CHAPTER TWENTY-SIX

THE RIGHTS TO PRIVACY AND DATA PROTECTION IN THE AGE OF INTERNET: A COMPARATIVE ANALYSIS ACROSS THREE CONTINENTS

Abdulkareem Ademola Mashood* Kazeem A. Oyinwola Esq**

Abstract

This paper examines rights to privacy and data protection using the jurisprudence of European Union, United State, India and Nigeria. The right to privacy and data protection entail the 'right to be let alone'; the legal right to control what is shared, when and to whom it is shared. While right to privacy is a fundamental human right across many jurisdictions, data protection is not except within the member states of the European Union. Although there may not be express provision in most national laws recognizing data protection; however data protection is today being considered as a right at the very core of the right to privacy and thus receiving similar attention as right to privacy in many jurisdictions both online and offline. Unlike in the offline interactions where individuals often need to divulge information about themselves in order to interact and build trust with other people, the online space the position is different. On the internet, third parties such as companies or corporations facilitate the online interactions thereby requiring individuals to divulge information about themselves to third parties. This paper employs the traditional legal research methodology of collecting data from primary and secondary source of law in reviewing and analyzing various works in this study. The library materials sourced involve an exposition of available literatures and drawing logical conclusion by offering relevant solutions. It is the finding of this paper that despite the jurisprudential difference that exist across different jurisdictions in terms of their scope and application in the online and offline environments, the protection of right to privacy and data protection are interrelated. This is so in view of the fact that the protection of one leads to the safeguard of the other. It is the recommendation of this paper that the functioning of the online environment requires some minimum level of disclosure of information about individuals, this no doubt makes the application of legislation/regulation on the right to privacy and data protection in the internet age necessity in the countries under analysis. Challenges such as weak or inadequate regulation, surveillance capitalism, data mining, data breaches etc. typical of advancements of the internet age abound.

Keywords: *Privacy, Data Protection, Internet*

1. Introduction

One common features of the Internet Age is the dichotomy between the online and the offline environments. This relatively recent balkanization of the world into online and offline environments has led to a renewed advocacy that the same human rights, especially right to privacy and data protection, that people enjoy offline should also apply online.[1] The United Nations General Assembly(UNGA)session in its resolution 70/1 passed by the Human Rights Council (HRC) at its thirty-second session affirmed that the same rights that people enjoy and invoke offline must also be protected online.[2] This resolution ostensibly put to focus the debate as to whether the privacy protection afforded offline also applies on the internet.

Unlike in the offline environment, application of right to privacy and data protection on the internet is not without their unique features and challenges. Usually, in the offline interactions,[3] individuals often need to divulge information about themselves in order to build trust with other people. However, in the online environment, the position is different'. On the internet, third parties such as companies or corporations facilitate the online interactions. For the individuals, privacy and data protection online entail the 'right to be let alone'; the legal right to control what is shared, when and to whom it is shared. Thus, a proper functioning of the online environment requires at least some minimum level of disclosure of information about individuals. The involvement or participation of third parties in this regard does not come without significant legal issues of concern such as the

* LL.B (Ilorin), BL (NLS, Abuja), LLM (Ife). Lecturer, Faculty of Law, Federal University Dutsin-Ma, Katsina State. Email: aamashood@fudutsinma.edu.ng
**LL.B (Ilorin), BL (NLS, Yola), LLM (Keffi). Managing Partner, Amofin Solicitors, Federal Capital Territory, Abuja

[1] E. Boyle, 'UN Declares Online Freedom to be a Human Right that must be Protected' Independent Newspaper (United Kingdom, Tuesday 5 July 2016) available at <https://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html>, accessed on 14th July, 2021

[2] The UN General Assembly Resolution 70/1 (Human Rights Council Thirty-second Session) 27 June 2016 A/HRC/32/L.20 available at <Https://Www.Article19.Org/Data/Files/Internet_Statement_Adopted.Pdf> accessedon 14th June, 2021

[3] Op. cit.

duty of the third parties as regards the retention of information sensitive or personal to individuals, risk of accidental data loss, malicious attack, data mining in large scale, and surveillance by states and non-state actors using the third parties.

Even though the line of demarcation between right to privacy and data protection appears to be blurred, both serve to afford some level of protection for individuals' data or information in the online environment. In European Union (EU) jurisprudence for instance, right to privacy and right to data protections are two separate but distinct fundamental rights each having different level of articulation with respect to the scope of the right they guarantee. This is not the case in Nigeria. Though right to privacy is a fundamental right in Nigeria, right to data protection would need to be stretched to be upgraded to the level of fundamental right. Thus, the difference between right to privacy and data protection is not only in terms of the level and scope of their protection in the online environment, it is also in relation to jurisprudential differences between them in terms of jurisdiction. This paper therefore did a comparative analysis of right to privacy and right to data using the jurisprudence of European Union, United State, India and Nigeria.

2. Legal Framework for Right to Privacy and Data Protection in the Online Environment

In the offline environment, right to privacy has been held to apply to and in varying relationships and circumstances. Articles 12 and 17 of the Universal Declaration of Human Rights (UDHR) 1948 and International Covenant on Civil and Political Right (ICCPR)? guaranteeright to privacy and provide that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[4]Both the ICCPR and UDHR single out 'privacy', 'family', 'home or correspondence,' 'honour and reputation' in the text of their provisions. The provision of Article 16 of the Convention on the Right of the Child (CRC)? also guarantees right to privacy of the child in terms similar to those of the ICCPR and UDHR except that the word 'home' is omitted in the text of the article.

