ISSN: 2581-4311
DOI: doi.org/10.30967/IJCRSET/Ashimi-Saoban-Adedayo/213

URF PUBLISHERS
connect with research world

International Journal of Current Research in Science, Engineering & Technology

https://urfpublishers.com/journal/ijcrset

Vol: 9 & Iss: 1

Research Article

Privacy Rights and Cybercrime Investigations in Nigeria: Reconciling National Security with Human Rights

Ashimi Saoban Adedayo* and Adeyemo Habeebullah Adekunle

University of Ilorin, Ilorin Kwara State Nigeria

Citation: Adedayo AS, Adekunle AH. Privacy Rights and Cybercrime Investigations in Nigeria: Reconciling National Security with Human Rights. *Int J Cur Res Sci Eng Tech* 2025; 9(1), 556-570. DOI: doi.org/10.30967/IJCRSET/Ashimi-Saoban-Adedayo/213

Received: 23 February, 2026; **Accepted:** 27 February, 2026; **Published:** 02 March, 2026

***Corresponding author:** Ashimi Saoban Adedayo, University of Ilorin, Ilorin Kwara State Nigeria

ABSTRACT

The tension between privacy rights and cybercrime investigations in Nigeria is transparent beyond the slightest ambiguity. As cybercrimes such as fraud, business email compromise schemes, illicit child exploitation, cryptojacking and hacking among others augment in scale and sophistication, law enforcement agencies have intensified digital surveillance and data access practices. However, these measures frequently conflict with constitutionally protected privacy right under Section 37 of the 1999 Constitution of Federal Republic of Nigeria (as altered) and international human rights standards. This paper underscores the relevant legal frameworks, particularly the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 alongside judicial attitudes towards privacy intrusions in the context of criminal investigations. The conflict between privacy rights and cybercrime investigation is examined alongside an examination of the Nigeria Data Protection Act 2023 (NDP Act 2023) enacted in reforming the overall legal framework for data protection. Furthermore, the paper explores the justification for state interference with privacy on grounds of national security and the principles that must govern such interference, namely necessity, proportionality and oversight. Challenges such as loopholes in Cybercrime Act, political misuse of surveillance for non-security purposes which basically amounts to misuse of the power are duly addressed. Finally, the paper proposes a balanced approach in safeguarding privacy rights while combatting the menace of cybercrime[1,2].

Keywords: Privacy; Cybercrime; Cybersecurity; Communication; Surveillance; Nigeria

Cybercrime rise in nigeria

Following the continuous growth and acceptance of technology in Nigeria, crimes have gone from being committed physically alone, to being committed digitally. Cybercrime involves using computers and the internet to commit crimes, including types such as child exploitation, cryptojacking, cyberespionage, cyberextortion, identity theft, malware and hacking, while cybersecurity is a rapidly growing field within Information and Communication Technology that focuses on reducing organizations' risk of hacks and data breaches[3].

Coming with technological advancements are cybercrimes like hoofing phishing attacks, ransomwares, cyber bullying amongst others. Although, following the continuous rise of cybercrimes in Nigeria, there have been a primary Act which has been enacted to address the issues of cyber-crimes, which is the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. But the question is, how effective is it?

Despite this dedicated legislation and improved technological adoption in the investigation and prosecution of cybercrime, Nigeria remains one of the hotbeds of cybercrime.

The Nigeria Communications Commission (NCC) reported that the country loses an estimated $500 million per annum to cybercrime. Nigeria's leading anti-corruption agency, the Economic and Financial Crimes Commission (EFCC), has recorded a consistent increase in cybercrime prosecution figures. In a three-year period, the conviction figures by the EFCC more than tripled. Specifically, in 2020, the EFCC recorded a total of 976 convictions. In 2021, this figure had increased to 2,220 convictions. By 2022, this figure had jumped to 3,785 convictions. While these figures are not all cybercrime, a majority of them are related to cybercrime[4].

