African Journal on Privacy & Data Protection

To cite: AE Akintayo 'Trends and implications of Nigerian courts' jurisprudence on privacy and data protection: Lessons from comparative foreign jurisprudence' (2024) 1
African Journal on Privacy & Data Protection 99-118
https://doi.org/10.29053/ajpdp.v1i1.0006

Trends and implications of Nigerian courts' jurisprudence on privacy and data protection: Lessons from comparative foreign jurisprudence

*Akinola E Akintayo**
Senior Lecturer and Legal Consultant, Department of Public Law, Faculty of Law, University of Lagos, Lagos – Nigeria

Abstract:

The world is in a data-driven era. From telecommunication to retail, to health care, to banking, to insurance, security services, and so forth, industries and governments are using data to drive business and governmental functions. There is a need, therefore, to effectively regulate data processing in ways that both foster innovation and protect fundamental human rights, especially the right to privacy. The roles and place of courts in the endeavour, however, cannot be overemphasised. Studies show that even in jurisdictions with expansive data protection frameworks, courts are still needed to clarify the law and effectively protect and advance fundamental human rights, including the right to privacy, in the face of ever-expanding technology. Furthermore, the pace of contemporary technology

* LLB (Lagos), LLM (Pretoria), LLD BL (Pretoria); (akinat2002@yahoo.com. An extract of this article was published on a blog: https://thenigerialawyer.com/nigerian-courts-jurisprudence-on-privacy-and-data-protection-and-its-implications-for-freedom-and-autonomy-lessons-from-comparative-foreign-jurisprudence/, earlier in 2023 to enlighten the general public. My gratitude goes to the anonymous reviewers of the *African Journal on Privacy and Data Protection* whose incisive comments and suggestions added notable value to the article.

development is such that questions are already being asked as to whether data protection is not gradually becoming outdated and obsolete. Consequently, a proactive and progressive judiciary is required to ensure that technological development does not leave the law too far behind. Adequate knowledge and awareness of technology-driven development and conceptualisation of the right to privacy is necessary for the courts to effectively perform these critical roles. This brings to the fore the need to articulate the changing paradigm of the right to privacy in the data-driven era and its nexus with effective regulation of data processing (data protection) in the digital age. This article adopts a comparative and doctrinal research methodologies to interrogate and analyse the trends in the Nigerian privacy and data protection case law; it examines their defects, identifies best practices and learning points for Nigerian courts from comparative foreign jurisprudence as well as highlights right to privacy enhancing provisions of the new Nigeria Data Protection Act 2023 for a nuanced and more robust approaches to privacy and data protection adjudication in Nigeria.

Key words: right to privacy; data protection; Nigerian courts' jurisprudence; emerging technologies; Nigeria Data Protection Act 2023

1 Introduction

The world is in a data-driven era. From telecommunication to retail, to health care, to banking, to insurance and security services, and so forth,; industries and governments are using data to drive business and governmental functions.[1] Thus, the need to effectively regulate data processing in ways that both foster innovation and protect human rights, especially the right to privacy, has never become more important. The roles and place of the courts in this endeavour cannot be gainsaid. First, studies reveal that even in jurisdictions with expansive data protection frameworks, courts are still needed to effectively protect and advance individuals' right to privacy in the face of ever-expanding technology. This is more so the case in Nigeria where the Nigeria Data Protection Act 2023, the substantive framework for the regulation of data processing in the country, has just been passed. Second, the pace of contemporary technological development is such that questions are already being asked as to whether data protection is not already becoming outdated and obsolete.[2] This fact makes appropriate and effective privacy regime and enforcement central to citizens' well-being and freedoms in the face of ever-expanding technologies.

However, a proactive and progressive judiciary is a prerequisite to ensuring that technological developments do not leave the law too far behind. Adequate knowledge and awareness of technology-driven development and

1 W Kim and others 'A taxonomy of dirty data' (2003) 7 *Data Mining and Knowledge Discovery* 81-82.

2 D Hallinan and others 'Neurodata and neuroprivacy: Data protection outdated?' (2014) 12 *Surveillance and Society* 55.

conceptualisation of privacy is necessary for the courts to be able to perform these critical roles. There is a need, therefore, to articulate the changing paradigm of the right to privacy in the data-driven era and draw an appropriate nexus between privacy and regulation of data processing (data protection) through the correct conceptualisation of the right to privacy in the digital age.

Two schools of thought are discernible in the judicial conceptualisation of the right to privacy in Nigeria from the academic literature and case law. The first school of thought maintains a clear distinction between privacy and data protection, while the second maintains that data protection is part of and cognisable under the right to privacy.[3] Thus, while a few of the courts' decisions affirm the connection between privacy and data protection, a preponderance number of the cases disavow such connection with the attendant conflicts in the decisions of the courts at the High Court and Court of Appeal levels. This necessitates the articulation of the changing paradigm of the right to privacy in the data-driven era and the charting of the appropriate course for Nigerian courts in the resolution of the conflicting jurisprudence of the courts on privacy and data protection. In doing this, insights will be drawn from comparative foreign jurisprudence in the area of privacy and data protection to identify best practices and learning points for Nigerian courts.

To achieve the above objectives, this article is divided into five parts. Part 1 is this introduction. Part 2 discusses the changing paradigm of the right to privacy in comparative foreign jurisprudence. Part 3 analyses Nigerian case law on privacy and data protection to highlight current trends, identify gaps and discuss the implications of the decisions on fundamental rights and freedoms of citizens. Part 4 identifies pertinent features of comparative foreign jurisprudence and learning points for Nigerian courts. Part 5 concludes the article.

2 Changing paradigm of privacy in comparative foreign jurisprudence

This part discusses the changing perspectives of the right to privacy in light of emerging technologies in comparative foreign jurisprudence below.