[4] Art. 17 ICCPR and art. 12 of UDHR

Furthermore, Article 11(1) and(2) of the American Convention on Human Rights (ACHR)?is similar in terms to those of the ICCPR, UDHR and the CRC except that in addition to the components mentioned in the texts of those provisions,[5] it includes 'dignity'. While article 8 of European Convention on Human Rights (ECHR) provides for right of everyone to respect for 'private and family life', home and correspondence, it does not include 'honour', 'reputation' or 'dignity' found in ICCPR, UDHR and CRC.

In Nigeria, Section 37 1999 Constitution of the Federal Republic of Nigeria (CFRN) is similar with the provisions of UDHR, ICCPR, CRC and ECHR in its mention of 'home and correspondence'. The section also mentions 'telephone conversations' and 'telegraphic communications' in addition to 'correspondence' and 'homes' in its provision.[6] The area of convergence among the several provisions of law guaranteeing right to privacy are 'home', 'family' and 'correspondence'. There has been suggestion that the right to data protection is intended and imbedded in the right to privacy specifically provided in the above textual provisions. Even though this may seem acceptable especially when one considers the use of words such as 'correspondence', 'telegraphic information' especially in Section 37 CFRN, however the jurisprudence of the EU on right to privacy and data protection belie this suggestion.[7]

Nevertheless, the United Nation General Assembly (UNGA), the UN Human Rights Commission (UNHRC) and regional organizations such Council of Europe (CoE) and the EU have all affirmed in their respective resolutions that human rights protection offline can as well be extended to the online environment.[8] Relying on this, the Association for Progressives Communication

---

[5] See art. 12 Ibid, art. 17 Ibid and art. 16 CRC?.

[6] Section 37CFRN was mentioned because other jurisdictions being examined alongside Nigeria have specific provision for privacy in their Constitutions. For instance, India and US have no specific provisions guaranteeing right to privacy hence, reference to s.37 CFRN.

[7] ICCPR, UDHR and CRC include 'honour' and 'reputation' in the text of their provisions. While ACHR includes 'dignity', art. 8 of the ECHR did not include 'honour', 'Reputation' or 'dignity' but qualifies its scope with 'private and family life.' Section 37 of the CFRN neither mentions 'honour', 'reputation' or 'dignity' but use 'telephone conversation' and 'telegraphic communication'.

[8] D. Brown, 'UN General Assembly Adopts Resolutions to Protect Human Rights Online for Journalists and Human Rights Defenders' Association for Progressive Communication (United Kingdom, 21 June 2021)available at<https://www.apc.org/en/news/un-general-assembly-adopts-resolutions-protect-human-rights-online-journalists-and-human-rights>accessed on 30th October 2019. See also UN Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/38/L.10/Rev.1)available at<Https://Ap.Ohchr.Org/Documents/Dpage_E.Aspx?Si=A/Hrc/38/L.10/Rev.1> accessed on 3rd August 2021

(APC) has firmly established in the Internet Rights Charter[9] to the effect that the internet related human rights such as right to privacy and data protection are embedded in the UN Human Rights System based on the UDHR and other related instruments.[10] It further suggest that the question of dichotomy between online and offline human right especially as regards right to privacy is settled, at least in principle, even though the implementation of the offline regulations in the online space raises further challenges.

More so, the data protection legislations and regulations of the many countries establish the right of individual to the protection of their data. The common feature of this regulation and legislation is that their application transcends offline environment. The provisions apply both online and offline. One of the main international instruments on privacy and data protection is the 1981 Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention).[11]The CoE Convention is regarded as the first binding international instrument protecting individuals against abuses associated with the collection and the processing of personal data. It among others, regulates the trans-frontier flow of personal data and guiding **principles for** 'personal data undergoing automatic processing'. To this effect, personal data is required to be obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.'

Another significant, though non-binding, document on privacy and data protection at the international scene is the Organization for Economic Co-operation and Development (OECD) Guidelines on Protection of Privacy and Trans-border flows of Personal Data from 1980 but updated up to 2013.[12]This

---

[9] See Association for Progressive Communication (APC) Internet Rights Charter (Published by the APC, November2006)available at<https://www.apc.org/sites/default/files/APC_charter_EN_0_1_2.pdf>accessed on 3rd July, 2021

[10] Other instruments like ICCPR CRC, ACHR, ECHR etc.

[11] (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108 Strasbourg, 28/01/1981 - Treaty open for signature by the member States and for accession by non-member States 01/10/1985 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> Accessed on 22nd July, 2021

[12] Organization for Economic Co-operation and Development (OECD) Guidelines on Protection of Privacy and Trans-border flows of Personal Dataavailableat<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>accessed on 22ndJune, 2021

guidelines inspired many international, regional as well as national regulations on privacy and data protection. Virtually, all the OECD countries have enacted their privacy laws and give the authorities the power to enforce them.[13] Although the OECD's principles have been widely adopted, differences exist as regards its implementation particularly in Europe and the United State of America (USA). In Europe, there is a comprehensive legislation on data protection. While in the US, privacy regulations are sectors-based and the same thing obtains in Nigeria and India.

