International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Overview of the Perceptions on the Dilemma between Data Privacy and Public Security Challenges in Africa

Pidalatan Eyana MANZI

School of International Law, Zhongnan University of Economics and Law; Nanhu Square, Hubei, China
Email: *princeiznam[at]gmail.com*

Abstract: ***The protection of privacy and personal data is increasingly becoming a predominant issue in Africa with the development and spread of new technologies and connected devices. The search for the right balance between security and privacy has always been a conundrum for States and a subject of discussion in the public debate. Likewise, approaches adopted by States on the Continent differ from one country to another. Several countries have adopted data protection laws, and among them, few have implemented data protection authorities, but many countries are still to enact frameworks to protect personal data. In addition, the spillover of terrorism and violent extremism threats to public security has led many States to introduce laws on surveillance, personal identification and biometric data collection. However, the lack of adequate data protection frameworks in most countries, amidst inadequate safeguards and remedies, weak oversight mechanisms and potential for abuse of surveillance against dissenting opinions by government agencies do not provide for a transparent and accountable processing of personal information. The present research, using a hybrid methodology, including doctrinal, comparative and quantitative methods, briefly presents the legal framework surrounding data privacy and the nexus between data privacy and security on the Continent and provides an analysis of the perception of privacy and data protection in Africa.***

Keywords: Data Privacy, Public security, Surveillance, Terrorism and Violent Extremism

1. Introduction

The research of the right balance between privacy and security has always been at the center of debates for many years. Striking the right balance between privacy and security is a complex issue that varies depending historical and socio political contexts. In recent years, the threat of violent extremism and terrorism has spread in Africa over all regions of the Continent, threatening the way of life of millions of people. In the same time, the Continent has known an exponential rise of digital services and the growing access to internet. The population of internet users in Africa was estimated at around 570 million in 2022, more than doubling, compared to 2015 (Saleh, 2023). Hence, the conjunction between violent extremism, terrorism and the protection of personal data is increasingly apparent. At first, the internet, social media and smartphone have become new digital weapons of war (Liang, 2022, p73). Indeed, violent extremist and terrorist groups use the internet and social media as platforms for recruitment and encouraging radicalization, communication, disinformation, fundraising, planning and broadcasting acts of terror.

In response to these threats, many Countries have developed strict counter terrorism and surveillance laws allowing the use of large amounts of personal data and information by State entities, including intelligence and law enforcement agencies. Several countries have even used personal databases to create systems of mass surveillance including surveillance by CCTV, biometrics and personal profiling. However, sometimes, the perception and expectations of the people, whose safety is at risk, are often eroded. What must be people expectations regarding privacy and security? In reality, the value of privacy is very dependent on the background of every society and community. Hence, people's expectations with regard to privacy and security also vary. Some consider that the withdrawal of privacy and privacy rights is too much a price to pay for the purpose of security. Some other do not feel at all threaten by the proliferation of security measures such as mass surveillance. Others between the two tendencies are just doubtful that surveillance measures and technologies are actually efficient in preventing terrorism to counter balance such infringement on privacy rights.

It is therefore crucial, in implementing policies or in the legal debate to have an overview of the perception and public understanding of security imperatives and privacy rights. Decision makers at their level, are sometimes surprised about the negative public reception of enforcement measures that they take on behalf of ensuring security when citizens are not willing to sacrifice their privacy for more security. In this article, we offer through a survey, an overview of privacy and security perceptions in Africa and the necessary balance that must exist between the two concepts. It offers an insight of the perception of data privacy on the Continent and its relationship with public security and fight against terrorism and violent extremism.

2. Literature Review

Privacy linked to data and data protection in its broad sense, has particularly drown attention in recent years due mainly to development in technology. The arsenal of researches on the topic is quite limited especially when it comes to data protection in the areas of public security. In Africa, data protection has even been less of a research topic for scholars as it is still an emerging field of law on the continent. Among the very few African scholars who have consistently undertaken to shed light on this very important matter, is Dr. Alex Makulilo of the Open University of Tanzania whose extensive works on the subject in the African context have

been of great relevance. As to date, many countries are still to provide a legislative framework in this regard. Back in 1999, David Banisar in '*Privacy and Data Protection around the World*' noted that no country in Africa had data privacy legislation. Several scholars such as Bygrave (2002) and Serge Gutwirth (2005) shared a similar view, however, Gutwirth went further to point out that even the African Charter on Human and Peoples' Rights 1981 (ACHR) fails to mention privacy. However, a common feature is that even back then, many African States mentioned and provided for privacy protection in their constitutions. Up to date, several African countries have enacted data protection laws and many others are in the process of enactment.

