UNIVERSITY OF PRETORIA

FACULTY OF LAW

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

CRITICAL REFLECTIONS ON PRINCIPLES GOVERNING THE PROTECTION OF PERSONAL DATA IN THE DEMOCRATIC REPUBLIC OF CONGO

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE DEGREE OF LL.M (HUMAN RIGHTS AND DEMOCRATISATION IN AFRICA)

BY

FAZILI MIHIGO Christian

STUDENT NUMBER: 21805581

PREPARED UNDER THE SUPERVISION OF

Prof Derek POWEL

(UNIVERSITY OF WESTERN CAPE)

&

Mr Trésor MAKUNYA

(UNIVERSITY OF PRETORIA)

AT THE

UNIVERSITY OF WESTERN CAPE

(Faculty of Law)

29 OCTOBER 2021

PLAGIARISM DECLARATION

I, Fazili Mihigo Christian, student number u21805581, declare as follows:

1. I understand what plagiarism entails, and I am aware of the University's policy in this regard.
2. This mini- dissertation is my own, original work. Where someone else's work has been used (whether from a printed source, the internet or any other source) due acknowledgement has been given and reference made according to the requirements of the Faculty of Law.
3. I did not make use of another student's work and submit it as my own.
4. I did not allow anyone to copy my work with the aim of presenting it as his or her own work

Signature:

Date: 29 October 2021

DEDICATION

To my lovely parents Mihigo Serumisi Thomas and Vunabandi Nkundwanabake Mediatrice

ACKNOWLEDGMENTS

I would like to express my sincere gratitude and appreciation to all persons who, without their support, encouragement and help in one way or another, this dissertation would not have been possible. First and foremost, I thank the Almighty God, the master of times and circumstances, for his love, grace and protection, which he has never ceased to show to me. May his name be glorified forever!

I am extremely grateful to my supervisors Prof. Derek Powel and Trésor Makunya, for their invaluable guidance and insightful suggestions from the initial step in this research that enabled me to understand my subject. Without their constructive criticism, unwavering advice, and practical suggestions, the completion of this dissertation would not have been possible.

I want to express my gratitude to the European Union through the Global Campus of Human Rights and the Royal Norwegian Embassy in Pretoria, South Africa, for funding the Master's in Human Rights and Democratisation in Africa (HRDA). I also thank the Centre for Human Rights, University of Pretoria, for providing me with this opportunity to be part of the prestigious program of HRDA 2021.

I am grateful for my parents Mihigo Thomas and Vunabandi Meditrice, whose constant love, prayers and support keep me motivated and confident. My achievements and success are because they believed in me. Similarly, I extend my thanks to my siblings James, Joel, Steven, Esther, Shalom, Souverain, Cedrick and all my relatives for their moral support and encouragement. I owe my deepest gratitude to my love, Innocente Kabano, who always believe in my abilities. I am forever thankful for the unconditional love and support throughout the entire program and every single day. Many thanks to my law firm, particularly Sabra Mpoyi and Blaise Bikoro, for their financial support during my travel to this program.

I want to acknowledge the special assistance of my colleague Abdulmalik Bello during the whole program and significantly in writing this work. I gratefully acknowledge also the help of my colleagues Davina Murden and Kwame in editing this work. It would be ungrateful not to acknowledge the support and camaraderie of all my HRDA 2021 classmates, especially Wachira, Hilma, Ramou, Benjamin, Christian, Rado, Sanele, and Tobekile, with whom I spent this time of hard work. Their exchange and expertise have opened my mind and given me a different way of perceiving the world.

TABLE OF CONTENTS

ACRONYMS

ACHPR	:	African Charter on Human and Peoples' Rights
ACHR	:	American Convention on Human Rights
AU	:	African Union
AUCCSPD	:	African Union Convention on Cyber Security and Personal Data
ACRWC	:	African Charter on the Rights and Welfare of the Child
ARPTC	:	Post and Telecommunications Regulatory Authority
ARPTIC	:	Autorité de Régulation des Postes, Technologies de l'Information et de la Communication (DRC's Regulatory)
CIPESA	:	Collaboration on International ICT Policy in East and Southern Africa
DRC	:	Democratic Republic of Congo
DPA	:	Data Protection Act
EU:		European Union
ECCAS	:	Economic Community of Central African States
GDPR:		General Data Protection Regulation
HRC	:	Human Rights Council
ICCPR	:	International Covenant on Civil and Political Rights
ICT	:	Information communication technology
OECD	:	Organisation for Economic Co-operation and Development
POPIA	:	Protection of Personal Information Act
SADC	:	Southern African Development Community
UDHR	:	Universal Declaration of Human Rights
USA	:	United States of America

CHAPTER 1: INTRODUCTION

1.1 Background

This research aims to do a critical analysis of principles governing the processing of personal data in the Democratic Republic of Congo (DRC) to assess the extent to which they comply with international and African regional human rights standards applicable to data protection. It principally assesses the gaps in the Telecommunications and Information and Communications Technology (2020 ICT Act) and the developments in the ICT Act while bringing to light its prospect to strengthen the protection of personal data in the DRC. The research also assesses the weaknesses therein that may require development going forward.