Under comparative foreign laws, the changing paradigm of privacy driven by changing technologies is most noticeable in Europe where early developments and changes in the law were first recorded. This started with the article 8 privacy provisions of the European Convention on Human Rights adopted in 1950 (European Convention) and culminated in the watershed European Union (EU) law on personal data protection – the European Union General Data Protection

3 O Babalola 'Privacy versus data protection debate in Nigeria: The two schools of thought' 31 January 2021, https://thenigerialawyer.com/privacy-versus-data-protection-debate-in-nigeria-the-two-schools-of-thought/ (accessed 7 August 2022).

Regulation (GDPR) adopted by the European Union Parliament and European Council in April 2016. Long before GDPR, however, the European Court of Human Rights (European Court) has been using the right to privacy provisions of article 8(1) of the European Convention to engage the rapid evolution and development of information and communications technology (ICT) technologies within the EU. This has given rise to a robust and extensive privacy and data protection jurisprudence of the Court.

The first case analysed by the Court in this regard is *Leander v Sweden*.[4] The Court in this case held that the storing and release of the applicant's personal information in the secret police register without giving him the opportunity to refute the information violated his right to respect of private life under article 8(1) of the European Convention. The Court, however, concluded that the restriction in this particular case was necessary and justifiable in a democratic society.

Data protection has also been held by the Court to be a fundamental part of the privacy provisions of article 8(1) of the European Convention. This is reiterated by the Court in *Z v Finland* as follows: 'In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art 8).'[5] In its elaboration of the scope of personal data, the Court relied on Convention 108 of the Council of Europe that defines personal data as 'any information relating to an identified or identifiable individual ("data subject")'.[6] Thus, information directly identifying a person, such as names and surnames,[7] as well as information indirectly identifying a person, such as the recording of voice samples,[8] internet protocol addresses,[9] banking details,[10] and so forth, has been held to be within the ambit of personal data. Article 8 of the European Convention also covers or protects not only natural persons but also applies to artificial entities where the privacy of their homes or correspondence is deemed to have been violated.[11]

Activities or actions that will implicate data protection or qualify as data processing have been interpreted by the courts to include the 'storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination' in terms of the meaning of data processing in Convention 108'.[12] Thus, the collection and storage of monitoring data collected via global positioning system (GPS) and other surveillance

4 Application 9248/81.
5 Application 22009/93 para 95.
6 Art 2(a) Convention108 of the Council of Europe.
7 *Mentzen v Latvia* Application 71074/01 (December 2004).
8 *PG and JH v The United Kingdom* Application 44787/98 (September 2001).
9 *Benedik v Slovenia* Application 62357/14 (July 2018).
10 *MN & Others v San Marino* Application *28005/12 (*0ctober 2015).
11 *Liberty & Others v The United Kingdom* Application 58243/00 (2008).
12 Art 2(c) Convention108 of the Council of Europe.

measures,[13] the recording and disclosure of closed-circuit television (CCTV) footage of a person in the process of committing suicide,[14] the disclosure of a patient's highly-confidential medical information by a hospital, and so forth, have been held to qualify as the processing of data within the meaning of article 2(c) of Convention 108.

The courts have also recognised the fact that certain categories of data merit heightened protection. These are categories of data referred to as sensitive data in Convention 108. These include 'personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life ... [and] personal data relating to criminal convictions'.[15] Consequently, the Court has held that 'fingerprints, DNA profiles and cellular samples, constitute personal data'[16] and that personal information tending to reveal ethnic or racial origin, gender identification, sexual orientation or sexual life, and so forth, belongs to a special category of data subject to heightened protection under article 6 of Convention 108.[17] Other categories of personal information, such as employment records, financial details, meta data of telephone conversations, GPS location data and voice samples, among others, are also the subject of special concern and consideration.[18]

The courts have also held that the data protection dimension of article 8 of the European Convention imposes two types of obligations on state parties, namely, positive and negative obligations. In *Copland v The United Kingdom*[19] the applicant alleged the unlawful monitoring of her telephone calls, emails and internet usages by her employer, a public higher institution/body for which the respondent state is responsible. The Court held that the case 'relates to the negative obligation on the state not to interfere with the private life and correspondence of the applicant' under article 8 of the European Convention.[20] In *Söderman v Sweden*[21] the Court reiterated that article 8 of the European Convention essentially imposes a negative obligation not to arbitrarily interfere with the private and family life of right bearers but that the article also imposes positive obligations on state parties to take measures to secure respect for private life even in relations between individuals *inter se.*[22]

In India there is plethora of statutes and subsidiary legislation regulating the processing of data in the country before 2017, when the Indian Supreme

13 *Uzun v Germany* Application *35623/05* (September 2010).
14 *Peck v UK* [2003] EHRR 287 Application00044647/98.
15 Art 6 Convention 108 of the Council of Europe.
16 *S and Marper v The United Kingdom* Applications 30562/04 and 30566/04 (December 2008) para 68.
17 *Marper* (n 16) paras 66-67.
18 See, eg, *GSB v Switzerland* Application 28601/11 (December 2015).
19 Application 62617/00 (April 2007).
20 *Copland* (n 19) para 39.
21 Application 5786/08.
22 *Söderman* (n 21) para 78.