Importance of privacy rights in democratic societies

Democracy thrives best when individuals are free to live their lives without any form of intrusion in their private life, without surveillance or undue interferences in their personal lives. For that reason, everybody is left to make decisions as they so wish, elect who they want as their leaders and many other things. Additionally, personal autonomy enables individuals to make choices without undue interference, while free expression empowers people to voice their opinions and beliefs without fear of retribution. However, the right to privacy can sometimes be misused, potentially leading to derogation from such rights. Moreover, privacy rights may pose threats to national security if misused for malicious activities. In some instances, privacy can also shield harmful behavior, thereby causing social harm.

In this wise, striking a balance between protecting privacy rights and addressing societal needs is pivotal in democratic societies, ensuring that individual freedoms are preserved while also safeguarding the greater good.

Legal foundations of privacy and cybercrime investigation in Nigeria

Privacy rights refer to the freedoms of individuals to have their private life to themselves without any form of intrusion by an external person and to either use or disclose their information. In the words of American Judge, Thomas Cooley, it could be described it as "the right to be let alone."

Scope of privacy rights

The context of privacy rights encompasses the fundamental freedoms that safeguard individuals' personal information, autonomy and private lives from unwarranted intrusion, interference surveillance, with a guarantee of human dignity, liberty and security in both physical and digital spaces. The following are the areas covered by privacy rights:

- **Physical privacy:** Physical privacy is the type of privacy which a person has over his physical personal life in order to protect himself from any intrusion to his physical space ranging from his body to his properties. It is trite in law that a person is protected from being touched anyhow by any person without the consent of such person. In the case of Collins v Wilcock,[5] the court clarified the meaning of battery as a touching of another with hostile intent or in other words any intentional touching outside of the scope of what normally acceptable. Although there's exception to touching, by the principle of implied consent through the conduct of one's daily life activities.
- **Informational privacy:** This is a protection one has over personal and sensitive information which are not easily disclosed to the public. This ranges from his private medical records, to his financial life down to his family records. Except those privileged to have these types of information, any other person is excluded from getting access to them without the consent of the owner. Even those privileged to have the information still require the consent of the owner either expressly or by implication and an unauthorized access may result in an action against such intruder.
- **Communications privacy:** Communications like phone calls, emails, social media texts and other form of correspondences are protected under here. A notable example is while using instant messaging social media apps like WhatsApp. In every DMs, it is always stated that chats and calls are end to end encrypted and only people in the chats can read or listen to them. Not even WhatsApp has access to them. Although debatable, the extent of the truth, but inclusion of that signifies that Meta (the mother company of WhatsApp) acknowledge the importance of communications privacy.

Nature of cybercrime investigation

Cybercrime investigation refers to the use of legal skills combined with tech skills to identify a cybercrime, analyse it and trace it to the attacker. Cybercrime investigation involves skilled professionals from agencies like the FBI, NSA, Secret Service and others, using digital forensics to track, analyse and dismantle types of cyber-crime and cyber threats[6].

Some of the techniques cybercrime investigators utilize include collecting, preserving and analysing data from computers, phones, mobile networks; tracing the source, particularly IP address of where the data emanated from and using that as a trace to tracking down the cyber-criminal.

Constitutional basis: Section 37 of the 1999 constitution

It goes without saying that privacy is an essential thing in a well-functioning democratic society, as without privacy, there's basically no freedom for people to hold their opinions, dignity or make independent decisions by themselves. Due to that, the 1999 Constitution of the Federal Republic of Nigeria (as altered) has provided for privacy right in Section 37 worded as the Right to private and family life[7].

That serving as a foundation, it is pertinent to know that having a constitutional basis, an action against any form of infringement on privacy is actionable in a court of law.

Lawful interception & Data retention under the cybercrime act 2015

The notable enactment for cybercrime in Nigeria is the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Section 21 of the Act provides records retention and protection. By virtue of Section 21(1), "a service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being responsible for the regulation of communication services in Nigeria."

Furthermore, Section 21(4) and (5) state; "Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction." (5) "Anyone exercising any function

under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement." Section 21(6) then provides for the punishment of going against the Act. "Subject to the provisions of section 20 of this Act, any person or entity who contravenes any of the provisions of this section commits an offence and is liable on conviction to imprisonment for a term of not less than three year or a fine of not less than N7,000,000.00 or to both fine and imprisonment.