Besides the above-mentioned instruments, the EU enacted the 1995 EU Data Directive presumably to ensure stronger data protection.[14] The EU Data Directive formed an important legislative framework for processing of data in the EU with huge impacts on the development of national legislation not only in Europe but also globally.[15] It regulates the processing including the collection, use, storage, disclosure, and destruction Individuals' personal data.[16] Since the Directive was passed, at least each of the twenty-eight EU member states[17] has separately implemented the directive into its own national law. For example, the United Kingdom enacted its Data Protection Act of 1998 which virtually incorporated the provisions of the Directive as part of the UK domestic laws.[18] This Directive continued to apply until advancement in Information technology (IT) heralded new developments which necessitated stronger needs to ensure efficient privacy protection in the current technological environment. This subsequently led to the EU passing the new General Data Protection Regulation (EU GDPR) adopted in

[13] As at 22nd September 2019 the OECD member countries comprises 36 member countries spanning across the globe, from North and South America to Europe and Asia-Pacific. See OECD Member Countries<http://www.oecd.org/about/members-and-partners/> accessed on 22nd June, 2021

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.Adopted by the European Commission in 1995, the Directive sets out the frameworkfor data protection regulation in the EU<https://edps.europa.eu/sites/edp/files/publication/dir_1995_46_en.pdf>accessed on 23rd July, 2021

[15] The NDPR adopted some of the principles of the Directives. See Part VI, Regulations 34-38 of the NCC's Consumer Code of Practice Regulations 2007 Federal Republic of Nigeria Official Gazette No. 87 Lagos - 10th July, 2007 vol. 94Government Notice No. 56.

[16] See articles 6, 7, and 8-21 of the Directive 95/46/EC.

[17] Norway and Liechtenstein (which are European Economic Area countries) but not EU member states. See EU member countries in brief <https://europa.eu/european-union/about-eu/countries/member-countries_en>Accessed on 23rd July 2021

[18] Thompson Reuters Glossary, EU Data Protective Directives available at<https://uk.practicallaw.thomsonreuters.com/6-501-7455?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1> accessed on 23rd July 2021

2016 to replace the 1995 Directive.[19] The new EU GDPR enshrines the right to erasure/de-indexing (right to be forgotten) of personal data.[20]

Nigeria has a comprehensive data protection regulation and also awaiting the passage of data protection bill to law at the National Assembly, apart from some other industrial specific codes regulations guaranteeing right to privacy and data protection in relation to the industry. India is yet to have a comprehensive legislation/regulation on data protection as its draft Data Protection Bill 2019 is yet to come into force. While the EU countries are guided by the GDPR, the United States has no comprehensive data protection legislation/regulation comparable to that of the EU. Thus, while right to data protection is somewhat fused in some countries, it is separated in the EU.

Nonetheless, right to privacy and data online requires specific approaches and while the Internet brings challenges related to enforcement, the existing rules on privacy appear appropriate. It suffice to say or point that at the international level right to privacy and right to data protection are cognizable right in the online environment.

3. Scope and Application of Right to Privacy and Data Protection

As universal as right to privacy portends, there is an agreement of no common consensus across jurisdictions as regards the scope of its protection. The existing laws guaranteeing right to privacy at the international, regional and national levels have certain areas of convergence as well as areas of divergence as regards their application. More so, judicial interpretation and exposition of the right vary from jurisdiction to jurisdiction just as there are areas of convergence and divergence with respect to its application.

There are also variations as regards the scopes of right to privacy especially as regard their judicial interpretations which largely depend on the jurisdiction. In Europe for instance, the court has defined the scope of privacy guaranteed under article 8 of the ECHR broadly even when a specific right is not set out in the

[19] The new EU GDPR became applicable in May 2018.

[20] F. Detmering and A. Splittgerber, 'One Year of GDPR–How have EU Member States Implemented and Enforced the New Data Protection Regime?'Reedsmith Technology Law Dispatch (US, 30th May 2019) available at<https://www.technologylawdispatch.com/2019/05/privacy-data-protection/one-year-of-gdpr-how-have-eu-member-states-implemented-and-enforced-the-new-data-protection-regime/> accessed on 23rd July 2021

article.[21] For instance, the applicability of article 8 has been determined, in some contexts, by a severity test to cover attacks on a person's reputation in *Denisov v Ukraine*[22] and *Nicolae Virgiliu Tănase v Romania.*[23] It was also used to cover acts or measures of a private individual which adversely affect the physical and psychological integrity of another. Furthermore, the cases of *Pretty v The United Kingdom*[24] and *Peck v The United Kingdom*[25] have established in Europe that the scope of right to privacy especially as it concerns 'private life' may 'embrace multiple aspects of the person's physical and social identity.[26] 'Through case-law, the ECHR and the European Commission (EC) have widened the scope of privacy providing guidance as to the meaning and scope of private life for the purposes of article 8 of the ECHR.[27] In *X and Y v The Netherlands*[28], the ECHR (the court) indicated that the concept of private life covered the physical and moral integrity of the person. This decision to the effect that private life 'embraces multiple aspects of the person's physical and social identity' has been used in Europe to assert reproductive rights,[29] make choices as regards end of life issues[30] and issues concerning burial etc.[31] The courts in Europe have similarly extended the scope of privacy to cover to aspects relating to personal identity, such as a person's name, photograph, or physical and moral integrity,[32] honour and reputation.[33]

[21] For instance, art. 8 ECHR does not include 'honour', 'reputation' found in UDHR, ICCPR, CRC and 'dignity' found in ACHR or 'telephone conversation' and 'telegraphic communications' found in s37 CFRN. Even though art. 8 ECHR does not specifically include 'reputation', the ECtHR has held that reputation is protected under article 8 ECHR as part of private life in the cases of Axel Springer AG v Germany [GC] (Application No. 39954/08) 83; and Chauvy and Others v France, No. 64915/01, ECHR 2004-VI September 2010) available at<https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-109034%22]}> accessed on 15th July, 2021

[22] Denisov v Ukraine [GC], No. 76639/11, 25 September 2018, p. 111-112 and 115-117

[23] Nicolae Virgiliu Tănase v Romania [GC], No. 41720/13, 25 June 2019 p. 128

[24] No. 2346/02, ECHR 2002-III

[25] No. 44647/98, ECHR 2003-

[26] See S. and Marper v The United Kingdom [GC], Nos. 30562/04 and 30566/04, ECHR 2008.