Court extended the frontiers of the right to privacy in its very popular decision in *Justice KS Puttaswamy (retd) v Union of India*.[23] In *Puttaswamy* the Supreme Court of India found the existing data protection regime inadequate in effectively protecting the privacy and personal data of Indians. The Court held that although not expressly provided for under the Constitution of India, privacy is implied and can be derived from the right to life and personal liberty in article 21 of the Constitution of India. The Court held that privacy was a natural and fundamental human right inherent in all human beings and constituted the important core of any individual's existence because it is a necessary condition for dignified enjoyment of other fundamental human rights.[24]

Furthermore, the Court noted that privacy has at least three dimensions, namely, the protection of individuals' physical body from intrusion; informational privacy; and privacy of choice. According to the Court, informational privacy is an important aspect of the right to privacy. The Court reasoned as follows:

> The old adage that 'knowledge is power' has stark implications for the position of individual where data is ubiquitous, an all-encompassing presence. Every transaction of an individual user leaves electronic tracks without her knowledge. Individually these information silos may seem inconsequential. In aggregation, information provides a picture of the beings. The challenges which big data poses to privacy emanate from both state and non-state entities.[25]

The Court, therefore, underlined the need to regulate the extent to which personal information can be stored and processed by state and non-state actors alike if the balance of power between individuals and state and non-state actors alike is to be maintained.[26] The Court was of the view that '[t]he concept of "invasion of privacy" is not the early conventional thought process of "poking one's nose in another person's affairs". It is not so simplistic. In today's world, privacy is a limit on the government's power as well as the power of private sector entities.'[27]

The Court held that privacy was not an absolute right but can be restricted by a just, fair and reasonable law that passes the test of proportionality and serve a legitimate governmental aim.[28] On this basis, the Court validated the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Aadhaar Act) and its many regulations. The Act and its regulations compel the registration and collection of biometric and other data of citizens for the purpose of issuing them with unique identification numbers as a basis for delivery of benefits and entitlements under the Aadhaar Act. The Court held that although the Act and subsidiary legislation contained wide-ranging provisions invasive of privacy, they are, however, constitutional as they serve a legitimate governmental

23 Writ Petition 494/ 2012.
24 *Puttaswamy* (n 23) 125-126.
25 *Puttaswamy* (n 23) 150.
26 *Puttaswamy* (n 23) 155.
27 As above.
28 *Puttaswamy* (n 23) 158.

purpose of providing subsidies, benefits and services to needy members of the Indian society. The Personal Data Protection Bill 2019, to implement the far-reaching decision of the Supreme Court of India on privacy and data protection in *Puttaswamy*, was initially pending before the Indian Parliament.[29] The Bill, however, was withdrawn on 3 August 2022 in order to incorporate a long list of recommendations of the Joint Parliamentary Committee of the Indian Parliament.[30] At the time of writing, the Digital Personal Data Protection Bill 2023 was being tabled.

In Kenya, the data protection regime evolved from the constitutional right to privacy protected under the Kenyan Constitution.[31] The constitutional right to privacy, therefore, forms the foundation for the data protection regime in Kenya. As such, even before the enactment of a comprehensive data protection regime, the courts adopted expansive interpretations of the right to privacy to protect the personal information of citizens.[32]

Article 31 of the Kenyan Constitution of 2010 guarantees the right to privacy, which includes the right not to have '(a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed'.

While the need for a more specific data protection regime led to the enactment of the 2019 Data Protection Act, Kenyan courts have before the coming into force of the Act, protected personal information by relying predominantly on the constitutional right to privacy in the Kenyan Constitution. In *Nubian Rights Forum & Others v The Hon Attorney-General & Others*[33] the High Court of Kenya relied chiefly on the constitutional right to privacy and ruled that the collection of GPS and DNA data pursuant to certain legislative amendments was not a justifiable infringement of the right to privacy of Kenyan citizens. The Court also noted that the data protection regime in Kenya, at the time, was not adequate to cater for concerns related to the protection of the personal information of citizens in relation to the collection of biometric data. To reach this decision, the Court sought to balance the benefits from the collection of citizens' data

29 Chambers and Partners 'India's Personal Data Protection Bill, 2019 – An update' 25 January 2022, https://chambers.com/articles/india-s-personal-data-protection-bill-2019-an-update (accessed 9 July 2022).

30 DLA Piper 'India: Government withdraws long-awaited Personal Data Protection Bill' 4 August 2022, https://blogs.dlapiper.com/privacymatters/india-government-withdraws-long-awaited-personal-data-protection-bill/?utm_source=mailpoet&utmmedium=email&utm_campaign=privacy-matters-newsletter (accessed 4 August 2022).

31 For a comprehensive analysis of how the data protection regime evolved before the enactment of the Data Protection Act by the Kenyan legislature, see AB Makulilo & P Boshe 'Data protection in Kenya' in A Makulilo (ed) *African data privacy laws. Law, Governance and Technology Series* (2016) 317-335.

32 B Andere 'Data protection in Kenya: How is this right protected?' https://www.accessnow.org/wp-content/uploads/2021/10/Data-Protection-in-Kenya.pdf (accessed 30 March 2023).

33 Consolidated Petitions 56, 58 & 59 of 2019 (High Court of Kenya, Constitutional and Judicial Review Division).

against the dangers posed by the collection of the data. By acknowledging the inadequacy of the data-protection regime in Kenya, the Court noted that for the data collection and aggregation process to be justifiable, it ought to be done against the backdrop of a comprehensive data-protection regime. It is worth reiterating that the protection of the rights of the applicants was only possible because of the constitutional right to privacy regime. This is despite the fact that the Data Protection Act became law while the case was pending before the Court.