Indeed, Africa has registered a significant increase in internet penetration in the last two decades or so. In 2000, the number of internet users in Africa was 4.5 million, and by 2010, the number had rapidly grown to 100 million.[1] According to Minawatts Marketing Group, on 20 May 2021, internet users in Africa were estimated at 590 296 163, representing 12.975,5% of the total internet users in the world.[2] This increase in internet penetration in Africa has facilitated the easier flowing of information between individuals and public and private entities. In addition, it gives everyone with an internet connection the possibility of gathering and sharing information, including personal data.[3]

However, the emerging form of new technologies creates new challenges related to the analysis of data sharing, profiling, tracking, and artificial intelligence.[4] For example, daily human activities are accomplished online with electronic banking and electronic marketing services.[5] Additionally, more data is generated and collected by factors or activities of human beings, such as place, environment, inhabit, devices he carries with him or wears, applications, and devices installed in the home.[6] Consequently, personal data collected from these activities may be used without knowing who accessed them, why they were collected, and what purpose.[7] Furthermore, the lack of an adequate framework and regulations for collecting and processing personal data can violate the right to privacy. In this regard, there is increasing recognition and consciousness of the right to privacy and data protection worldwide.[8]

---

[1] Solar Winds Pingdom 'The incredible growth of the Internet since 2000' (2010) https://www.pingdom.com/blog/incredible-growth-of-the-internet-since-2000/ (accessed 07 September 2021).
[2] Miniwatts Marketing Goup, 'Internet users statistics for Africa' 2021 available at https://www.internetworldstats.com/stats1.htm (accessed 07 September 2021).
[3] ALT Advisory 'Data Protection Africa' 2021, available at https://dataprotection.africa/trends/ (accessed 28 August 2021).
[4] Privacy International 'Data Protection' available at https://privacyinternational.org/learn/data-protection (accessed 28 August 2021).
[5] A Harris et al 'Privacy and security concerns associated with mobile money application in Africa' (2013) 8 *Washington Journal of Law, technology* & Arts 245.
[6] L Abdulrauf & C Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 2, available at https://repository.up.ac.za/bitstream/handle/2263/60613/Abdulrauf_African_2016.pdf? (accessed 6 August 2021).
[7] As above 3.
[8] As above 3.

But, there are severe problems with the enforcement of the right to privacy due to institutional, infrastructural and legislative deficiencies.[9]

Internationally and especially in the DRC, there are gaps of data protection regulatory organs, the relevant legal frameworks and issues around the implementation of the right to privacy and data protection.[10] Accordingly, public and private data practices are mostly left unregulated and unchecked in modernisations in policy and technology. More specifically, they facilitated the collection of personal data such that the personal privacy of people worldwide became threatened and jeopardised.[11] This can have significant implications in protecting individuals' rights and developing the economy of the DRC, Africa, and the world.[12] Therefore, there is an urgent need for a human rights approach that will check the processing of personal data to safeguard the interest of people who are the data subject.[13] This ultimately culminates in the right to data privacy.

Nowadays, states have relatively been engaged in adopting data protection laws and policies that ensure more protection and control of their citizens' rights.[14] Nevertheless, as a matter of general principle and state practice, the formulation and enactment of national laws are guided by the international and regional standards, albeit countries may differ on the degree of adoption of the set of rules due to economic, cultural and religious factors, among others.[15]

At the international level, the right to privacy was expressly recognised under the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[16] Although omitted in the African Charter on Human and Peoples' Rights (ACHPR), other regional treaties such as the European Convention on Human Rights (ECHR) and the American Convention on Human Rights (ACHR) expressly recognised the right to privacy.[17] However, the relevant provisions under these treaties are general.

Until 2018, there was no adequate International instrument dealing with data protection.[18] The increasing calls and efforts to come up with such an instrument finally brought into force the General Data Protection Regulation (GDPR) in Europe.[19] It became the most advanced data protection instrument with its provisions that ensure the security of personal data.[20] Since it came into force, the GDPR has inspired the enactment of data privacy legislation worldwide. Over 16 countries already have

[9] As above 4.
[10] As above 4.
[11] As above 5.
[12] As above.
[13] As above
[14] Thales 'Beyond GDPR: Data protection around the world' (2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world (accessed 26 August 2021)
[15] As above.
[16] Article 17 of the ICCPR and article 12 of the UDHR.
[17] Article 8 of the ECHR and Article 11 of the ACHR.
[18] Thales (n14).
[19] As above.
[20] As above.

data privacy protection laws modelled on the GDPR, including Nigeria, Kenya, Uganda, and Mauritius.[21] More importantly, GDPR is a landmark data protection standard with extraterritorial jurisdiction.[22] As a result, it has influenced the reform of data protection legislations and policies of non-European Union countries, including Africa.[23]

At the African level, the omission of the right to data privacy in the ACHPR has attracted considerable attention from academic scholars. It has been argued that the right to data privacy may be read into the person's right to life and integrity, the right to liberty and security of person, and the right to dignity.[24] This was the approach of the African Commission on Human and Peoples' Rights (African Commission) in *Social and Economic Rights Action Centre and Another v. Nigeria*.[25] To fill the gap, the African Union adopted the African Union Convention on Cyber Security and Personal Data (AUCCSPD) modelled on the GDPR.[26] The Convention defines personal data as:[27]

> [a]ny information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity.