[27] See Paradiso&Anorv v Italy [GC], No. 25358/12, 24 January 2017, 159

[28] ECtHR, 26 March 1985, Series A No. 91

[29] See A, B and C v Ireland [GC] No. 25579/05, ECHR 2010 [GC] 214 and 245

[30] In Pretty v The United Kingdom No. 2346/02, ECHR 2002-III, it was held that right to decide the manner of one's death is an element of private life under article 8 ECHR.

[31] See Solska and Rybicka v. Poland Nos. 30491/17 and 31083/17, 20 September 2018,

[32] See Von Hannover v Germany (No. 2) [GC], Nos. 40660/08 and 60641/08, ECHR 2012

[33] Rotaru v Romania [GC] No. 28341/95, ECHR 2000.

In the US, despite the absence of express provision in the US constitution guaranteeing right to privacy,[34] the judicial expositions of right to privacy as a fundamental right have been used to assert family and reproductive rights,[35] invalidate search and seizure by the use of GPS technology,[36] nullify the search of the cell phone of an individual's arrested without warrant,[37] and it has been used by same-sex couples to assert their right to same sex marriage.[38]

The peculiar nature of India, in view of the absence of express provision guaranteeing right to privacy in its constitution, might be one of the reasons the scope of privacy in India is not yet as widened as it is already in Europe and in the US. It was not until 2017 in the landmark case of *Justice K.S. Puttaswamy (Retd.) &Anor. v Union of India &Ors,*[39] that the Supreme Court of India settled it that right to privacy is a fundamental right in India. Before then, judicial authorities were inconsistent on whether it is a fundamental right or not. Nevertheless, few cases available on it have established that the scope of right to privacy extend to cover doctor-patient relationship,[40] sexual identities,[41] unlawful search and seizure,[42] telephone tapping,[43] and same has been used to invalidate the government's action mandating uniform biometrics-based identity card on Indians (India government's Aadhaar scheme).[44]

---

[35] In the United States, right to privacy is carved out of many rights, including the Fourth,Fourteenth and the Ninth Amendments. See N. Kaur, 'Right to Privacy in the United States of America', The Leaflet (New Delhi, May 28, 2018) available at<https://theleaflet.in/specialissues/right-to-privacy-in-the-united-states-of-america-by-nehmat-kaur/> accessed on 16th August, 2021

[36] In Griswold v Connecticut (1965)381 U.S. 479

[37] In 2012 in United States v Jone(2012) 565 US 400, the validity of a search and seizure by the use of technology was challenged. The Supreme Court held that the use of GPS technology on a car would be an invalid search violative of privacy.

[38] In 2014, in Riley v California (2014)573 US 373, the search of an individual's cell phone during a warrantless arrest was held to be unconstitutional search and seizure of the digital content.

[39] In a landmark judgment of 2015 in Obergefell v Hodges (2015) 576 U.S.
WRIT PETITION (CIVIL) NO. 494 OF 2012

[40] See Mr. 'X' v Hospital Z (1998) SC/0733where it was held that doctor- patient relationship though basically commercial, is professionally a matter of confidence and therefore, doctors are morally and ethically bound to maintain confidentiality.

[41] See Naz Foundation v Union of India(1981) 2 SCR 516 wherein the Delhi High Court relied on article 21 of the Indian Constitution to strike down section 377 of the Indian Penal Code, 1860 and decriminalized a class of sexual relations between consenting adults.

[42] Maneka Gandhi v Union of India (1978) AIR 597.

[43] R.M. Malkani v State of Maharashtra (1973) 1 SCC 471

[44] Aadhaar scheme is a uniform biometric-based identity number introduced by the India government which comprises a 12-digit unique identity number that can be obtained voluntarily by residents of India, based on their biometric and demographic data<.https://timesofindia.indiatimes.com/india/Aadhaar-now-must-for-government-schemes-benefits/articleshow/54337574.cms> Accessed on 15th July, 2021

In Nigeria right to privacy is a fundamental right that has received less attention which scope has not been judicially widened like it obtains in the Europe and the US. Only few cases exist on the right to privacy itself much less its scope of protection. Nevertheless, the decision of the Nigerian Supreme Court in the case of *MDPDT v Okonkwo*[45] extended the scope of right to privacy to cover doctor-patient relationship, freedom of thought, conscience and religious belief.[46]
Arising from the above and as earlier noted, it is glaring that there are areas of convergence in terms of scope of right to privacy. Nonetheless, there are also certain areas of divergence regarding the interpretation of the scope of privacy across jurisdictions. One notable area of divergence is the one that exists between Nigeria and EU and US. While the scope of right to privacy has been held to apply to cover same-sex marriage relationship in Europe and US, its scope does not protect same-sex relationship in Nigeria.[47]

4. Relationship between Right to Privacy and Data Protection

To begin with, the conception of right to privacy derives from three related aspects namely: decisional privacy, informational privacy and physical privacy. It has been argued from some quarters that data protection relates to 'informational privacy,' one of the tentacles of right to privacy. Data protection, though considered by some to be narrower in scope than right to privacy, it has a privacy dimension. In the digital environment, data protection specifically relates to privacy/protection of personal or informational data which is narrower in scope than right to privacy which encloses not just personal data but also privacy of family life, home and correspondence, telephone conversation and telegraphic information, honour, reputation and dignity.[48] The common understanding from this is that as far as the online environment is concerned, in terms of digitization,