Furthermore, in *Communications Authority of Kenya v Omtatah Okoiti & 8 Others*[34] the respondents were successful in a privacy infringement lawsuit at the High Court of Kenya where the Court ruled that the device management system (DMS), which sought to collect data from subscribers, was an infringement on the privacy right of the subscribers. Again, this judgment was reached by the Court prior to the enactment of the Data Protection Act. Although the High Court decision was upturned on appeal by the Kenyan Court of Appeal on the ground that the infringing acts alleged had not yet occurred or been implemented,[35] the Court nevertheless ordered the agency to continue with consultation with stakeholders. The Court reached this conclusion by relying solely on the constitutional right to privacy. The primary issue considered by the Court of Appeal was whether the DMS installation was a violation of the right to privacy of the citizens/customers. The Court acknowledged that the DMS was designed to address and protect the interests of the telecommunications operators from the pervasive nature of counterfeit products in the industry. The Court also recognised the fact that the appellant had the statutory power to regulate and license operators and operations in the industry. In the opinion of the Court, seeing that there was no concrete evidence that the agency had concrete plans to violate the right to privacy of citizens other than unsubstantiated statements in the media, the right to privacy could not be said to have been violated. The Court, therefore, noted that the desire for access by the agency was valid and necessary in order to tackle the challenges in the industry and that the agency was acting as a regulator pursuant to its statutory powers. The right, therefore, would be said to have been violated only where the access to the data of consumers was unjustifiable and done without any safeguards whatsoever. Consequently, the Court disagreed with the High Court that mere access to users' data was a violation. This case, therefore, is authority for the view that access to consumers' or customers' data is not in itself a violation as long as it is necessary and justifiable and necessary safeguards for the management of the data are put in place. The Court thus emphasised that access to the data of customers and citizens may be necessary to address certain challenges as long as the access was managed within the purview of certain safeguards. The Court criticised the High Court for being

34 Civil Appeal 166 of 2018.

35 The Court also ruled that the suit was premature since consultations were still being carried out and the agency had not yet implemented the infringing act. This was because the respondents instituted the suit at the High Court on the basis of the appellant's proposals that had not yet been implemented.

overly focused on mere access as the basis for privacy rights violation without attempting to balance the interests of privacy and the mandate of the regulator to tackle the challenges in the industry.

Finally, in *Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others*[36] the High Court of Kenya considered a plethora of constitutional and human rights issues in relation to Kenya's hasty enactment of the Security Laws (Amendment) Act 19 of 2014. In relation to the data privacy issues considered in this case, the applicants had argued that (a) the hastiness in enacting the amendments to the statute was unconstitutional and was in violation of the legislative standing orders, thereby making the process lacking in legitimacy; and (b) the introduction of measures to intercept communication for the purpose of combating terrorism in the amendment was unjustifiable and amounted to a violation of the privacy rights of the citizens. The respondents opposed these arguments and argued that the process of making the statute was necessary and not in violation of the Constitution and the legislative standing orders. Additionally, the respondents argued that the restriction on the citizens' right to privacy was necessary and justifiable in a democratic society. They also argued that the restrictions were necessary for democracy since the objective of the enactment was to prevent terrorist activities. Also, the interested parties aligning with the respondents also argued that the right to privacy was not absolute.

In reaching its decision, the Court noted that since there was reasonable public participation in the process of enacting the law, despite the hastiness in the enactment of the law, the process was constitutional and justifiable in the circumstances. Additionally, in relation to the issue of the validity of the restrictions imposed on the privacy of the citizens, the Court held that the violation was justifiable, constitutional, and did not infringe on the right to privacy. The Court's basis for holding that the restriction was justifiable was that the restriction has a reasonable basis, given the objective of preventing terrorism in Kenya.

A number of conclusions are deducible from the analysis of comparative foreign laws and jurisprudence above. The first is that privacy as a fundamental human right features very strongly in the jurisprudence of the different courts. Second is the fact that data protection is regarded not only as part and parcel of privacy alone, but that it has evolved into a stand-alone right. Third is the fact that even in jurisdictions with expansive data protections frameworks, the intervention of the courts is often needed to fill gaps in the laws and keep the law apace with developments in technology. Detailed features and insights deducible

36 Petition 628 of 2014 consolidated with Petition 630 of 2014 and Petition 12 of 2015 (High Court of Kenya at Nairobi Constitutional and Human Rights Division).

from analysis of comparative foreign jurisprudence done in this part are discussed in part 4 below.

3 Trends and implications of Nigerian courts' jurisprudence on privacy and data protection

Nigeria privacy and data protection framework rests on three principal norms: the Nigerian Constitution via section 37; the Nigerian Data Protection Regulation 2019 (NDPR) promulgated by the National Information Technology Development Agency (NITDA) in 2019; and the newly-enacted Nigeria Data Protection Act 2023 (new Act) which was signed into law in June 2023. Section 37 of the Constitution provides that '[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'. NDPR on its part provides for the principles of data processing, the lawful basis for processing data, rights of data subjects in Nigeria, among others. The newly-enacted Act, as the substantive and main data-protection framework in Nigeria, preserves NDPR that has been in use since 2019 to the extent that its provisions do not conflict with the provisions of the new Act. This part of the article examines the trends and implications of Nigerian courts' jurisprudence on privacy and data protection in order to decipher judicial approaches and attitudes as well as identify gaps and implications of the existing jurisprudence. The next part identifies learning points for Nigerian courts from comparative foreign jurisprudence analysed in part 2 above.

Ezugwu Emmanuel Anene v Airtel Nigeria Ltd[37] is one of the earliest Nigerian cases on privacy and data protection. In this case the applicant, a lawyer; sued Airtel, his service provider, at the FCT High Court, Abuja on the ground of countless unsolicited calls and text messages by the respondent and third parties to whom the respondent had disseminated his phone number. He claimed that the interference with his solitude violated his constitutional right to privacy. The respondent did not defend the suit. The Court relied on the applicant's evidence to find the respondent liable. An amount of N5 000 000,00 in damages was awarded by the Court against the respondent.

A similar decision was reached in *Godfrey Nya Eneye v MTN Nigeria Communication Ltd*,[38] where the Nigerian Court of Appeal held that disclosure and dissemination by the appellant of the applicant/respondent's mobile phone number without his consent and the consequent unsolicited messages were a violation of the applicant/respondent's right to privacy.