The AUCCSPD mandates state parties to commit to establishing a law that strengthens the protection of physical data and punishes violation of privacy of any kind while allowing for the free flow of personal data.[28] Sadly, only eight countries have ratified the Convention, and it has not come into force since it requires 15 ratifications.[29] However, many African states, including Nigeria, Kenya, South Africa, Uganda and Mauritius, have enacted specific privacy or data protection laws that align considerably with the GDPR.[30]

In the same way, it can be seen that African countries are currently adopting comprehensive data privacy laws and establishing data protection authorities.[31] In total, 28 out of 54 African countries have data protection legislations representing 52%.[32] Nine countries have draft legislation on data

---

[21] M Woodward '16 countries with GDPR-like Data Privacy Laws' (2021). https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws (accessed 26 August 2021)
[22] A Makulilo 'The long arm of GDPR in Africa : reflection on data privacy law reform and practice in Mauritius' 2020, *The International Journal of Human Rights* available at https://doi.org/10.1080/13642987.2020.1783532 (accessed 10 August 2021).
[23] As above.
[24] Singh and Power 'The Privacy awakening: The urgent need to harmonize the right to privacy in Africa' (2019) NUMBER OF THE ISSUE *African Human Rights Yearbook*, 202, *Social and Economic Rights Action Centre and Another v. Nigeria* (2001) AHRLR 60 (ACHPR 2001).
[25] As above.
[26] M Woodward (n 21).
[27] Article 1, AUCCSPD.
[28] Article 8, AUCCSPD.
[29] African Union 'List of countries that have signed, ratified/acceded to the Convention on Cyber Security and Peraonal Data' (2021) https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed 07 September 2021).
[30] As above.
[31] ALT Advisory (n 3).
[32] United Nations Conference on Trade and Development 'Data Protection and Privacy Legislation Worldwide' 2020 available at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed 28 August 2021).

protection, representing 17%, and thirteen countries do not have data protection law, representing 24%.[33] In addition, four countries do not have any data protection law or legislation, representing 7%.[34] In 2019, Kenya and Togo enacted their data protection laws. They were followed by Egypt, whose data protection law was passed on 24 February 2020 and South Africa, whose Protection of Personal Information Act was enacted in June 2020.[35]

Even though some African countries have established data protection legislation with regulatory organs, other countries such as Zimbabwe and Namibia are still drafting legislation on data protection.[36] In other countries like Botswana, Uganda, Lesotho and Angola, data protection legislation was enacted but had not come into force or is enforceable only in limited instances.[37] Other African countries are trying to update existing data protection laws and policies or establish structures of enforcement of existing data protection laws and policies.

On this front, the development in the Democratic Republic of Congo (DRC) has been very slow and insignificant compared to the waves of development of data protection laws in other African countries that are increasingly adopting or updating their data protection laws and regulations. As a result, until now, there is no specific comprehensive data protection legislation in the DRC. Nevertheless, a provision related to privacy can be found in the Constitution of 2006.[38] Despite that provision, other provisions related to privacy could be found in Act 013/2002 of 16 October 2002 on Telecommunications[39] and Act 14/2002 of 16 October 2002 on the creation of the Post and Telecommunications Regulatory Authority (ARPTC).[40] These Acts guaranteed the secrecy of correspondence transmitted by telecommunications. However, they did not capture technological progress at all levels, including the normative, institutional, and infrastructural developments. Also, they constituted a gap paving the way for criticism and rallying calls for amendment.[41] In addition, the lack of provisions that could protect the privacy and personal data against the multiple dangers resulting from the development of information and communication technologies prompted parliament to enact new

[33] As above.
[34] As above.
[35] ALT Advisory (n 3).
[36] As above.
[37] As above.
[38] Article 31 of the DRC Constitution.
[39] Act 013/2002 of 16 October 2002 on Telecommunications in the Democratic Republic of Congo available at http://www.droit-afrique.com/upload/doc/rdc/RDC-Loi-2002-13-cadre-telecom.pdf (accessed 18 August 2021).
[40] Act 14/2002 of 16 October 2002 on the creation of the post and telecommunications regulatory authority available at https://www.droitcongolais.info/files/7.35.11.-Loi-du-16-octobre-2002_Autorite-de-recgulation-de-la-poste-et-des-telecommunications.pdf (accessed 18 August 2021).
[41] International ICT Policy for East and Southern Africa, 'Etat des lieux des libertés sur Internet en République Démocratique du Congo : Les stratégies des gouvernements africains pour étouffer les droits numériques des citoyens' 2016 avalable at https://cipesa.org/?wpfb_dl=242 (accessed 18 August 2021).

legislation.[42] As a result, they were repealed and replaced on 25 November 2020 by Act 20/017 relating to Telecommunications and Information and Communications Technology (2020 ICT Act).[43]

However, although it is not explicitly devoted to data privacy only, Chapter III has some privacy and personal data provisions. It tries to fill in the gap by directly addressing and strengthening issues around protecting the right to privacy, the confidentiality of correspondence and personal data while, overall, improving surveillance accountability.[44] Furthermore, the Act makes criminal the infringement of these rights and provides befitting penalties for such breaches.[45] Where adequately enforced, the Act has the prospect to strengthen the security of personal data and the protection of the right to privacy of network users.

1.2 Problem Statement

There is an increased collection of personal data facilitated by ICTs which, undoubtedly constitute a threat to data privacy.[46] In this regard, the DRC's government and private entities, including banks, schools, hospitals, police, court, etc., increasingly use ICT to collect or process Congolese personal data. As a result, the right to data privacy is threatened due to the lack of specific legislation determining the condition and modalities of processing personal data.