[45] (2001) 6 NWLR (Pt.710)
[46] The matter was decided during the application of 1979 Constitution wherein (i) right to privacy is contained in section 34; and (ii) right to freedom of thought, conscience and religion is contained in section 35.
[47] See section 1 and 2 of the Same Sex Marriage (Prohibition) Act, 2014 which prohibits and criminalizes same sex marriage/union in Nigeria with a punishment of a term of 14 years imprisonmentor 10 years imprisonment upon conviction.
[48] This largely depends on jurisdiction. For instance telegraphic communication is protected under section 37 of the CFRN 1999; honour and reputation are protected under article 12 and 17 of the UDHR and ICCPR. See supra foot notes. 163 and 163

data protection is intrinsic in the right to privacy itself making it an aspect of right to privacy. This therefore makes the issues of data protection a relevant one when discussing right to privacy in the Internet Age.

Although, the EU recognizes right to data protection as a separate distinct right, it has not diminished the fact that right to privacy constitutes the very nucleus of right to data protection. Data protection and right to privacy are both separate but distinct fundamental rights[49] protected by different systems of law in Europe.[50] Using the European model which somewhat represents the model of what data protection encapsulates, data protection sets forth the basic principles for data subjects' protection.[51] Personal data are protected to not only enhance the privacy of the subject, but to also guarantee other fundamental rights in relation to specific areas.[52] The specific rights guaranteed in this regards include the 'right to freedom of speech/expression - this encircles the right to know what data is gathered about a data subject as well as the right of the data subject to have access to such data; and the right to ask for modification, erasure or deletion of the data including the right to de-indexing.[53] In effect, the data subject has a right to know not only what personal data is collected, or on what legal grounds, but also how it is used, for how long it is used and kept; and who collects the data.[54] Therefore, it can be submitted that right to data protection specifically gives the data subjects such rights as right to *access,* modify, update or ask for deletion, or erasure of the data whereas right to privacy does not encapsulates these specific guarantees.[55] This goes to show that even though right to privacy and data protection may appear somewhat relate, the scope of their guarantee and protection are different.

---

[49] Art.8 Charter of Fundamental Rights of the European Unionprovides thus: 'Everyone has the right to the protection of personal data concerning him or her.'

[50] Right to Privacy as a fundamental right in Europe is guaranteed under article 8 of ECHR while fundamental right to Data Protection is separately guaranteed under art. 8 of the Charter of the Fundamental Rights of the European Union ("the Charter'). There are also two separate but distinct systems for protecting these two rights in Europe. While the European Court of Human Rights (ECtHR, the Strasbourg Court) administers the ECHR ("The Convention") the Court of Justice of the European Union (CJEU, the Luxembourg Court) administers the CFREU ("The Charter") available at<http://www.europarl.europa.eu/charter/pdf/text_en.pdf> accessed on 22nd June, 2021

[51] Data Subject means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity'. See article 1 and article 1.3 of the Nigeria Data Protection Regulation 2019 available at <https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf> accessed on 23rd July, 2021. See also art. 8 of the Charter of Fundamental Rights of the EU, 2000/C 364/01 Official Journal of the European Communities <https://www.europarl.europa.eu/charter/pdf/text_en.pdf>Accessed on 9th August, 2021

[52] See D. Manolescu, 'Privacy vs Data Protection'E-Crime Expert Blog, Data Protection and Privacy Awareness (Brussels. November 27, 2012) <https://ecrimeexpertblog.wordpress.com/2012/11/27/privacy-versus-data-protection/>Acessed on 15th July, 2021

[53] Ibid.

[54] See article 8 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108Strasbourg,28.I.1981.<https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>Accessed on 22nd July, 2021

[55] Ibid. See also article 8 of the Charter of Fundamental Rights of the European Union. See also article 31 of the Nigeria Data Protection Regulations (Supra n.10).

5. Right to Privacy and Data Protection in selected Jurisdictions

Separating right to privacy from data protection though superficially appears to be a distinction without difference, the distinction between the two concepts is appreciated using the jurisprudence of EU. In some jurisdictions right to privacy and right to data protection are fused without any clear line of demarcation between the two rights.[56] An appreciable understanding of jurisdictional difference would require examining right to privacy and data protection in the selected jurisdictions.

6. Right to Privacy and Data Protection in EU Jurisprudence

The concepts 'right to privacy' and 'data protection' within the jurisprudence of EU are like two streams of water flowing from the same spring through separate channels into a meander separated by a watershed. The two concepts may be similar but are definitely not the same in EU jurisprudence. Although, a mere examination of the concepts may induce a tendency to regard or deal with right to data protection as an expression of right to privacy, the conceptual approach to the EU to subject draws a distinction between both rights and the distinction as enshrined in the ECHR and the Charter cannot, presumably, be merely symbolic.[57] This is because the two fundamental EU human rights instruments separately guarantee right to privacy and fundamental right to the protection of personal data.[58]

The jurisprudence of the ECHR and the Court of Justice of the European Union (CJEU) demonstrates that in spite of substantial overlaps there are significant differences between right to privacy and right to data protection, especially, as regards their scopes and limitations.[59] In Europe generally, there are two distinct frameworks for protection of fundamental human rights. The first system is the ECHR ('the Convention')[60] and the final arbiter on the Convention is the European Court of Human Rights ('ECHR') established by article 19 of the Convention.[61]

---

[56] For instance in Nigeria and India, data protection is assumed to be an extension of right to privacy rather than a distinct and separate fundamental human right.

[57] Ibid.

[58] Ibid.