On the theoretical aspect, few scholars on the continent have attempted a definition of the concept. Neethling (2005) appears to be the first author to attempt a definition of privacy in Africa. However, Neethling's concept of privacy largely follows the pattern of Western theories of privacy, particularly in terms of control theory. In that aspect, Banisar (2010) has provided a detailed analysis of the threat posed by ICTs in the African contexts highlighting their impact on information systems and privacy including developments of national ID card systems, biometric passports, DNA databases, and body scanners. He also pointed out other areas of concern regarding communication issues such as surveillance capabilities, identity of users, and cyber-crimes. Likewise, several other scholars such as Alex Comninos, and IlhemAllagui have also fairly dealt with issues and interconnections between ICTs and privacy with an emphasis on the role of ICTs in the context of the Arab spring in Tunisia, Egypt, and Libya. Their literature shows to what extent ICTs, particularly social networks (Twitter and Facebook), were used by the protestors to organize and wage protests and at the same time to what extent and how the regimes in those countries relied on the same facilities to snoop on protestors with no regard to their privacy rights

3. Research Methodology

The methodological approaches used in this research are diverse. A doctrinal approach is used to examine the legal framework surrounding data privacy in Africa at regional, sub regional and national levels. Complementarily, a quantitative research methodology has been used through a survey, to analyze the perception of data privacy rights in Africa and their importance in relation to public security, especially concerning terrorism and violent extremism. Therefore, an online survey was conducted through a questionnaire deployed on KoboToolbox and KoboCollect. The survey was conducted from 6 to 26 January 2023 by accessing the online questionnaire on a web page provided by KoboToolbox. The link to access the web page was shared by emails and WhatsApp. The data collected from the questionnaires were then imported in Excel format for treatment and cleansing. Microsoft Excel and Kobo analyze data were later on used alternatively for the construction of graphics and charts.

Most questions proposed in the survey were closed questions, with multiple or double choice answers. The questionnaire contained 23 questions divided into 5 parts. The first part, entitled "Personal information" was to collect information about the nationality of the participant; his/her gender and age. The second part, titled "General information" (questions 1 to 5) was about the participant's habits such as his/her frequency of using internet and ICTs, the type of websites or services that he/she uses the most. The third part "About data protection" contained 4 questions (6 to 9) and was used to assess the participant's knowledge and familiarity about data protection and its implementation in his country. The fourth part (questions 10 to 15) was about confronting privacy rights to security imperatives. Hence, choices were to be made between privacy and security and to report as to whether or not the participant was ready to sacrifice some privacy in exchange for more security and if he/she was willing for law enforcement and intelligence agencies to access his/her personal data in order to protect public security or fight against violent extremism and terrorism. The last part of the survey (questions 16 to 23) contained miscellaneous questions about the African Convention on Cybersecurity and Personal Data Protection, data sovereignty, the fear of surveillance practices and the fear of abuse of surveillance by states agencies in fighting terrorism and violent extremism.

Overall, 514 people have participated in the survey from 6 to 26 January 2023. Participants originated from 46 African countries and all 5 Sub-regions. 7 French and 1 US participants also took part in the survey. The distribution based on gender indicates that male participants represented around 61% of participants and female participants around 39%. Concerning age, the participants aged between 25-34 represented 32.68% of the population surveyed, closely followed by the 35-44 who represented 31.13%.

Table 1: Geographical distribution of participants

Country	Frequency	Percentage	Country	Frequency	Percentage
Togo	87	16,92	Nigeria	8	1,55
Burkina-Faso	31	6,03	Rwanda	8	1,55
Cameroon	22	4,28	Libya	8	1,55
Benin	22	4,28	Tunisia	8	1,55
Ethiopia	20	3,89	France	7	1.36
Burundi	20	3,89	Mauritania	5	0,97
Chad	20	3,89	Angola	5	0,97
Senegal	19	3,69	Liberia	5	0,97
Egypt	18	3,50	Cape Verde	4	0,77
South Africa	16	3,11	Lesotho	3	0,58
Mali	15	2,91	Malawi	2	0,38
DR Congo	14	2,72	Gambia	2	0,38
Morocco	14	2,72	Mauritius	2	0,38