37 Suit FCT/HC/CV/545/2015 (unreported).
38 Appeal CA/A/689/2013 (unreported).

Also, in *Emerging Market Telecommunication Services v Barr Godfrey Nya Eneye*[39] the claimant, a legal practitioner, had sued the operators of Etisalat mobile line for unauthorised exposure or dissemination of his phone number to persons/companies that sent him unsolicited text messages and advertisements. He claimed that this violated his right to privacy under section 37 of the Nigerian Constitution. The Federal High Court found in his favour at first instance. On appeal by Etisalat, the Court of Appeal upheld the decision of the trial court and held that misuse of personal information of the applicant was a violation of the right to privacy under section 37 of the Nigerian Constitution. Damages in the amount of N1 000 000,00 only were awarded by the Court of Appeal against the respondent.

However, in *Adeyemi Ibironke v MTN Nigeria Communications Limited*[40] the appellant alleged that the respondent had surreptitiously obtained and retained information from her SIM card on the respondent's database, and that the respondent send messages to the appellant's phone every 10 to 20 seconds. The appellant contended this action violated her right to privacy and amounted to nuisance, which unduly interferes with her peaceful use and enjoyment of the MTN line. The Court of Appeal observed the following: '[W]as there any credible evidence to, again on the balance of probabilities, establish any breach of privacy by the messages and notification sent to the appellant's sim card, *even if unsolicited*?'[41] The Court answered the question in the negative and held that there was no credible and satisfactory evidence to substantiate the breach of appellant's privacy by the alleged messages or notifications. The Court appeared more disposed to found that the unsolicited and annoying messages amounted to nuisance but not a breach of privacy. Even then, the Court was of the view that credible evidence had not been adduced to ground the claim of nuisance. According to the Court:

> The messages may be inconvenient and sometimes irritating or even annoying since they were unsolicited for and may, in appropriate cases, constitute a nuisance that may be actionable, but the appellant did not set out the details of the messages and notifications which reasonably interfered with his use and enjoyment of the sim card for which he subscribed and was registered with the respondent.[42]

The Court thus implied that unsolicited messages and incessant messages and notifications sent to appellant's phone that disturbed his peace and solitude did not amount to a violation of his privacy. This posture of the Court clearly misapprehended the nature and scope of the changing paradigm of privacy in contemporary times. Such posture, of course, will not effectively protect privacy in the digital age.

39 (2018) LPELR-46193.
40 (2019) LPELR-47483.
41 *Ibironke* (n 40) 32.
42 *Ibironke* (n 40) 32-33.

Also, in *Incorporated Trustees of Digital Rights Lawyers Initiative v LT Solutions & Multimedia Limited*[43] the respondent had offered 200 million Nigerian and international email lists containing other personal information such as age, local government area, state, city and industry of the owners for sale. The applicant sued the respondent on the grounds that the data was published without the consent of the owners; that the respondent had no right or legal basis for the processing of the data; and that the processing violated the rights of the applicant to privacy under section 37 of the Nigerian Constitution. The applicant also alleged that the respondent had breached the provisions of NDPR by failing to publish its privacy policy, which would contain a description of personal information collected, the purpose for the collection of data, the methods of data collection, and so forth, on its website. The High Court of Ogun State per Ogunfowora J held that the right to privacy extended to the protection of a citizen's personal information. The Court, however, held that there was nothing in the affidavit of the applicant to show that consent of the owners of the emails had not been obtained. The Court also held that although it was established that the respondent did not publish its privacy policy as required by NDPR, the Court did not see how this violated the right of the applicant to privacy. Furthermore, the Court held that absent a grant of power in NDPR for state courts and entities to enforce its provisions, a state court is without jurisdiction to adjudicate violations of NDPR. What is clear from this decision is that, despite the fact that the Court acknowledged that the protection of personal information is within the ambit of privacy, the Court in the end did not adopt a rights-based approach to the resolution of the dispute. Otherwise, the Court would not have declined jurisdiction or proceeded on the basis that findings under NDPR are dispositive of the matter. Under the Nigerian human rights regime both state and federal courts can adjudicate violations of human rights, privacy inclusive. A clear implication of the decision will be to restrict the scope of privacy and ability of claimants to litigate their violations in Nigeria.

In *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission*[44] the claimant/appellant's date of birth was wrongly recorded. He approached the respondent to have the information rectified. He was asked to pay N15 000,00 only as administrative charges. The claimant sued the respondent on the ground that he has a right to have the data rectified without cost to him under the section 37 right to privacy provisions of the Nigerian Constitution and clause 3.1(7)(h) of NDPR. At first instance, the trial High Court of Ogun State, per AA Akinyemi J, interpreted the right to privacy rather restrictively. The trial Court held that the right to privacy relates to the protection of the personal spaces and personal information from intrusion. The Court thus linked the right to privacy under the Constitution to the protection of personal information under NDPR. Notwithstanding the linkage,

43 Suit HCT/262/2020 delivered 9 November 2020.

44 *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission* Suit AB/83/2020 (unreported) judgment delivered 15 July 2020.

however, the trial Court held that right to rectification of data under NDPR was not cognisable under the privacy provisions of section 37 of the Nigerian Constitution. The Court, therefore, concluded that no intrusion of personal information had been shown by the claimant. The case was consequently struck out. The claimant, dissatisfied with the decision of the trial Court, appealed to the Court of Appeal. On appeal, the Court of Appeal found that personal information protection comes within the scope of section 37 of the Constitution. The Court was also of the view that NDPR was made in furtherance of the privacy provisions of the Constitution and, consequently, a part thereof. In the final analysis, however, the Court agreed with the trial Court that the right to have data rectified under NDPR was not cognisable under section 37 privacy provisions of the Constitution. The appeal was therefore dismissed for lacking merit.[45]

The clear implication of this decision is that the data subject's rights provided for in NDPR are not cognisable under section 37 of the Constitution and cannot be enforced via the FREP Rules. In other words, they do not amount to fundamental human rights. As has been rightly observed, the Court of Appeal in the case gives with one hand and takes away with another.[46] The non-recognition of the data subject's right to rectification in the case is likely to adversely affect the litigation of other data subject rights under NDPR going forward.