[59] Reference to EU jurisprudence here is because the EU appears to have set the pace for a comprehensive approach to data protection. Today, the principles formulated by the EU have been adopted as the underlying principles that underscore data protection. Also, EU appears to have a clear jurisprudential distinction between the right to privacy and right to data protection.

[60] It is an international agreement between the 47 States of the CoE in which all the member states of the EU are part of this organization including however third states such as Switzerland, Russia, and Turkey.

The second framework for the protection of fundamental rights in Europe is based on the jurisprudence of the Court of Justice of the CJEU[62] which developed as general principles of EU law in close alignment with the Convention system but is now based on the Charter.[63]

Both article 8 of the Convention and article 7 of the Charter guarantee right to privacy. In addition, article 8 of the Charter then provides that 'everyone has the right to the protection of personal data concerning him or her' and that such data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[64]The provision further guarantees right of access to data including the right to such data rectified.[65] Meanwhile, no corresponding provision on data protection exists in the Convention.[66] This therefore supports the submission that the difference between right to privacy and data protection in the EU jurisprudence is not merely symbolic.[67] Article 8 of the Charter does not only distinguish between data protection and right to privacy, it also lays down some specific guarantees of fundamental right to data protection.[68] Nonetheless, the EU jurisprudence still considers privacy to be at the core of data protection notwithstanding the distinction between them.

[61] The ECtHR hears complaints from individuals on allegation of breaches of human rights by signatory states. See articles 19-51 of the ECHR.

[62] The Court of Justice of the European Union (CJEU) interprets EU law to make sure it is applied in the same way in all EU countries and settles legal disputes between national governments and EU institutions. It guarantees the protection of fundamental human rights within the EU<europa.eu/european-union/about-eu/institutions>accessed on 22ndJune, 2021.

[63] The ECtHR (the Strasbourg Court) applies the ECHR (The Convention) while the CJEU (the Luxembourg Court) applies the Charter of Fundamental Freedom of the EU (the Charter). See Charter of Fundamental Rights of the European Union C364/20, Official Journal of the European Communities 18.12.2000 available at <http://www.europarl.europa.eu/charter/pdf/text_en.pdf> accessed on 22nd July, 2021

[64] That is apart from article 7 of the Charter which separately guarantees the right to privacy.

[65] See article 8 of the Charter.

[66] There is no equivalence of article 8 of the Charter in the Convention.

[67] Despite the omission, the court has nevertheless applied article 8 of the ECHR (covering the right to privacy) to give rise to a right of data protection as well in theECtHR in the cases of Amann v Switzerland, No. 27798/95, ECHR 2000-II, para. 65;Rotaru v Romania [GC] App no 28341/95, ECHR 2000-V, para. 43.

[68] See art. 8 of the Charter of Fundamental Rights of the EU and art. 8 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

7. Right to Privacy and Data Protection in the United States

In the US, data protection is a sub-set of right to privacy and it is not separately treated as a distinct fundamental right. In the first place, the constitution of the US does not contain an elaborate provision on right to privacy; right to privacy is subsumed from the provision of the Fourth Amendments to the constitution. Conversely, there is a clear line of demarcation between privacy and data protection in Europe; and the two rights are regarded as distinct fundamental rights, each having its specific guarantees.

The approach of the US to data protection is also quite different from the EU. Unlike in EU, no single-comprehensive codified data protection legislation exists in the US. The US adopted a rather sector-specific approach in which different enactments on data protection exist both at the states and federal level. In effect, in the US, legislation that exist on data protection are either sector-specific or are legislation focusing on particular types of data.[69]

Another distinctive factor between the EU and the US as regards data protection is that what is regarded as 'personal data' in Europe[70] is, in the US, referred to as 'personal information.' Therefore, privacy and data protection is more of self-regulation in the US than what obtains in the EU where there is comprehensive data protection legislation enforced by public authorities.[71] The provisions on protection of personal information in the US are provided for by different enactments in such a manner that the line of demarcation between right to privacy and data protection is somehow blurred. This is because some of the laws that make specific guarantee for the protection of personal information do so as part of protection of right to privacy. For instance, the Federal Trade Commission Act of 1914 empowers the Federal Trade Commission (FTC) to bring enforcement action against any unfair and deceptive practices on consumers and to further enforce privacy and data protection regulations and not as an enactment for the protection of personal data as a distinct fundamental human right. Thus, most of

[69] ICLG.Com: Data Protection 2019 available at <https://Iclg.Com/Practice-Areas/Data-Protection-Laws-And-Regulations/Usa> accessed 25th July, 2021

[70] Under article 2(a) of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data,'Personal Data' is 'any information relating to an identified or identifiable individual ('data subject')'. In the US information relating to individuals is regarded as 'personal information.' Again, the definition of personal information is not uniform in States in the US as certain data may be considered as person information in one state for one person or under one regulation but not for another.

[71] J. Kurblija Op. cit.

the enactments that would be examined on the protection of personal information would be dealt with under the right to privacy.