Furthermore, most Congolese are not warned about the threat of their data privacy, and they do understand the importance of protecting their personal data. In addition, the emergence of the Internet and social media in DRC has increased the number of users.[47] Also, there is an increase in the number of internet users, cell phones, and all electronic gadgets in the DRC.[48] Consequently, there is a high risk of data privacy violation in the DRC, where there is currently no data protection legislation ensuring adequate data protection. In this regard, the DRC Telecommunication Act of 2002 did not contemplate the rights of individuals in the digital age, nor did it provide for the required infrastructures that may enable the protection of the right to privacy and strengthen data protection. Therefore, the 2020 ICT Act was enacted to fill this gap and be a fresh and recently enacted law.

---

[42] Explanatory statement of the 2020 ICT Act.
[43] Act 20/017 relating to Telecommunications and Information and Communications Technology available at https://legalrdc.com/2020/11/25/loi-n-20-017-du-25-novembre-2020-relative-aux-telecommunications-et-aux-technologies-de-linformation-et-de-la-communication/ (accessed 18 August 2021).
[44] Articles 131, 132 and 133 of the 2020 ICT Act.
[45] Article 190 of the 2020 ICT Act.
[46] C Nyemba 'Right to Data Privacy in the Digital Era: Critical assessment of Malawi's Data Privacy protection regime' Dissertation HRDA University of Pretoria (2019) 1.
[47] B Kandolo wa Kandolo 'Réseaux sociaux : réflexion sur l'émergence d'une nouvelle forme de gouvernance des droits de l'homme en République Démocratique du Congo' *Revue générale de Droit et Interdisciplinaire de Likasi* (2018) 338 available at https://www.leganet.cd/Doctrine.textes/Decon/ReseauxsociauxetdroitsdelhommePDF (accessed 8 October 2021).
[48] ARPTC' the DRC global rate of cell phone penetration and internet' available at https://deskeco.com/2021/09/03/rdc-larptc-situe-le-taux-de-penetration-global-de-la-telephonie-mobile-471-et-celui-de-linternet (accessed 6 October 2021).

This study seeks to analyse principles governing personal data with regard to the 2020 ICT Act. It assesses the gaps in the 2020 ICT Act with regard to those principles and compares to what extent they comply with international and regional standards.

1.3 Research questions

This research shall attempt to answer the following central question: To what extent do the principles have governing personal data protection in the DRC comply with the international and regional standards on personal data protection?

The following sub-questions will help to answer the main question:

1. What are the international and African regional standards on personal data protection applicable to the DRC?
2. To what extent has the legal framework on personal data protection in the DRC complied with the international and regional standards.

1.4 Research methodology

This study employs desk-based methodology research. It is a qualitative study based primarily on the desktop research method since its focus is on data protection in the DRC, which shall be gauged against the international and regional standards. The method will involve looking at relevant international, regional and domestic legal instruments, applicable government policies and published materials, including textbooks, journals, news and media publications, articles and internet sources. These resources will help in responding to this study's research questions.

The research will also adopt the comparative approach to assess and suggest best practices in Mauritius and South Africa, which have recently adopted comprehensive data protection legislation modelled on the GDPR, which has been influenced the State's data protection legislation across the world. On the one hand, Mauritius was among the first African countries to enact data protection legislation with international standards. In addition, it was the first country in Africa, with the Data Protection Act of 2004, to establish and make operational the Data Protection Commissioner.[49]

On the other hand, The South African data protection legislation is the Protection of Personal Information Act (POPIA).[50] It is the latest data protection legislation in the world modelled on the

[49] ALT ADVISORY 'Data protection in Africa Factsheet: Mauritius' (2020) 1. https://rm.coe.int/dpa-2017-maurice/168077c5b8 (accessed 10 September 2021).
[50] ALT ADVISORY 'Data protection in Africa Factsheet : South Africa' (2020) 1 https://dataprotection.africa/wp-content/uploads/2020/08/South-Africa-Factsheet-updated-20200803.pdf (accessed 17 October 2021)

GDPR.[51] Furthermore, it is comprehensive legislation that explains clearly and broadly data protection principles and has established an independent Regulatory to ensure enforcement.[52]

1.5 Research Objectives

Generally, the main objective of the research is to analyse the general principles governing the processing of personal data in the DRC to understand the extent to which they have complied with the international and African regional human rights standards relevant to the general principles of data protection. Specifically, the research assesses the gaps in principles governing personal data in the 2020 ICT Act and the developments in the ICT Act while bringing to light its prospect to strengthen the protection of personal data in the DRC and the weaknesses therein that may require action going forward.

1.6 Scope and limitations

This research is limited in scope and by other following factors:

Firstly, it approaches the issue of data protection principles as a fundamental human right but not a commercial issue. In this regard, the research does not cover data protection issues for marketing, trade, or any other business, but a human right that every person must enjoy.

Secondly, this research does not cover any other ICTs issue. Instead, it is focused on technologies that threaten the right to privacy with the collection, and processing of raw data, including databases, computer systems, cell phones, and all internet platforms.[53]

Thirdly, this research is limited by the lack of Congolese literature on privacy and data protection. Therefore, the analysis will generally look at international standards and best practices in data protection, particularly in some African countries like Mauritius and South Africa.

1.7 Conceptual clarifications

In order to make clear the following discussion and avoid confusion, it is necessary to a description of some key concepts. Therefore, the definition of personal data, privacy and data protection, information regulation authority, the data controller, data processor, data subject, data user and a third party are successively provided.