Flowing from the above, it is seen that the Act provides for the people entitled to holding information, as well as the extent to which they have the power, as well as the punishment of not complying with the provision of the act[8].

Relevant International Instruments: African Charter on Human and Peoples' Rights; ICCPR

As intrusion of privacy is not only prevalent in Nigeria, it is something that could happen anywhere. So to say, it's not only Nigerian enactments that provide for the protection of human privacy. There are international instruments that also make provisions for it, some of these include African Charter on Human and Peoples' Rights, International Covenant on Civil and Political Rights (ICCPR) and many others. By virtue of Article 17 of ICCPR, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

Conflict between privacy rights and cybercrime investigation

A cybercrime investigation is kickstarted with a check on a user's computer system documentation, system logs, background and personnel. If a suspect is identified, the investigator will find out the equipment used and the depth of the expertise of such person. Cybercrime investigations may impact the enjoyment of numerous human rights like right to a fair trial, freedom of expression as it is not limited to privacy which is the focus of this paperwork. The quest for cybersecurity has taken centre stage in global policy due to increased cyber criminality, including identity thefts, distributed denial of service (DDOS), internet hacking and even cyberterrorism, the prevention and prosecution of which may require authorities to access or collect personal data from third parties, including business enterprises or to intercept, disclose or share digital communications and intelligence data. This has made the protection of online privacy more challenging[9].

Right in place is the Nigeria Data Protection Act 2023 (NDP Act 2023) enacted in reforming the overall legal framework for data protection. However, the NDP Act 2023 exempts from its purview, subject to the human rights provisions of the Constitution and their limitations, the processing of personal data carried out by a 'competent authority' as is necessary for the purposes of the prevention, investigation, detection, prosecution or adjudication of a criminal offence or the execution of a criminal penalty prevention or control of a national public health emergency as is necessary for national security[10].

The non-specified 'competent authorities' would in the real sense include government agencies like the Economic and Financial Crimes Commission (EFCC) have been tasked with preventing financial crimes, including online fraud, given the country's large internet population as well as the national security agencies established under the Nigeria Security Agencies Act 1986. These are the Defence Intelligence Agency (DIA), the National Intelligence Agency (NIA) and the State Security Service (SSS).

The Nigerian Communications Act 2003 obligates licensees or service providers upon written request by the Commission or any other authority, to assist as far as reasonably necessary in preventing an offence, enforcing the law and in the preservation of national security[11].

Going further, Section 146(3) of the Nigerian Communications Act protects licensees from any liability while carrying out any such duty. This could be in the event of a public emergency, in the interest of public safety, to protect national security and so forth.

The LICR 2019 permits an 'authorised agency' such as the State Security Service (SSS) and the Office of the National Security Adviser (NSA) to intercept any communication in Nigeria based on a court warrant. Warrantless interception and monitoring of online communications are authorised to prevent danger to human life or where otherwise necessary, although judicial authorisation must be obtained within 48 hours thereof. The authorised agencies must submit an annual report of all concluded interception cases to the Attorney General of the Federation (AGF)[12].

Above all, the digital transformation of the Nigerian society has led to a dramatic rise in cybercrime, prompting Nigerian authorities to adopt aggressive investigative methods. However, these efforts often place privacy rights, enshrined under Section 37 of the 1999 Constitution of Federal Republic of Nigeria (as altered)[13], in direct conflict with national security imperatives. Striking a balance between these competing interests remains a fundamental challenge for Nigeria's legal system.

Cybercrime investigations in Nigeria typically involve mass surveillance, interception of communications, access to private data and search and seizure of digital devices. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 grants law enforcement broad powers to monitor electronic communications, particularly under Sections 38 to 41. Practically, the resultant effect of this avenue is that authorities can gain access to emails, social media accounts and financial information, sometimes without sufficient judicial oversight.

The case of Digital Rights Lawyers Initiative v. National Identity Management Commission[14] is apt in this regard. In this case, the Appellant filed an appeal, at the Court of Appeal, which was also dismissed. However, the Court issued far-reaching resolutions touching on privacy and data protection in Nigeria. It upheld the trial court decision that the right to privacy under the impugned section includes the right to protection of personal data and personal information. The Court of Appeal also observed that the Nigerian Data Protection Regulation must be construed as providing such legal instruments that safeguards the right to privacy of its citizens as it relates to protection of personal data or personal information.

