria, India, and South Africa concerning national security and the protection of fundamental human rights. Although privacy has been enshrined as a right in their constitutions and regulations have been passed in order to control personal data and communications, there remains a lot to be achieved in terms of bridging the gap between theoretical provisions and practical governance (Bhandari and Lahiri, 2020). It appears that the key issue that needs to be addressed is not the lack of privacy provisions but the existence of extensive surveillance powers, exemptions under the guise of national security, insufficient oversight and a lack of transparency in government practices of surveillance (Kakkar et al. 2023).

What can be observed from these cases is the varying degree of development of the legal system in each of the states studied. South Africa stands out due to its well-developed privacy provision, Constitutional Court and independent data protection authority. For example, the court ruled in the AmaBhungane case that surveillance laws must undergo constitutional scrutiny. It should be noted that India has achieved the creation of a comprehensive constitutional framework on account of the Puttaswamy decision. It involves acknowledging privacy as a fundamental right subject to restrictions based on the principle of legality, legitimate purpose, and proportionality (Sonkar, 2026; Sidharth, 2024). Nonetheless, the enforcement of

these criteria in practice is far from being reliable, especially concerning issues related to national security and intelligence activities. Nigeria has both the constitutional right to privacy and an adopted data protection framework; however, it still struggles with problems associated with enforcement of privacy rights through the courts and lack of regulatory oversight (Chika and Tochukwu, 2020; Odugbemi, 2026).

In the context of comparison, it can be argued that privacy rights need more than just constitutional recognition for effective implementation. This is because privacy needs an independent court system, strong regulatory bodies, a well-designed mechanism of regulation, and surveillance legislation that is proportionate to the purposes of its adoption (Athar et al., 2025). Otherwise, the constitutional right to privacy will remain nothing more than declarative. In any case, the protection of the right to privacy is about ensuring the balance between national security on one hand and the freedom of people, their dignity, and personal autonomy on the other hand.

1.9 Recommendations

To enhance privacy rights while taking care of legitimate security concerns, the following recommendations are put forth for implementation in all three jurisdictions. Firstly, all surveillance should be conducted only after obtaining prior judicial authorization. Authorisation by the courts would guarantee protection from any arbitrary or unreasonable surveillance activity, and thus it would be consistent with the constitutional and international requirements. Secondly, there should be a legislative provision of post-surveillance notification once the threat has been removed. Post-notification will enable people to dispute such surveillance and is an important tool for ensuring accountability.

Thirdly, there should be limited national security exceptions under data protection law and be open for independent review by regulators. Regulators, like data protection authorities, should have the power to undertake confidential inspections of security and intelligence services to make sure that their activities are consistent with law and the principles of human rights. Finally, each jurisdiction needs to set up special parliamentary oversight committees that can deal with surveillance practices and look into classified documents and issue reports. The implementation of these reforms would significantly strengthen the protection of privacy rights while ensuring that surveillance powers remain necessary, proportionate, and subject to effective oversight in accordance with constitutional and international human rights obligations.

REFERENCES

- Adeoti, E. A. (2023). A new era of data protection and privacy: Unveiling innovations & identifying gaps in the Nigeria Data Protection Act of 2023. SSRN. <https://doi.org/10.2139/ssrn.4520238>
- Aloamaka, P. C. (2025). A critical analysis of the Nigeria Data Protection Act 2023: Elevating standards to global norms. *UCC Law Journal*, 154.
- Arun, P. (2023). A mosaic of dovetailing laws: India's communications surveillance regime. *Indian Law Review*, 7(3), 302–321.
- Arun, P. (2025). Regressive and authoritarian: Surveillance powers in the Telecommunications Act 2023 and Post Office Act 2023. *Indian Law Review*, 9(1), 80–99.
- Athar, S., Gosain, D., Feldmann, A., Kaur, M., & Dao, H. (2025). Nobody should control the end user: Exploring privacy perspectives of Indian internet users in light of DPDPA. *Proceedings on Privacy Enhancing Technologies*, 115–134.
- Babalola, O. (2022). Nigeria's data protection legal and institutional model: An overview. *International Data Privacy Law*, 12(1), 44–58.
- Bhandari, V., & Lahiri, K. (2020). The surveillance state, privacy and criminal investigation in India: Possible futures in a post-Puttaswamy world. *University of Oxford Human Rights Hub Journal*, 3(2), 15–35.
- Bhandari, V., & Sane, R. (2018). Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018. *Socio-Legal Review*, 14(2), 143–168.
- Bhattacharya, G. (2026). Cybersecurity and data protection laws in India: Challenges and prospects. *ShodhKosh: Journal of Visual and Performing Arts*, 7(7), 550–562.
- Cachalia, F., & Klaaren, J. (2023). Towards a public law perspective on the constitutional law of privacy in South Africa in the age of digitalization. *Journal of African Law*, 67(1), 112–130.
- Chika, D., & Tochukwu, E. (2020). An analysis of data protection and compliance in Nigeria. *International Journal of Research and Innovation in Social Science*, 4(5), 377–385.
- Coetzee, J. (2024). Cross-border data flows and the Protection of Personal Information Act 4 of 2013—Part I: The territorial scope provision. *Potchefstroom Electronic Law Journal*, 27, 142–165.
- Erickson, A. (2019). Comparative analysis of the EU's GDPR and Brazil's LGPD: Enforcement challenges with the LGPD. *Brooklyn Journal of International Law*, 44, 859–890.