Niger	14	2,72	Zambia	2	0,38
Côte d'Ivoire	13	2,52	Uganda	2	0,38
Central African Republic	13	2,52	Zimbabwe	2	0,38
Ghana	10	1,94	Comores	1	0,19
Guinea Conakry	10	1,94	Sierra Leone	1	0,19
Namibia	10	1,94	Mozambique	1	0,19
Madagascar	10	1,94	Kenya	1	0,19
Djibouti	9	1,75	Seychelles	1	0,19
Republic of Congo	9	1,75	Eritrea	1	0,19
Gabon	9	1,75	Tanzania	1	0,19
Algeria	8	1,55	United States of America	1	0,19

Valeur	Fréquence	Pourcentage
25-34	168	32.68
35-44	160	31.13
45-59	92	17.9
18-24	59	11.48
+60	23	4.47
12-17	12	2.33

Figure 1: Distribution of participants based on age

4. Research findings and discussion

4.1The protection of data privacy with regard to security challenges

The concept of privacy is largely accepted in Africa as a relatively recent one, imported from the West (Makulilo, 2016), with regard to the social and cultural organization of most African communities, based on the dominance and preeminence of the community on the individual and where individuals' interests are inferior to the group (Olinger et al, 2007). Moreover, the African Charter on Human and Peoples' Rights, which is the main human rights instrument on the Continent, does not provide any express provision guaranteeing privacy, let alone data protection. These settings have led many commentators argue that privacy and data protection are not considered as fundamental human rights in Africa or that Africans do not value privacy (Bygrave, 2008; Gutwirth, 2002). However, such a conclusion does not seem adequate for several reasons.

In fact, there are three layers of privacy and data protection in Africa. The first level of protection is through international law- mainly- international human rights law. Indeed, the Universal Declaration of Human Rights (article 12) and the International Covenant on Civil and Political Rights (article 17) - to which 53 African States are parties- provide a universal and strong privacy protection. In International Humanitarian Law (IHL), data are progressively becoming strategic assets in modern warfare (Work et al, 2020). Although its protection is limited, IHL also provides several rules that apply and guide the processing of personal data and information in times of armed conflicts.

At regional level, as mentioned before, the African Charter on Human and Peoples' Rights does not specifically provide for the protection of privacy. However, according to commentators, such a protection can be implicitly inferred from other provisions such as article 5, which protects dignity. The African Charter on the Rights and Welfare of the Child is thus, the first treaty on the Continent to provide a specific protection for privacy rights (article 10). The

African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014, also known as the Malabo Convention is the comprehensive treaty dealing with data protection on the Continent. However, due to a lack of signatories States, the Convention is yet to enter into force. At sub-regional level, privacy and data protection are regulated by instruments adopted within the frameworks of the different Communities such as the ECOWAS Supplementary Act, the SADC Model Law or the EAC's Bill of Rights and Legal Framework for Cyber Laws. At national level, privacy and personal data are protected in different ways. Firstly, they are protected in the Constitution of more than 50 African countries with different scopes and applications. They essentially protect privacy by prohibiting arbitrary searches, restricting collection and processing of information relating to family and private affairs and protecting privacy of communications. Secondly, they are protected in several countries through judicial decisions and case law. At last, but not at least, many countries on the Continent - to date, about 33 countries - have enacted comprehensive data protection laws.

With regard to public security and the threats posed by the new forms of criminality, mainly violent extremism and terrorism, many Countries on the Continent have enacted specific legislations that infringe on the private sphere, through communication interception, reinforced surveillance, monitoring of online activities, etc. For instance, several countries have adopted provisions requiring telecom and Internet Service Providers (ISP) to install equipment and software that permit access for surveillance purposes and to save all data that enables the identification of persons for a period of up to 10 years (CIPESA, 2021, p 7). Such a requirement can seem excessive with regard to the AU Convention on data protection, article 22, providing that personal data should not be kept for no longer than necessary. In addition, some national provisions directly infringe on the rights to privacy with generalized surveillance practices, imposing for instance, on internet cafes to install surveillance cameras inside cafés and require identification cards to monitor users' activities (CIPESA, 2021, p 8), which constitutes a violation to the secrecy and privacy of personal correspondence, guaranteed by national constitutions. Moreover, some counter terrorist legislations allow enforcement agencies to conduct physical searches on individuals and property, where there is "reasonable suspicion" of terrorist activity without requiring a warrant, regardless if the threat is imminent or not (Adarkwah, 2020), which is inconsistent with the fundamental rights guaranteed by most national constitutions.