Ordinarily, the designated agencies justify such intrusions basically on grounds of national security, public safety and crime prevention. This argument is rooted in Section 45 of the Constitution, which permits the restriction of certain

fundamental rights in the interest of public order, morality or health. Nigerian authorities contend that cybercrime including online fraud, identity theft and cyberterrorism poses serious threats that necessitate preemptive surveillance and data access. Through the Cybercrimes Act, law enforcement is empowered to act swiftly to secure digital evidence, disrupt criminal networks and protect critical national infrastructure. The justification, therefore, centers around the principle that national survival and public security outweigh individual privacy when appropriately regulated.

Nigerian courts have demonstrated cautious deference to state interests while reaffirming the necessity of protecting human rights. In EFCC v. Diamond Bank Plc[15], the court held that the bank breached its duty of care by placing a PND on the claimant's account without demanding a valid court order from the EFCC, describing the bank's actions as negligent and unlawful. The judge emphasized that neither the EFCC nor the bank had the legal authority to unilaterally freeze a customer's account without court authorization and condemned the practice as contrary to the rule of law. The court addressed the tension between financial surveillance and privacy, emphasizing that while financial institutions may cooperate with investigations, privacy must not be violated arbitrarily.

Similarly, in Federal Republic of Nigeria v Abdulrasheed Maina Dikko & Anor case, the court upheld the freezing of bank accounts linked to suspected cybercrimes but stressed that such actions must be authorized by a court order to avoid unconstitutional violations of privacy and property rights. The case affirms that cybercrime investigations must adhere to procedural safeguards to reconcile national security concerns with fundamental human rights.

These judicial authorities conjunctively illustrate that Nigerian jurisprudence attempts to maintain a striking balance, although law enforcement practices often straggle judicial pronouncements.

Legal and practical challenges in reconciling privacy and security

The task often is that, how does one reconcile the trend of increasing security while upholding the fundamental rights and privacy of citizens without through surveillance infringe on their privacy? In some instances, the authorities intrude people's privacy as citizens and base their justification on protecting citizens against cyber-attacks, while the main purpose of doing is actually not to protect citizens. Some of the notable challenges include:

- **Overbroad investigation powers: Loopholes in cybercrime act:** It is only ideal to say that every legislator while making a law does not necessarily have the intention of totally erasing a crime, as there will in a way or other be loopholes in the enacted Act. So does that apply to the Cybercrime Act. According to Mr Emmanuel Edet, Head Legal Services & Board Matter Unit, National Information Technology Development Agency (NITDA), "one of the challenges we had when going through the law was definitions. There is a danger of confusion when we use specific definitions. For example, if we say someone commits a crime with an ATM machine and in the future, we have another machine that is not called ATM to commit fraudulent act, that means, by definition, the person has not committed any offence or done anything wrong." Similarly, Mr. Alex Mouka, an erstwhile NBA Lagos Chairman, criticized the law, calling it "structurally deficient" and "irresponsible legal legislation." He expressed concerns about its drafting and effectiveness[16].
- **Abuse of powers/Political misuse of surveillance for non-security purposes:** Due to no demand of accountability by citizens, authorities sometimes abuse their powers by utilizing surveillance tools to monitor activities of oppositions, citizens, journalists, activists whose activities pose threat to the government and other people. There are widespread violations of laws relating to surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations finds that over 90 countries engage in illegally monitoring the communications of political opponents, human rights workers, journalists and labour organizers[17].

Towards a balanced approach: Safeguarding privacy while combating cybercrime

Privacy protection is an essential thing for humans in the society, so is the security to ensure that people are not harmed. However, security sometimes requires infringement of people's privacy which often causes conflicts between the two concepts. Balancing things between the two concepts is an essential thing as it ensures safe space on the internet and also ensures upholding of human rights. The General Data Protection Regulation (GDPR), implemented by the European Union in 2018, is an example of legislation that prioritises individual privacy rights. The GDPR requires companies to obtain explicit consent from users before collecting their personal data and provide them with the right to access, correct and delete their data. Companies that fail to comply with these regulations face severe penalties, including fines of up to 4% of their global revenue.