- Foucault, M. (1991). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Penguin. (Original work published 1975)
- Gupta, A., & Chima, R. S. (2019). State surveillance and the right to privacy in India. *National Law School of India Review*, 11(2), 109–128.
- Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. *International Journal of Law and Information Technology*, 28(1), 65–98.
- Ilori, T. (2021). Framing a human rights approach to communication surveillance laws through the African human rights system in Nigeria, South Africa and Uganda. *African Human Rights Yearbook*, 5, 147–171.
- Ilori, T., & Killander, M. (2025). Special focus: Communication surveillance law and human rights in Africa. *African Human Rights Law Journal*, 25, 774–786.
- Jemilohun, B. O. (2015). An appraisal of institutional framework for data protection in the UK, USA, Canada and Nigeria. *Journal of Asian and African Social Science and Humanities*, 1(1), 8–24.
- Kakkar, J., et al. (2023). The surveillance law landscape in India and the impact of Puttaswamy. Centre for Communication Governance.
- Katzav, G. (2022). Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act. *South African Law Journal*, 139(2), 432–455.
- Leipsig, C. (2025). Regulating automated decision-making: An analysis of section 71 of POPIA and its implications for privacy and data protection. *Pretoria Student Law Review*, 18(1), 212–234.
- Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.
- Mahmoud, R. F., Yusuf, E., & Olohungebe, M. (2025). Blockchain and data privacy in Nigeria: Reconciling innovation with the Nigeria Data Protection Act 2023. *Agora International Journal of Juridical Sciences*, 19(2), 206–223.
- Mishra, N. (2026). The emerging framework for non-personal data protection in India: Perils, promises, and lessons for the developing world. *International Journal of Law and Information Technology*, 34, 123–145.
- Modilim, S., et al. (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 and Humanities*, 143–162.
- Nayyar, A. (2025). Privacy in the digital economy: How the Indian government interprets the fundamental right to informational privacy. *Privacy Studies Journal*, 4, 126–148.

- Odugbemi, G. (2026). Privacy in public: Can Nigeria's Data Protection Act regulate street recording? SSRN Working Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6428678
- Okoro, U., et al. (2026). Governance and regulation of artificial intelligence in developing countries: A case study of Nigeria. arXiv. <https://arxiv.org/abs/2604.06018>
- Okpara, E. T., & Okpara, E. C. (2025). The Nigeria Data Protection Act, 2023 and the right to privacy: Constitutional implications under the 1999 Nigerian Constitution (as amended). *Alex Ekwueme Federal University Law Journal*, 2, 43–61.
- Pooja, G. N. (2023). Justice K. S. Puttaswamy (Retd) v Union of India & Ors: A contemporary review of the right to privacy. SSRN Working Paper. <https://ssrn.com/abstract=4468344>
- Rana, H. (2026). Balancing privacy and power: A critical study of India's data protection regime after Puttaswamy. *Indian Journal for Research in Law and Management*, 3(8), 112–129.
- Sabo, S., & Utulu, S. (2023). Organisation studies based appraisal of institutional propositions in the Nigerian Data Protection Regulation. arXiv. <https://arxiv.org/abs/2309.12893>
- Sidharth. (2024). Surveillance vs privacy: Balancing national security and individual rights in India. *International Journal of Creative Research Thoughts*, 12(5), 121–130.
- Singh, A., & Power, M. (2019). The privacy awakening: The urgent need to harmonise the right to privacy in Africa. *African Human Rights Yearbook*, 3, 199–219.
- Singler, S., & Babalola, O. (2025). Digital colonialism beyond surveillance capitalism? Coloniality of knowledge in Nigeria's emerging privacy rights legislation and border surveillance practices. *Social & Legal Studies*, 34(5), 102–123.
- Sonkar, A. (2026). Privacy after Puttaswamy: Constitutional boundaries of state data collection under the Digital Personal Data Protection Act, 2023. *Law and Justice Research Centre Review*, 209–228.
- Staunton, C., & de Stadler, E. (2019). Protection of Personal Information Act No. 4 of 2013: Implications for biobanks. *South African Medical Journal*, 109(4), 109–111.
- Swales, L. (2021). The Protection of Personal Information Act and data de-identification. *South African Journal of Science*, 117(7/8), 321–327.

- Swales, L. (2022). The Protection of Personal Information Act 4 of 2013 in the context of health research: Enabler of privacy rights or roadblock? Potchefstroom Electronic Law Journal, 25, 149–171.
- Unnam, D. U. (2015). Informational privacy and security amid growing activities on electronic platforms in Nigeria: A case for data protection law. Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 6, 27–40.
- Uwadinma, I. A. (2025). The digital economy and consumer protection in Nigeria: A legal analysis of data privacy laws under the Nigeria Data Protection Act 2023. AUN Journal of Law, 50–69.
- Westin, A. F. (1967). Privacy and freedom. Atheneum.