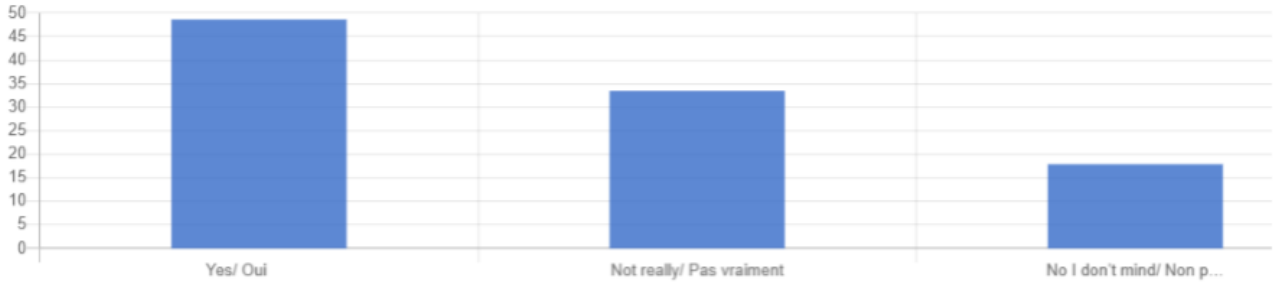
Therefore, many laws do not align with the spirit and fundamental liberties guaranteed in national constitutions and international law. Furthermore, in practice, they present deliberate flaws and potential for abuse.

4.2 The perception of participants regarding privacy and security

Among the population surveyed and their attachment to data privacy in general, just 48.64% of participants have said to be concerned about the treatment of their personal information that are collected while online while 33.46% where not really concerned and 17.9 did not mind at all.

5) Are you concerned about the treatment of your personal information that are collected?/ Etes-vous soucieux du traitement réservé à vos données personnelles qui sont collectées?

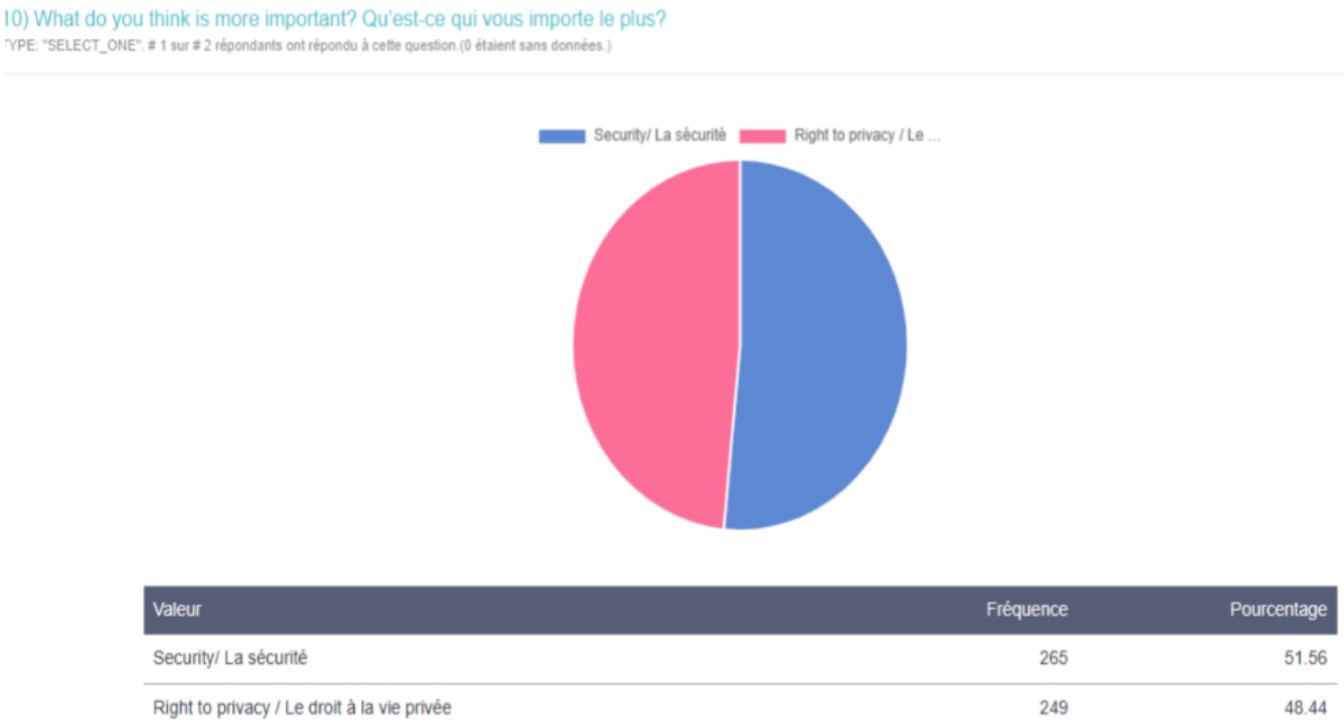
TYPE: "SELECT_ONE". # 1 sur # 2 répondants ont répondu à cette question.(0 étaient sans données.)