However, some argue that privacy regulations can hinder security efforts. For instance, the US government has been in conflict with technology companies such as Apple over their refusal to provide access to encrypted data on their devices. The government argues that access to this data is crucial for national security purposes, while Apple maintains that granting access would compromise user privacy and security[18]. Pavel Durov, the founder of Telegram also faced series of issues with the government for not allowing access to people's data on the platform. This led to a serious of issues with the government.

It is worthy of note that although, they are agents of the states, security agents are human just like the people that own these data, they having unnecessary access to these data can be used to harm these people or give out information about them. Personal data tells a lot about people, their preferences, their ideas and basically their way of life. Having access to these data may be harmful to their lives.

In a bid to balance things between these two things, there must be a key relationship between lawmakers, technological companies and users, as although the privacy of user's matter, so does the society's security.

- **Necessity and proportionality principles:** The principle of necessity requires that restriction be placed on privacy rights, as long as doing that is necessary to sustain the

security of the nation. Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. Necessity is also fundamental when assessing the lawfulness of the processing of personal data. The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing. The principle of proportionality requires that actions taken by the state should be proportionate to the aim being pursued. More specifically, the limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure. A pre-condition is that the measure is adequate to achieve the envisaged objective. In addition, when assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed[19].

- **Public awareness and digital rights education: Empower citizens to demand accountability:** Most countrymen don't demand accountability from the authorities. It can be said that citizens only participate in elections to elect their leaders every election period and go on with their daily life activities post elections. Digital rights education is a vital tool for ensuring citizens are able to demand accountability from leaders and hold them responsible for their actions and inactions. Citizens who are educated get to know their rights, the importance of their privacy, their freedom to express themselves and hold certain opinions and are able to know when these rights are violated.

Conclusion

Conclusively, Nigeria's rising cybercrime rates necessitate a balanced approach between privacy rights and national security. While the Cybercrimes Act 2015 and other legislations aim to combat cybercrimes, concerns about privacy infringement and potential abuse of power remain. Under these legislations, the danger of confusion specific definitions is used has been discovered. However, a statute should be one that will, if not totally, largely curb a crime which it has been enacted to curb. However, to address the conflict between the duo, the approaches Nigeria should prioritize include public awareness, digital rights education and accountability, ensuring citizens' rights are protected while maintaining security. By embracing necessity and proportionality principles, Nigeria can safeguard individual freedoms while protecting its citizens from cyber threats and crimes. Behold, Nigeria must remain a rights-respecting Nigeria.

References

1. A 3rd Year Common and Islamic Law Student Undergraduate. Justice of the Students' Union Court, University of Ilorin.
2. A 100 Level Common Law Undergraduate. Faculty of Law, University of Ilorin.
3. Paradigm Initiative Nigeria: Cybersecurity in Nigeria: Need for a Paradigm Shift 2025.
4. Sibe R. Cybercrime and the Challenge of Static Legislations in Nigeria 2025.
5. Collins v Wilcock. Legal Case Summary 1984.
6. Borges E. Essentials of Cyber Crime Investigation 2025.
7. Section 37, 1999 CFRN 1999 (as amended) provides that The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.
8. Section 21. Cybercrimes (Prohibition, Prevention, etc.). Act 2015
9. Salau AO. Cybersecurity, state surveillance and the right to online privacy in Nigeria: A Call for Synergy of Law and Policy. African J Privacy Data Protection 2024:152-175
10. NDP Act 2023;3(2).
11. Nigerian Communications Act 2003;146(2)
12. Ibid. Resilience: The New Paradigm in Disaster Management-An Australian Perspective. Scientific Res 12.
13. The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.
14. (2021) LPELR-55623(CA)
15. (2018) CLR 4(P) (SC)
16. Adaramola Z. Nigeria's cybercrime law and its 'loopholes 2025.
17. UIA. Misuse of Electronic Surveillance by Government 2025.
18. Bessadi N. How Can We Balance Security and Privacy in the Digital World? 2025.
19. European Union. Necessity & Proportionality 2025.