[51] Cookietbot 'POPIA South Africa's Protection of Personal Information Act, enforcement update July 2021' available at https://www.cookiebot.com/en/popia/? (accessed 29 October 2021).
[52] As above.
[53] M Froomkin, 'The Death of Privacy?' (2000) 52(5) *Stanford Law Review* 1461, 1468.

1.7.1 Personal data

The GDPR defines personal data as any information related to a person identified or any information identifying a natural person.[54] An identifiable natural person can be recognised by numbers, location data, an online identifier, and other specific characteristics, including genetic, mental, economic, physical, physiological, and social identity.[55] Other factors such as cookie identifier, an IP address can identify an individual.[56] However, the 2020 ICT Act referred to information of natural persons 'identified or identifiable, directly or indirectly, by reference to an identification number or one or more elements specific to his physical, physiological, genetic, psychological, cultural, social or economic identity.'[57] Nevertheless, when reading the definition provided by the GDPR, it is broader. The 2020 ICT Act does not include special factors like location data, online identifiers, and mental and physiological factors. Moreover, the definition personal data as provided in the 2020 ICT Act does not cover information of juristic persons.

1.7.2 Privacy and data protection

Banisar explains that the wording privacy is broader. It can refer to the protection of relationships between persons and society or the security of relationships between persons, companies or governments.[58] According to ALT Advisor, there is interchangeability between the terms privacy and data protection.[59] Similarly, Makulilo asserts that privacy and data protection are used to describe personal information, but the location makes a difference; privacy is often used in the United States of America (USA), while data protection is frequently used in Europe.[60] In order to reconcile the two different views, the concept of data privacy was created. In this regard, Bygrave argues that it is more appropriate to use data privacy since it manages central interest at risk.[61] It further channels a link to synthesise North America and European policy discussion.[62] Similar to Byagrave's view, Karanja uses the concept of' information privacy'. For them:[63]

> the concept' information privacy' is concerned with the protection of personal data. In Europe, the term' data protection' is used to refer to 'information privacy'. Although the two concepts, information privacy and data protection, may differ somewhat in meaning and the scope of the former being wider than the

[54] Article 4 (37) of the 2020 ICT Act.
[55] As above.
[56] Information Commissioner's Office 'Guide to the General data protection regulation (GDPR)' available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/? (accessed 30 September 2021).
[57] Article 4 (37) of the 2020 ICT Act.
[58] D Banisar 'The right to information and privacy: balancing rights and managing conflicts' 2011 6 available at https://openknowledge.worldbank.org/handle/10986/23022 (accessed 30 September 2021).
[59] ALT Advisory (n3) 20.
[60] A Makulilo 'Privacy and data protection in Africa: a state of the art' International Data Privacy Law, (2021) 164.
[61] LA Bygrave, 'Privacy Protection in a Global Context: A Comparative Overview' (2004) 47
[62] As above.
[63] SK Karanja, 'Schengen Information System and Border Control Cooperation: A Transparency and Proportionality Evaluation', PhD Thesis, Faculty of Law, University of Oslo, (2006) 86, A Makulilo (n 60 above) 165.

latter (sic). Both expressions are used interchangeably to refer to the same thing protection of personal data.

1.7.3 Information regulation authority

An information regulator is an independent public body established by a state. It aims to regulate data protection in order to safeguard fundamental rights. It also protects the freedoms of the natural person related to the process and further facilitates the free flow of personal information.[64]It is the body that is usually established in specific legislation on data protection and responsible for the enforcement of the legislation.[65] It is empowered to monitor and enforce compliance with the data protection legislation by public and private bodies.

1.7.4 Data controller, data processor, data subject, data user and third party

The data controller is also called a data medium or responsible party.[66] Indeed, a data controller can be anybody such as a public authority, an agency, a legal or a natural person, entitled to determine the purposes and ways of processing personal data alone or with other bodies.[67] While a data processor can be a legal person or natural person, or an agency, public authority or any other body which aim to process personal data under the supervision and control of the data controller[68]. In the same way, Byagrave asserts that as the data controller uses the data processor on its behalf, the latter is the body that carries out the processing of personal data. [69]

On the other hand, a data subject is the owner of personal data. It is an identifiable person or a person well-identified whose processing of personal data pertains.[70] Compared with, a data user, also called the recipient, is someone who uses them for different objectives after receiving personal data from a data subject.[71] In the same angle, occasionally, a third party can also be differentiated. It is any other different party which is not a data processor or controller or subject, but it is controlled directly by the data controller or the data processor.[72]

1.8 Literature review

In the DRC, no outstanding researcher has the benefit of assessing the effectiveness or compliance of the 2020 ICT Act with the international and regional standards on the right to privacy and data protection.

---

[64] Article 51 GDPR.
[65] ALT Advisory (n 3) 3.
[66] A Roos 'The Law of data (privacy) protection: a comparative theoretical study' PhD Thesis University of South Africa, (2009) 19 available at http://hdl.handle.net/10500/1463 (accessed 16 October 2021).
[67] Article 4(7) GDPR & article 2(d) Convention 108.
[68] Article 4(7) GDPR & article 2(d) Convention 108.
[69] Bygrave Data protection law 21. In the UK Data Protection Act of 1984, a processor was called a computer bureau, Roos (n 66).
[70] As above.
[71] As above.
[72] Roos (n 66) 20.