Valeur	Fréquence	Pourcentage
Yes/ Oui	250	48.64
Not really/ Pas vraiment	172	33.46
No I don't mind/ Non peu importe	92	17.9

Figure 2: Distribution of participants according to the level of concern for their personal data .

Regarding the most important feature between security and privacy, a slim majority (51.56%) opted for security against (48.44%) for privacy. In the same idea, when asked if they think that, considering the security context in their country or region, the Government should have the right to track and monitor online activities, a majority of participants responded yes (61.09%) against (38.91%) who considered that governments should not monitor online activities.



Valeur	Fréquence	Pourcentage
Security/ La sécurité	265	51.56
Right to privacy / Le droit à la vie privée	249	48.44

Figure 3: The opinion of participants regarding privacy and security

Similarly, almost the same proportion of responses were recorded on the question, "*would you like the Government to access your personal information (address, online activities, biometric data, facial recognition data), in the war against terrorism and violent extremism?*". 62.45% percent responded "yes", and 37.55% "no". However, less participants (58.17%) agreed to have their personal information accessed by the Government for other public security reasons such as (COVID and health measures, immigration, public order, etc.) against 41.83%. Moreover, 47.86% of participants have said to have "*a little bit*" fear of a mass surveillance society, where everything is controlled by the State. Concerning surveillance methods, 58.95% of the pool has declared to be concerned about facial recognition and profiling while 41.05% are not.