Also, in *Incorporated Trustees of Laws and Rights Awareness Initiative v The National Identity Management Commission*[47] the applicant sued for an injunction to restrain the respondent from further collection and processing of personal data of Nigerian citizens in furtherance of the establishment of a national identity database and issuance of national identity cards to citizens pending the conduct of a data processing impact assessment and independent experts' report on the safety and security of the respondent's operations. The rationale for the injunction was based on reported data breaches in the application rolled out by the respondent for citizens to download their digital identity cards from the Google store. It was claimed that the porous security features and consequent data breaches of the application violated the applicant's privacy under section 37 of the Constitution and Regulation 1.1(a) of NDPR 2019. The Federal High Court, per Ibrahim Watila J, held that that the breach of the data subject's rights under NDPR was not necessarily a breach of the section 37 right to privacy provisions of the Nigerian Constitution, on the ground that Reg 4.2(6) provides that a breach of any provisions of NDPR is to be construed as a breach of the provisions of the NITDA Act of 2007. Thus, the latter provisions take the proceedings outside the ambit of section 37 of the Nigerian Constitution and the FREP Rules. The implication of this decision, of course, is to shut out from the ambit of constitutional and human rights adjudication all issues relating to data

45 (2021) LPELR-55623 (CA).
46 S Okedara and others (eds) *Digital rights in Nigeria: Through the cases* (2022) 50.
47 Suit FHC/AB/CS/79/2020 (unreported).

protection in Nigeria and turn these into mere legal rights under the NITDA Act. This will run contrary to the conception of personal information as part and parcel of privacy under section 37 of the Constitution, as was held in cases such as *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission* by the Court of Appeal above.

In *Digital Rights Lawyers Initiative and Unity Bank*[48] personal data of 53 000 job seekers were exposed on respondent's website. The applicant, on behalf of the job seekers, brought a suit against the respondent and sought a declaration that the respondent's unauthorised exposure of personal data of the job seekers on the internet constituted a personal data breach under Regulation 1.3(xx11) of NDPR; also, that the unauthorised exposure of the personal data on the internet violated the right to privacy of the job seekers as guaranteed under section 37 of the Nigerian Constitution, among others. The Federal High Court, per Ibrahim Watila J, held that the exposure of personal data of persons was not within the privacy provisions of section 37 of the Constitution but only cognisable under the provisions of NDPR. The Court held further that even assuming that section 37 of the Constitution applies, a breach of personal data will qualify as an ancillary claim only and, thus, cannot be enforced via the more expeditious procedure of the FREP Rules, which requires that claims brought under it to be principal human rights claims. The Court also held the action incompetent because the condition precedent to the initiation of the action under NDPR, namely, referral to the Administrative Redress Panel (ARP), had not been complied with, among other grounds relied upon by the Court.

To start with the last ground for the decision of the Court: The opening paragraph of Regulation 4.2 (1) relied upon by the Court as mandating referrals to the ARP in cases of breaches of data subjects' rights in NDPR started with '[w]ithout prejudice to the right of a data subject to seek redress in a court of competent jurisdiction.' A literal reading of this provision clearly preserved the right of data subjects to approach the court with or without referral to the ARP. As has been correctly argued, Regulation 4.2 only empowers the NITDA to set up the ARP.[49] The provision is not intended to fetter the rights of data subjects to approach the courts. The argument that the illegal and unauthorised exposure of personal data does not come within the ambit of privacy or that assuming it does, that it is an ancillary claim also totally misconceived the ambit of the right to privacy and its nexus with data protection. The decision is clearly symptomatic of the traditional and narrow understanding of the right to privacy that has become outdated and obsolete in the current digital age and the onslaught of emerging technologies impacting on the right. The implication of the decision will be to stall the due development of the law and jurisprudence on privacy and data protection in Nigeria.

48 Suit FHC/AB/CS/85/2020 (unreported).
49 Okedara and others (n 46) 85.

Finally, in *Daniel John Daniel v True Software Scandinavia AB (Truecaller)*[50] the applicant sued the respondent for the publication of his phone number to users of the respondent's software without his consent. He contended that the unauthorised publication and disclosure of his telephone number violated section 37 of the Nigerian Constitution, among others. The High Court of Lagos State, per Bola Okikiolu-Ighile J, held that the publication was not a violation of his right to privacy under section 37 of the Constitution. According to the Court:

> A careful review of this shows that the applicant is not a registered member of the respondent's organisation. However, the publishing of the applicant's phone number on the platform of the respondent's software has not shown to me that his right to privacy has been breached. It goes without saying that these facts relied on by the applicant do not disclose any breach of fundamental human right of the applicant.[51]

The Court also held that processes were not properly served outside jurisdiction and that the Court has no jurisdiction. The case was thus struck out. The Court's pronouncement quoted above clearly showed the Court's narrow understanding of privacy in the digital age.

An analysis of the jurisprudence of Nigerian courts above shows that while a few of the cases apprehended the nexus between privacy and data protection and interpreted privacy liberally to cover data protection, a preponderance of the cases conceived the right to privacy in the more traditional sense and disavowed any connection between the two concepts. As rightly observed by Babalola, the case law is 'replete with straightjacketed privacy cases which relate to invasion of homes and offices as opposed to invasion of data privacy *stricto sensu*'.[52] Even in cases that affirmed the connection between privacy and data protection, there was an apparent lack of sufficient and adequate knowledge and appreciation of the technology-driven paradigm of privacy in the current digital age. Another conclusion reached through the analysis of the case law is that the law on the nexus between privacy and data protection remains unsettled with the consequent conflicting decisions of the courts both at the High Court and the Court of Appeal levels. The resolution of this conflict awaits the Supreme Court of Nigeria's intervention.