The above nonetheless, some enactments worth being mentioned as they make provision for protection of personal information. For instance, the Driver's Privacy Protection Act, 1994 regulates the processing, use, storage and retention of personal information such as photographs, social security numbers, driver's identification number, name, address, telephone etc. obtained by the State Department. The Children's Online Privacy Protection Act 1998 was enacted to govern personal information relating to children. The Act regulates and prohibits collection of certain information online about a child less than 13 years. It also requires the publication of privacy notes and requires collection of verifiable parental consent when information from a child is being collected. While Video Privacy Protection Act, 1988 protects wrongful disclosure of videotape, rental or sale of records, audio visual materials including online streaming, the Cable Communication Policy Act, 1984 protects subscribers of Cable Communications. Even though these enactments deal with protection of personal information (data protection), they are probably considered as part of privacy protection as it is glaring from their names.[72]

As earlier noted, the United States' approach to privacy and data protection is either sector-specific or data-type specific. The sector-specific laws include those covering healthcare and financial services, telecommunications and education. For instance, Gramm Leach Bliley Act, 1999 (GLB) governs protection of personal information in the custody of banks, insurance companies and other companies in financial services industry. It also addresses non-public personal information including any information that a financial service company collects from its customers in connection with provision of services. Fair and Accurate Credit Transaction Act, 2003[73] was enacted to restrict the use of information having anything to do with an individual's credit standing, credit capacity, credit worthiness, character, and general reputation etc. While Telephone Consumer Protections Act and Associated Regulations regulate calls, text messages to

[72] Driver's Privacy Protection Act of 1994; The Children's Online Privacy Protection Act 1998; Video Privacy Protection Act 1988 and Cable Communication Policy Act of 1984

[73] This was an amendment to Fair Credit Reporting Act 1978

mobile devices, calls to resident at phones meant for marketing purposes or using automated dialing systems or pre-recorded message, the Family Education Rights and Privacy Act, 1974 provides students with the right to inspect, revise their students records for accuracy and prohibits disclosure of those records or other personal information on the students without the students (in some instances) parent's consent.

From the above, it is obvious that the US has no plenary data protection regulations. What it does is to make the authority of its enforcement agency, Federal Communication Commission (FCC), very broad to set the pace on data security and federal privacy.

8. Right to Privacy and Data Protection in India

As of date, India has no comprehensive legislation dealing with data protection and privacy. Though the existing legislation and policies impacting on data protection are essentially sector-based, India has Information Technology Act, 2000 (IT Act) which, among others, govern collection, process and use of personal data and, what the Act regarded as, 'sensitive person data[74] or personal information'[75]. Other sector-based Acts, rules and regulations also exist regulating personal information/data in India. In effect, India has key-sector specific laws or regulations impacting on data protection.[76]

The IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 ('IT Rules') can be regarded as the primarily legislation[77] impacting largely on data protection/privacy in India. The two pieces of legislation protect 'personal information' and 'sensitive personal data or information.' These are information relating to password, bank account, credit details etc.

Under the IT Act, it is an offence to secure access a computer system or network or

[74] See S2(1)(o) of the Information Technology Act, 2000 (IT Act).

[75] Like it obtains in Nigeria, India also adopts the mixture of the 'term personal information or personal data' to describe what in Europe is regarded as 'person data' and 'personal information' in the US.

[76] These include legislation relating to telecommunication, banking, medicine and healthcare, insurance, right to information and the Aadhaar scheme.

[77] That is the IT Act, 2000 and the IT Rules, 2011

'downloads, copies, or extracts any data, computer data base or information from such computer' or conceals, alters, steals, or destroys any computer source code with an intention to cause damage. The offender is liable to pay damages[78] in form of compensation not exceeding the sum of INR 1,00,00,000 (Rupees One Crore) to the person so affected.[79]

Apart from the IT Act, the IT Rules made there under also impact on data protection in India. For instance, rule 4 of the IT Rules makes it mandatory for any one dealing with information provider's information to make and provide privacy policy for handling of or dealing in such information while rules 5 forbids any person from collecting sensitive personal data/information unless the collection is for a lawful purpose and necessary for that purpose. It is also required that the owner/holder of the information be made aware of the collection, its purpose, and its intended recipients.[80]

Besides the IT Act and the IT Rules, the Indian Telegraph Act, 1885 ('Telegraph Act') is an enactment which, though not primarily a data protection legislation, impacts on data protection in India. Section 5 of the Act allows the government to intercept or authorize the interception of telegraphic message in the interest of public safety, the security of the State, sovereignty and integrity of India, friendly relations with foreign States, public order or for preventing incitement to the commission of an offence.

Apart from the above, other regulations also exist, this include; Clause 21 of the National Long Distance Licence, Clauses 37, 39 of the Unified Access Service License and Clause 42 of the Cellular Mobile Telephone Service, State Bank of India Act, 1955; section 44 of the Banking Companies (Transfer and Acquisition of Undertakings) Act, 1980 and section 3 of the Public Financial Institutions (Obligation As To Fidelity And Secrecy) Act, 1983 ('PFI Act') and Credit Information Companies (Regulation) Act, 2005 ('CIC Act') as well as the Credit Information Companies Regulations, 2006 ('CIC Regulations') among others.

[78] See section 43 (a), (b) and (i) of the IT Act.
[79] Ibid.
[80] Ibid.

9. Right to Privacy and Data Protection in Nigeria

Until the introduction of the Nigeria Data Protection Regulation (NDPR) in 2019, Nigeria did not have comprehensive data protection legislation that is comparable in operation to what obtains in Europe.[81] Then what largely existed were sector-specific legislation enshrining provisions impacting on data protection in the sector.[82] The Nigerian Data Protection Regulation 2019[83](NDPR) issued by the National Information Technology Development Agency (NITDA) is the first comprehensive though subsidiary data protection in regulation in Nigeria.[84] The Regulation is divided into four different parts namely; part one (the objectives, scope and definition of terms);[85] part two (governing principles of data processing);[86] part three[87] (rights of Data Subjects[88]) and part four (implementation mechanism, administrative redress).[89]

The Regulation in 2.1 enshrines the underlying principles of personal data and this requires, among others, that personal data be collected and processed accurately in line with specific lawful purpose consented to by the data subject without prejudice to the dignity of human person. It also requires such data to be stored only for the period within which it is reasonably needed during which period it should equally be secured against all foreseeable hazards or breaches. It

---

[81] B. O. Jemilohun and Prof. T. I. Akomolede, 'Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative' [2015] (3)(4)Framework Global Journal of Politics and Law Research;1-16<eajournals.org/wp-content/uploads/Regulations-or-Legislation-for-Data-Protection-in-Nigeria.pdf>Accessed on 5th June, 2021

[82] ICLG.com,'Nigeria: Data Protection 2019' available at <https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria> accessed on 28th July, 2021

[83] This regulation was issued on 25th January 2019 by the Nigerian Information Technology Development Agency (NITDA) pursuant to Sections 6, 17 and 18 of the NITDA Act. By virtue of Part Four, Paragraph 4.2 of the Regulation, a breach of the guidelines is deemed to be a breach of the NITDA Act.