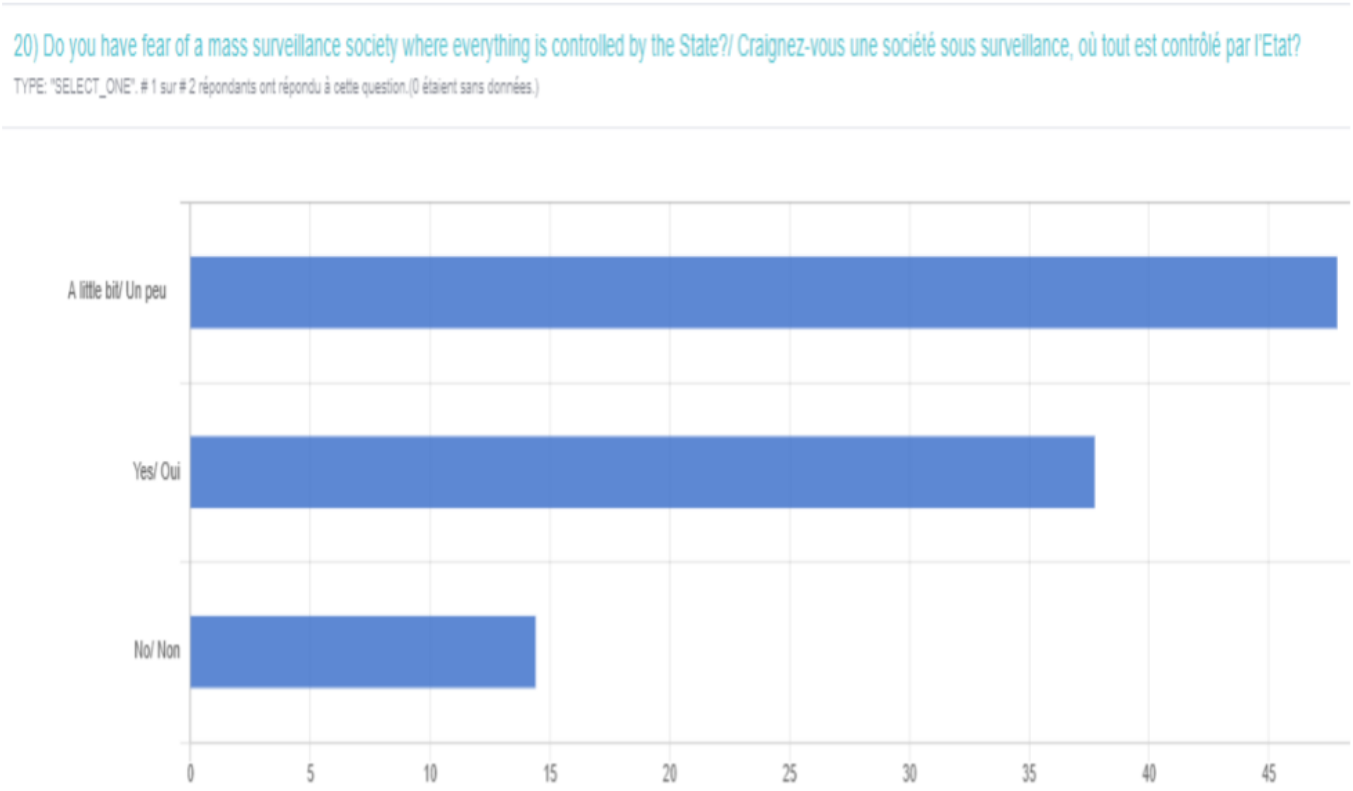


Figure 4: Participants opinion on mass surveillance society

Valeur	Fréquence	Pourcentage
Yes/ Oui	358	69.65
No/ Non	156	30.35

Figure 5: Perception of participants' fear of abuse of personal information treatment by law enforcement in fighting violent extremism and terrorism

Regarding abuses in the treatment of their personal information by law enforcement and intelligence services, a large majority of the pool responded (69.65) recognized to "*have fear*" about such abuses.

An interpretation of these results is that in general, participants tend to value security more than privacy. However, the margin is very narrow. Nevertheless, even for those that value privacy more, they seem incline to agree to State monitoring internet activities within certain limits. For instance, more participants (5 points of difference) seem more eager to State surveillance for fighting violent extremism and terrorism reasons, than for other public security purposes such as public health protection, insuring public order or immigration. Moreover, over 85% of participants have reported to be relatively afraid of a mass surveillance society where everything is controlled by the State. Another instance is that 58.95% of the participants have declared to be concerned about surveillance practices such as facial recognition and profiling.

In addition, the survey confirms an important aspect regarding the potential for abuse of surveillance and personal data processing by law enforcement and intelligence agencies. A large majority (69.71%) of the pool fears abuse of personal information treatment if enforcement agencies were to access them in the fight against terrorism and violent extremism. Still in relation to surveillance, 85.44% of participants declare "yes" to having fear and "a little bit" fear of mass surveillance society and 58.83% to have concerns about facial recognition and profiling. Therefore, the use of surveillance methods and the history of abuse by law enforcement agencies reveals to be a considerable issue for privacy and data protection on the Continent. This reluctance expressed by the participants is reasonable with documented abuses in recent years on the Continent such as in the Pegasus scandals. Indeed, such surveillance software instead of being operated to track terrorist activities as they are designed to, this type of surveillance is performed out of the scope of the law and is mostly targeted towards dissenting opinions.

5. Conclusion and Recommendations

"It is important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience". These are the words of then, US President Barack Obama (Obama, 2013) to justify the implementation of the PRISM Program and revelations about mass surveillance of phone and internet for counter terrorism purposes. Hence, the quest for the right balance between privacy and security has always been subject to debates in most jurisdictions. Areas of uncertainty remain as to how States can stock, use and process personal data in order to ensure public security in a manner consistent with the respect of basic human rights and privacy.

Overall, the present study has permitted to have an interesting and important insight on the perception of data privacy and security interconnections. Privacy is a fundamental human right and its protection in the context of sustainable and efficient counter terrorism activities is crucial. However, many countries in Africa still do not provide sufficient legal protection for the privacy of personal information. To that end, the following recommendations can be made in order to strengthen privacy protection on the Continent.