Indeed, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), in assessing DRC's policy and legislative environment in the ICT sector, has noted that there is no clear, comprehensive and updated legislative framework governing ICT issues in general and privacy and data protection in particular.[73] Furthermore, it states that the DRC's government has been slow in adopting or updating legislation and policies on ICT in the era of technological development. However, it recognised that some provisions on privacy and data protection are spread other legislation.[74] Ultimately, CIPESA recommended the DRC's government to determine circumstances, terms, and measures applicable to control the Internet in clear policies and legislation, in accordance with internationals human rights principles and bests practices. Also, it should take appropriate measures that ensure judicial enforcement, transparency and accountability.[75] It further recommended that companies and the Civil Society raise awareness of the need to respect privacy, data protection, and other digital rights. In addition, it recommended to the civil society to campaign for the establishment of an independent and impartial data protection Regulatory.[76]

In the same vein, Gayenga asserts that the protection of personal data in the DRC remains a great challenge as there is no specific law regulating the subject matter.[77] He was further concerned in his research by demonstrating how the DRC government makes no effort in adopting data protection legislation while most African countries are adopting and updating data protection legislation and policies.[78] These legislations are modelled on European standards. They have essential principles, including lawfulness, fairness and transparency, accuracy, rectification, purpose and storage limitation.[79]

However, he mentioned that personal data protection goes hand in hand with respect to the right to privacy, which is provided and in other Congolese legislation, including the Constitution, the 2020 ICT Act, and the 1940 Criminal Act.[80] He concludes that, concerning the lack of a specific Congolese data protection law, there is an urgent need for the DRC to adopt such legislation like other African and European Countries to ensure full-fledged protection of Congolese personal data.[81] Such law should define principles governing personal data and the rights and obligations of state and private

[73] CIPESA, 'State of internet freedom, Democratic Republic of the Congo 2019, Mapping trends in Government internet controls 1999-2019' (2020) 9 available at https://cipesa.org/?wpfb_dl=408 (accessed 20 September 2021) (accessed 10 August 2021).
[74] As above.
[75] As above.
[76] As above.
[77] C GAYENGA 'la protection de la vie privée et des données personnelles sur Internet en RDC : état des lieux, cadre juridique international et de la RDC'available at https://www.lecommunicateurnumerique.net/wp-content/uploads/2021/04/ARTICLE-PROTECTION-DES-DONNEES-PERSONNELLES.pdf (accessed 20 September 2021) (accessed 10 August 2021).
[78] As above 11.
[79] As above.
[80] As above 15.
[81] As above.

organisations dealing with personal data.[82] Further, it should determine that personal data processing must satisfy the conditions set out in those principles.[83]

In the same angle, Kandolo Wa Kandolo, in his reflection on social media as the emerging of the new form of governance of human rights in the DRC, states that social media have contributed to the emergence of new democratic practices in the DRC, sometimes inacceptable by the public power.[84] They go beyond state's governance as they invest nowadays in different places of social participation, including discussion of Facebook, forums of exchange, personal and professional bogs, personal and professional profiles on Twitter, Facebook, WhatsApp, Viber, Skype, Instagram etc.[85] He argued that the development of social media has raised several issues, including data protection, privacy, copyrights, accountability of websites of social media.[86] However, he was concerned about the lack of law in the DRC, regulating social media, internet and protecting users' personal data.[87] Therefore, he recommended the adoption of new legislation and policies regulating those issues.

Ultimately, Kodjo Ndukuma asserts that the DRC Constitution enshrines the fundamental right to protect the secrecy of correspondence in any medium, including online, using telecommunications.[88] He further states that the 2020 ICT Act organise a minimum system of protection of the right to privacy and personal data of social media and services users.[89] It refers to a ministerial decree for the modalities of personal processing data while reinforcing them with specific penal provisions.[90] However, he raised the issue that Africa in general and the DRC, in particular, are big data markets for great companies including, Google, Amazon, Facebook, Apple, that need big data for their running. But we don't have fundamental rights in the matter of informational self-determination: the right to consent to the collection of personal data, the right to object to it, the right to access, modify and delete personal data.[91]

Apart from the DRC context, the issues related to personal data have captured the interest of scholars, policy, and lawmakers in many countries. Westin and Miller were the first persons to write on data protection. At the same time, in the 1960s and 1970s, the issues on the exploitation of personal data using computer systems were originally raised and documented.[92] Both of them used the approach of data protection as a right to privacy information.[93] After a short period, the way of collecting and processing personal data and the adverse effect that it had on persons have been examined in detail by

[82] As above.
[83] As above.
[84] Kandolo wa Kandolo (n 47) 338.
[85] As above.
[86] As above 373.
[87]As above 350.
[88] A Kodjo *Les droits des télécoms et du numériques : Profil africain et congolais, prospective comparée d'Europe et de France*, L'Harmatan (2019)
[89] As above.
[90] As above.
[91] As above.
[92] Alan Westin, Privacy and Freedom (Bodley Head 1970); Arthur Miller, The Assault on Privacy: Computers, Data Banks and Dossiers (UMP 1971) discussed in Bygrave 'Privacy and Data Protection in an International Perspective' *Stockholm Institute for Sacandinavian Law* (2010) 167 available at https://scandinavianlaw.se/pdf/56-8.pdf (accessed 10 August 2021).
[93] As above.