[84] NITDA was established by the NITDA Act 2007 with the mandates to, inter alia, develop information technology in Nigeria through regulatory policies, guidelines, standards, and incentives; and to ensure the safety and protection of the Nigerian citizen's personal identifiable information (personal data) and by extension a successful implementation of the regulation on data protection.

[85] See paragraphs 1.1, 1.2 and 1.3 of the Regulation.

[86] Others include third party data processing contract, advancement of right to privacy, penalty for default, transfer to a foreign country and exceptions in respect of transfer to a foreign country. See, paragraphs 2.1 to 2.12 of the Regulation.

[87] See paragraph 3.1 of the Regulation.

[88] According to the Regulation, 'Data Subject' means 'any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.'

[89] Ibid., paras.4.1 to 4.3

is observed that these principles are in line with article 5 of the EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Regulation further provides indicia for measuring what amounts to lawful purposes.[90] Restriction is however placed on the transfer of data to a foreign country except in compliance with the Regulation and the supervision of the Attorney General of the Federation (AGF).[91] In the event the Agency[92] or the AGF makes no decision as to the adequacy of safeguards in a foreign country, a transfer or a set of transfer of personal data to a foreign country or international organization shall only take place with the consent of the Data Subject after being informed of the risk or if the transfer is absolutely necessary.[93]

Other sector-specific regulations impacting on data protection in Nigeria exists and they include the Central Bank of Nigeria Consumer Protection Framework (CBN-CPF).[94] Other laws impacting on data protection in Nigeria include Credit Reporting Act, 2017;[95] Cybercrimes (Prevention and Prohibition, etc.) Act, 2015; Evidence Act, 2011; Freedom of Information Act, 2011[96] and National Health Act, 2014 (NHA), the Cybercrimes (Prohibition, Prevention etc.) Act 2017, Freedom of Information Act, 2011 (FOI Act), National Health Act, 2014 (NHA), the NCC (Registration of Telephone Subscribers) Regulation 2011, Federal Competition and Consumer Protection Act, 2019 (FCCPA) etc.[97]

10. Conclusion

This paper looked at the right to privacy and right to data protection in the light of their scopes and application in the online environment. This necessitated an evaluation of the legal framework for right to privacy as well as the right to data protection in online. This paper established that Relationship exists between Right to Privacy and right to Data Protection especially on the digital

[90] See paragraph 2.2of the Regulation.
[91] Ibid.,para. 2.11
[92] i.e. NITDA
[93] See para. 2.12 (a) to (f) of the Regulation
[94] Through a letter dated 7th November, 2016 with reference No: CPD/DIR/GEN/CPF/03/004, the CBN issued the Consumer Protection Framework 2016 in exercise of the powers conferred on it by the CBN Act of 2007 (as amended) and the Banks and Other Financial Institutions Act of 2007 (BOFIA).
[95] Credit Reporting Act 2017<https://www.lawyard.ng/wp-content/uploads/2017/06/Credit-Reporting-Act-2017.pdf>Accesed on 3rd October, 2021
[96] Cap. E14 LFN 2004
[97] Enacted on 6 February, 2019

environment. However, the paper similarly finds that there is a line of difference in the scope and application of right to privacy as they apply both online and offline. The difference is informed by the uniqueness of the jurisprudential exposition of the two concepts in difference jurisdiction. Thus, while right to privacy is a fundamental right across many jurisdictions, data protection is not except within the context of the EU jurisprudence. Thus, this paper selected and examines the right to privacy and data protection in EU jurisprudence, United States, India and Nigeria for an appreciable understanding of the proper articulations of right to privacy and data protection. Hence, this paper finds that while the line of demarcation between privacy and data protection is blurred in the US, Nigeria and India, it is a clearly defined line in EU. Again, the paper finds that right to privacy and data protection are separate and distinct fundamental rights in EU, right to data protection is not a fundamental right in Nigeria, India and the United States.

11. Recommendations

The authors recommend the followings;

1. Adoption of speedy but effective legislative approach to privacy protection by States, especially Nigeria, to cater to the challenges of the application of right to privacy in the online environment.
2. Legislative approach should be tailored towards ensuring that the speed of technology does not outpace the processes of legislation and regulations on right to privacy and data protection.
3. Regulatory agencies having the power to enforce compliance with the provisions of NDPR 2019 and its Implementation Framework, 2020 should enforce compliance with the requirements of privacy-by-design enshrined in NDPR and the annual filing of data protection audit report by data controller and processors.
4. Data Protection Impact Assessment (DPIA) and data protection audit should contantly be conducted to assess the level of compliance with the country's privacy and data protection laws, and equally evaluate compliance by individual and businesses including government and non-governmental organizations.
5. Civil Society Organizations should serve as watch dogs and be active and alive to hold government, individual and businesses accountable to ensure derogation from right to privacy and data protection complies with the international standard.