The necessity to uphold the rule of law for the protection of data privacy while countering terrorism: Counter terrorism and surveillance activities must be conducted in a way consistent with the respect of the rule of law. Beside national legislations, international law provides a framework and limitations for the conduct of such operation. Article 29 of the Universal Declaration of Human Rights provides for a restriction of the right to privacy whereas, such limitation is

(i) provided by the law and (ii) implemented for the purpose of ensuring the rights and freedoms of others, morality, public order and general warfare in a democratic society. Likewise, regarding the International Covenant on Civil and Political Rights, international law practice has provided a limitation to the right of privacy provided in article 17, stating "The right to privacy is not an absolute right. Once an individual is under suspicion and subject to formal investigation by intelligence or law enforcement agencies, that individual may be subject to surveillance for entirely legitimate counter-terrorism and law enforcement purposes" (A/HRC/13/37 para. 13). Moreover, such surveillance is subject to the principles of necessity and proportionality.

The necessity to readapt the African Convention on Cybersecurity and Data Protection: The Malabo Convention adopted in 2014 is still yet to come into force. However, upon such entry into force, there is a need to update this important instrument in order to provide standards of protection adapted to current data privacy challenges, especially, the collection, treatment, storage and use of personal data in relation to criminal investigation, preventing and countering terrorism.

References

[1] Saleh, M. (2023) Internet usage in Africa- Statistics & facts, Statista. Available at statista.com/topics/internet-usage-in-Africa (Accessed: 10 April 2023).
[2] Liang, C.S. (2022) The Technology of Terror: from Dynamite to the Metaverse, in Institute for Economics & Peace. Global Terrorism Index 2022 p 74. Available at: http://visionofhumanity.org/resources (Accessed: 10 April 2023).
[3] Bygrave, L.A. (2008) 'International Agreements to Protect Personal Data', Global Privacy Protection: The First Generation, Cheltenham, UK, pp.15-49, at p. 17. Edward Elgar Publishing Limited.
[4] Gutwirth, S. (2005) Privacy and the Information Age, New York: Rowman& Littlefield Publ.
[5] Makulilo, A.B. (2016) African Data Privacy Laws. Springer, 379 pp. (pp. 228 et seq.).
[6] Olinger, H.N. et al. (2007), 'Western privacy and/or Ubuntu? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa'. The International Information & Library Review, Vol. 39, No. 1, pp. 31-43.
[7] Gutwirth, S. (2002) Privacy and the Information Age, New York: Rowman& Littlefield Publ.
[8] Bygrave, Lee A. (2002), Data protection law: approaching its rationale, logic and limits. Hague/London/ New York: Kluwer Law International
[9] Neethling. J, (2005), The Concept of Privacy in South African Law', The South African Law Journal 18–28
[10] Banisar, D. (2010), 'The Right to Information and Privacy: Balancing Rights and Managing Conflicts', Working Paper, The International Bank of Reconstruction and Development/The World Bank
[11] Adarkwah, S.B. (2020) Counter-Terrorism framework and individual liberties in Ghana, African journal of international and comparative law, volume 28(1), pp, 50-65.
[12] CIPESA, (2021) State of internet freedom in Africa: Effects of State surveillance on democratic participation. Available at https://iapp.org/media/pdf/resource_center/state_of_internet_freedom_in_africa_2021.pdf (Accessed: 15 May 2023).
[13] CIPESA, (2021) How African Governments Undermine the Use of Encryption. Available at https://cipesa.org/wp-content/files/briefs/How-African-Governments-Undermine-the-Use-of-Encryption-Oct-26.pdf (Accessed: 4 May 2023).
[14] Obama, B. (2013) Privacy and Security. Available at www.obamawhitehouse.archives.gov (Accessed: 25 March 2023).
[15] Work, R. and Tara Murphy Dougherty, T.M. (2020) It's time for the Pentagon to take Data Principles more seriously. Available at https://warontherocks.com (Accessed: 13 April 2023).

Author Profile

Pidalatan Eyana MANZI received a Bachelor degree in Political and juridical sciences, with an option in Business Law from University Saint Thomas d'Aquin in Burkina-Faso in 2012 and later on, a Master Degree in International Law from Zhongnan University of Economics and Law in China. His areas of expertise include public international law with a specialty in economic and investment law and data protection law. He is currently a PhD candidate at Zhongnan University of Economics and Law focusing on data privacy issues.