Granted, most of the cases analysed above were decided under NDPR before the advent of new Nigeria Data Protection Act 2023. The advent of the new Act, however, may not make much difference despite some of its privacy-enhancing provisions, if the courts refuse to interpret the new Act progressively and proactively. First and foremost, no data protection framework, no matter how expansive, will be able to keep pace with current technological developments

50 Suit LH/5868MFHR/2017 (unreported).
51 *Daniel* (n 50) 8.
52 O Babalola 'Nigeria: Data protection and privacy challenges in Nigeria (Legal Issues)' 9 March 2020, https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues- (accessed 11 May 2022).

in the absence of the expansive application of the right to privacy to serve as effective guardrails against inevitable depredations of fundamental human rights, autonomy and freedoms of persons by emerging technologies. Therefore, there is a need for the courts to adopt a proactive and expansive interpretation of fundamental rights and privacy upon which the new Act is hinged. Second, the Act is not likely to be able to cure the narrow and traditional reading of the right to privacy, which is out of tune with contemporary realities of the digital age, in the absence of changed attitudes and perspectives by the courts. Third, the new Act cannot also prevent the decoupling of privacy from data protection in the way it has been done by the courts except if the courts are ready to adopt a more expansive and robust reading of the right to privacy consistent with the tenor and intendment of the new Act and in accordance with comparative foreign jurisprudence and best practices in similarly-situated jurisdictions across the world. The above reasons and many more underscore the importance and necessity of the study even with the coming on board of the new Act.

Thus, drawing insights from comparative foreign jurisprudence discussed in part 2 above, the part below identifies pertinent features of international best practices for Nigerian courts to draw from and resolve their conflicting decisions on privacy and data protection in a bid to usher in a more robust privacy and data protection jurisprudence for more effective protection of the autonomy, well-being and freedom of Nigerians from the harmful effects and depredations of emerging technologies.

4 Insights from foreign law and jurisprudence

The first insight deducible from the analysis in part 2 above is that privacy has two strands: individual interest in avoiding disclosure of personal matters and the independence of individuals in making certain important life decisions. The protection of personal information dimension constitutes the privacy second strand and has birthed the right to informational privacy, that is, data protection, in the United States of America and the right to informational self-determination in Germany. Within the EU, the European Court of Human Rights has also clearly held in cases such as *Z v Finland, PG and JH v The United Kingdom* and *Benedik v Slovenia* that the protection of personal information is fundamental to the enjoyment of the right to privacy guaranteed under article 8 of the European Convention.

The second deducible insight is that data protection flowing from the right to privacy has evolved into a stand-alone right in comparative foreign law and jurisprudence and, thus, is conceptualised as a fundamental human right under both conventional and decisional laws in jurisdictions regarded as best practices. This clearly is the case under the Charter of Fundamental Rights of the EU which guaranteed a stand-alone right to data protection. Decisional laws in India via the Supreme Court of India decision in *Justice KS Puttaswamy (retd) v Union*

of India[53] have also gone a step further to assign the status of a natural right to privacy/data protection upon which the due exercise and enjoyment of other fundamental rights rests.

Third, as discussed in part 2 above, comparative foreign jurisprudence has clearly defined activities or actions that will amount to processing of data flowing from the right to privacy prism. The European Court of Human Rights in *Uzun v Germany* and *Peck v UK* recognised that operations performed on personal information that will qualify as data processing include collection, storage, carrying out of logical and/or arithmetical operations on data, alteration, erasure, retrieval, publication or disclosure, and so forth. Several activities enumerated in the cases as data processing suggest that, with a few exceptions, any handling of personal information whatever will qualify as data processing.

Four, in accordance with international best practices as codified in conventional data protection norms, the European courts of human rights have recognised the special and sensitive status of some categories of personal information referred to as sensitive personal information. These are personal information that tends to reveal racial origin, political opinions and religious or other beliefs and personal information relating to sexual orientation, health status, criminal convictions, and so forth. The Court has thus held in *S and Marper v The United Kingdom,*[54] among others, that this category of personal information is entitled to heightened protection and special concerns and consideration because of their tendency to expose data subjects to harmful differentiation and consequences.

Five, flowing from the right to privacy paradigm, the retention of data beyond the time and objectives for which the data is required is a negation of the control that data subjects should have over their personal information.

Lastly, comparative foreign jurisprudence has also recognised that data protection imposes two levels of obligations on states. In *Copland v The United Kingdom and Söderman v Sweden*[55] the European Court of Human Rights held that privacy and the concomitant right to data protection impose not only a negative obligation on states not to arbitrarily interfere with private and family life, correspondence and personal information of individuals, but also a positive obligation to take measures to secure respect and provide necessary facilities and enabling environment for the protection and full enjoyment of the rights from depredations and violations by third parties. The foregoing are some of the key features and learning points from comparative foreign jurisprudence and laws.

53 As above.
54 As above.
55 As above.

If the courts in cases such as *Adeyemi Ibironke v MTN Nigeria Communications Limited*[56] had recognised the nexus between privacy and data protection and the fundamental nature of privacy-dependent data protection norms in the data-driven era, the Court is not likely to have held that the disclosure of the appellant's phone number to third parties by the respondent and incessant unsolicited messages to the appellant's phone number is not a breach of privacy.

Also, had the courts in *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission* and *Incorporated Trustees of Laws and Rights Awareness Initiative v The National Identity Management Commission* conceptualised data protection as a fundamental right flowing directly from privacy, the courts in those cases would not have held that a breach of data subject rights is not necessarily violation of the right to privacy or that an action for the breach of the right cannot be brought under the FREP Rules.