rule.[94] As a result, data protections laws and regulations were promulgated, both in the United States of America and in Europe, due to issues of personal data raised previously.[95]

Nevertheless, Makulilo pointed out that data protection privacy was largely ignored in Africa despite the increased personal data processing facilitated by Information and Communication Technologies (ICT).[96] Based on his findings, after analysing the impact of the GDPR on African countries, he asserted that the latter had influenced the adoption of data protection legislations in Africa. He further argued that the GDPR had established the standards of data protection legislation worldwide. He observed that non-European countries, especially African countries, have enacted data protection legislation on the GDPR standards to attract investment from Europe. He used Mauritius as a case study due to its recent data protection law.[97]

Moreover, Abdulrauf & Fombad assert that internet activities are being threatened by data privacy in Africa. They assess the potential impact of the AUCCPD. This Convention is examined through its provisions related to privacy and data protection to attract adoption and implementation of African states. Finally, they compared the AUCCPD and Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) as the latter is the only data protection binding instrument in international law because it provides global data protection standards.[98]

In addition, Brian has recently explored the trends of establishing privacy and data protection laws in Africa. He shows how most African countries have made a significant effort to adopt and update or amend laws and regulations to establish a larger digital trade economy.[99] He asserts that the governance and regulation of personal data across Africa have been incited by adopting the European Union GDPR as Africa and Europe are interested in preserving the free flow of personal data among them.[100] He analyses African data protection policy status considering, as the adoption of GDPR in 2016, countries that have adopted laws governing data protection and countries that have not adopted that law. He concluded that the lack of a unique policy protecting personal data would hinder setting a common market in Africa with digital services and goods.[101]

Besides, Greenleaf has demonstrated the European standards outside Europe in adopting data protection laws and policies. By examining the EU Directive and the Convention 180+, he shows how these European standards have influenced the enactment of data protection laws globally and how this

[94] James Rule, Private Lives and Public Surveillance (1973) quoted in Adam Warren, James Dearnley and Charles Oppenheim, 'Sources of Literature on Data Protection and Human Rights' (2001) 2 *Journal of Information, Law and Technology* 1, 3.
[95] As above.
[96] A Makulilo, (n 60), 176.
[97] A Makulilo (n 22) 2.
[98] Abdulrauf &Fombad (n 6).
[99] B Daigle 'Data Protection Laws in Africa: A Pan-African survey and Noted Trends' *Journal of International Commerce and Economics* (2021) 1 available at https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf (accessed 10 August 2021).
[100] As above.
[101] As above.

influence is increasing. In addition, he examined the Convention 180 and its additional protocol from their possibility and their attractiveness of becoming the international standard on data privacy. Nevertheless, the European Council has to define accession policies that are not limited to European countries for such globalisation.[102]

1.9 Research Structure

The study is made up of four chapters. Chapter one provides an introduction to this study. It includes a background to the study, statement of the problem, research question, research methodology, limitation of the study, objective of the study, conceptual clarifications, literature review and the research structure.

Chapter two examines the DRC's background and approaches to the protection of personal data. It provides the evolution development of data protection by exploring how Constitutions and legislation which have provided the right to privacy and data protection since the independence. In addition, it provides the nature and scope of data protection in the DRC by locating the right to privacy and data protection under regional and international instruments applicable to the DRC.

Chapter three examines the major principles governing personal data by giving an overview of core principles governing data protection worldwide and applying those principles under the Congolese legal frameworks. Then, meaning, scope, nature and obligations are examined and mechanisms established to ensure the effectiveness of those major principles governing personal data. Further, it compares selected African countries such as South Africa and Mauritius with comprehensive data protection legislation.

Finally, chapter four concludes by summarising the findings and providing appropriate recommendations in order to ensure the protection of privacy and personal data in the DRC.

[102] Graham Greenleaf 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' 2012 *International Data Privacy Law.*

CHAPTER 2: BACKGROUND AND APPROACHES TO THE PROTECTION OF PERSONAL DATA IN THE DEMOCRATIC REPUBLIC OF CONGO

2.1 Introduction

The previous Chapter sets out the contextual problem of the study and delineates the research plan. In order to guide the research, this Chapter presents provides background and approaches to data protection in the DRC. It starts by presenting the evolution of data protection in the Congolese framework from independence. Next, it demonstrates the deficiency of legislation in protecting personal data. Afterwards, it gives the nature and scope of data protection in the DRC by locating the right to privacy and data protection in regional and international human rights instruments applicable to the DRC. In addition, it analyses the normative content of the current Constitution and legislative protection of personal data.

2.2 The evolution of personal data protection in the DRC

The right to privacy and data protection has evolved slowly under the Congolese legal framework. From independence in 1960 to 2003, no Constitution recognised the right to privacy and data protection. This section presents the evolution of data privacy protection from the independence of the DRC until the adoption of the current 2006 Constitution.

2.2.1 The paucity of post-independence constitutions in regulating personal data

Since it acceded to independence on 30 June 1960, the DRC has had so far ten Constitutions.[103] In those ten Constitutions, only two have had some provisions on privacy, namely the transition constitution adopted on 4 April 2003 and the constitution of 18 February 2006. Hence, the Congolese Constitutions did not recognise the importance of data privacy. The transition Constitution was adopted on 4 April 2003 was the first in the history of the DRC to guarantee the right to privacy. Under Article 34, it provided that:[104]

> Every person has the right to privacy secrecy of correspondence, telecommunication or any other form of communication. This right can only be infringed upon in the cases provided for by law.