In addition, if the courts had properly distilled what amounts to data processing in the light of best practices, the Court in *Digital Rights Lawyers Initiative v Unity Bank* would not have held that the disclosure of personal information of 53 000 job seekers on the website of the respondent is not within the ambit of the privacy provisions of section 37 of the Constitution or that the action brought upon it is not cognisable under the FREP Rules. Finally, if the courts had understood the proper scope and ambit of privacy in the digital age in line with international best practices, the Court in *Daniel John Daniel v True Software Scandinavia AB (Truecaller)* would not have held that the publication and disclosure of the applicant's details by the respondent to users of the respondent's software was not a violation of applicant's constitutional right to privacy.

An analysis under this part reveals that Nigerian courts have a lot borrow from comparative foreign jurisprudence for a more robust and effective privacy and data protection regime in Nigeria.

Fortunately, the new Act contains provisions that strengthen the constitutional, privacy and fundamental rights approach to data protection in Nigeria. First, unlike NDPR that approached data protection from a statutory rights point of view, the new Act directly connects the protection of personal information of data subjects to the protection of fundamental rights guaranteed under the Constitution of Nigeria.[57] Second, the new Act, while exempting the processing of personal data done solely for personal or domestic purposes, subjects the exemption to the fundamental rights to privacy of data subjects.[58] Third, the new Act also confers a right on a data subject to object to the processing of personal data.[59] Where a data subject objects to the processing of his or her personal data,

56 As above.
57 Sec 1(1)(a) Nigeria Data Protection Act 2023.
58 Sec 3(1) Nigeria Data Protection Act 2023.
59 Sec 36(1) Nigeria Data Protection Act 2023.

a data controller is obliged to cease further processing of the data unless the data controller can demonstrate public interests or legitimate grounds that override the fundamental rights, freedoms and interests of the data subject.[60] Four, there is a right of data subjects to object to processing of their personal data for direct marketing purposes.[61] Where a data subject objects to such processing, the data shall no longer be processed by the data controller.[62] Five, data subjects also have a right to object to the processing of personal data that is based mainly on the automatic processing of personal data.[63] The objection will not apply where the processing is required for the performance of a contract between a data subject and a data controller or where the processing is authorised by a written law that provides for necessary measures to protect the fundamental rights, freedoms and interests of data subjects.[64] Finally, in all circumstances of automatic processing of personal data, the data controller is mandated to implement measures to protect the fundamental rights, freedoms and interests of data subjects.[65]

The foregoing provisions clearly demonstrate that the new Act approached data protection from a constitutional, privacy and fundamental human rights perspective. This is an approach upon which counsel and litigants can leverage to persuade courts to depart from decisions that appear not to lean in favour of fundamental rights and privacy. In addition, rooting data protection in privacy and fundamental rights and freedoms in the Constitution, as was done in the Act, suggests that the various data subject rights under the new Act will be amenable to enforcement through the FREP Rules.

5 Conclusion

This article interrogates the trends, approaches and implications of Nigerian courts' jurisprudence on privacy and data protection. The need for and importance of the interrogation are set out in the introduction. Part 2 examines the changing conceptualisation and paradigms of privacy underpinned by changing technology and data-driven approaches in comparative foreign jurisprudence. It was found that the notion of privacy now is much more than a mere right to be let alone and is now a more complex and eclectic concept to engage with the drastically-changing society and technology. Part 3 analyses Nigerian case law on privacy and data protection. It was found that while a few cases interpreted privacy liberally and affirmed the connection between privacy and data protection, a preponderance of the cases follow the straight-jacketed and traditional conception of privacy and disavowed any connection between privacy and data protection. Even cases that appear to be more progressive show an apparent lack

60 Sec 36(2) Nigeria Data Protection Act 2023.
61 Sec 36(3) Nigeria Data Protection Act 2023.
62 Sec 36(4) Nigeria Data Protection Act 2023.
63 Sec 37(1) Nigeria Data Protection Act 2023.
64 Sec 37(2) Nigeria Data Protection Act 2023.
65 Sec 37(3) Nigeria Data Protection Act 2023.

of understanding and awareness of what privacy entails in the digital age. The foregoing scenario gave rise to conflicting decisions of the courts at both the High Court and Court of Appeal levels. Part 4 identifies pertinent features of comparative foreign jurisprudence that can serve as learning points for Nigerian courts. Provisions of the new Act that strengthen privacy and fundamental rights and upon which counsel and litigants can leverage to persuade courts to lean in favour of fundamental rights and privacy in their interpretation of the new Act were also highlighted and discussed.

The courts have a critical role to play in the development of the privacy and data protection norms of any country in the current data-driven era. No regime, no matter how explicit and expansive, will keep pace with the current level of development in technology. The right to privacy is the last bastion of hope to serve as effective guardrails against inevitable depredations of autonomy and freedoms inherent in the continued expansion and developments of emerging technologies. The mantle, therefore, falls on the courts to interpret privacy liberally and expansively to particular and live cases, thereby developing the privacy jurisprudence on an ongoing basis. The courts will be able to do this only if seized of the appropriate conception of privacy and data protection.

Going forward, the liberal and proactive approaches and best practices from comparative foreign jurisprudence discussed in this article are commended to Nigerian courts. This will equip them with the appropriate conceptualisation to discharge the critical burden they bear in this regard. The privacy and fundamental rights-enhancing provisions of the new Act identified in this article are also commended to the courts in their interpretation and enforcement of the provisions of the new Act. Finally, the courts are encouraged to approach data subject rights under the new Act as fundamental human rights amenable to adjudication and enforcement via the FREP Rules consistent with the intendment and tenor of the new Act.