However, the Constitution did not provide the cases where the law could infringe the right to privacy, and the meaning of the law was not defined. Despite this provision, there was no constitutional provision on the protection of privacy. In 2006, the current Constitution was adopted, repealing the transitional Constitution. It also guarantees under Article 31 the right to privacy of secrecy of correspondence, telecommunication and other forms of communication. However, this right can only be limited in specific cases provided by law. Also, this Constitution does not have any specific provision

[103] M Wetsh'okonda 'les textes constitutionnels congolais annotés' (2011) 7.
[104] Article 34 of the DRC Transition Constitution

on personal data. Further, it does not provide the meaning of law and give conditions under which the right to privacy can be infringed.

2.2.2 The deficiency of legislation in protecting personal data

The DRC is among states which do not have specific legislation on data protection. According to the *Autorité de Régulation de la Poste et des Télécommunications du Congo* (ARPTC), there was an increasing number of mobiles subscribers of about 1.95% to 41.[105] Five hundred ninety-five million subscribers from 40 798 million subscribers in the fourth quarter of 2021, the penetration rate is 24.6%'.[106] This shows a significant increase in users of ICT services, but the protection of their data still raises concerns. While other African countries are trying to adopt specific legislation on data protection or update their data protection legislation, it is not the case in the DRC. The only legislation with personal data provisions is the 2020 ICT Act, which has only a few provisions on personal data.

2.2.3 Post-2000 emergence of personal data protection

The increased number of ICT users in the DRC created a need for the protection of personal data. Furthermore, there were several violations of the right to privacy, especially for some politicians from the opposition parties. For example, in 2015, three parliament members from the opposition have reported that their phone numbers were blocked for over four months.[107] Similarly, between 2015 and 2017, the government obtained personal information of mobile users from Orange, a telecommunication company, upon 385 and 981, without compliance with DRC legislation and international human rights standards.[108] These information related to details of calls, names and addresses of callers, their geo-localisation and billing information.[109] All those personal information were provided in violation of the data subject's right, as there is no specific legislation protecting the privacy and personal data.[110] The government was using abusively personal data of politicians and other persons for its interests in violation of rules governing the processing of personal data.[111]

2.3 Nature and scope of the protection of personal data in the DRC

The right to data privacy is recognised under regional and universal human rights instruments applicable to the DRC.

[105] ARPTC (n 48)
[106] As above.
[107] T Makunya 'Digital space and protection of freedom and association and peaceful assembly in Africa: Report of CIPESA on the Democratic Republic of Congo' (2021).
[108] As above.
[109] As above.
[110] As above.
[111] As above.

2.3.1 Protection of personal data in global and regional human rights instruments applicable to the DRC

The Democratic Republic of Congo (DRC) Constitution recognises that international treaties and agreements regularly ratified prevail over national laws as a monist country.[112] Therefore, the DRC's legal framework on privacy and data protection is constituted by international, regional, sub-regional and national standards. The DRC is a party to the United Nations Charter, thus a member state to the United Nations. It is also a member of the African Union (AU) on the continental level. Considering its geo-strategic position on the continental level, the DRC is also a member of some Regional Economic Communities (RECs) that have adopted privacy and data protection frameworks. This is a case of the Economic Community of Central African States (ECCAS); the Common Market for Eastern and Southern Africa (COMESA); Southern African Development Community (SADC).

2.3.2 Locating the right to privacy and data protection in human rights instruments adopted under the United Nations

At the international level, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) adopted respectively in 1948 and 1966 constitute the main normative framework on the right to privacy. In addition, other international instruments on privacy and data protection were adopted by the United Nations (UN). The UDHR was the first international human rights instrument to guarantee the right to privacy as a fundamental right in 1948. It provides that:[113]

> No one shall be subject to arbitrary interference with his right to privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks.

Eighteen years later, in 1966, the ICCPR, a binding instrument, has recognised the same right under Article 17, which provides that:[114]

> No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Makulilo highlights that the ICCPR is the human rights treaty worldwide to protect the right to privacy.[115] Similarly, Baygrave asserts that the fundamental data protection principles were highlighted in international human rights case law by the clearest interpretation of the right to privacy is provided under Article 17 of the ICCPR.[116]

---

[112] Article 215 of DRC Constitution.
[113] Article 12 UDHR.
[114] Article 17 ICCPR.
[115] Makulilo (n 22) 4.
[116] L Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', *International Journal of Law and Information Technology* 6 (1998): 247–84 available at

Furthermore, the ICCPR has established a Human Rights Committee (HRC), a body of experts with the mandate of interpreting and overseeing the rights it enshrines. The HRC, in its General Comment, has interpreted the normative content of the right to privacy as provided under Article 17 above. It indicated that the right to privacy imposes an obligation on states parties to adopt legislation and other measures or policies to give effect to this right.[117]Therefore, the DRC, as a State party to the ICCPR, must comply with the requirement of the HRC. Accordingly, it must adopt legislation and measures and policies to give effect to the right to privacy, including a data protection law. Moreover, other UN treaties such as the Convention on the Rights of the Child (CRC) adopted in 1989 have also enshrined the same right.[118]

In addition to the treaties indicated above, the HRC, with its mandate globally to strengthen the promotion and protection of human rights, has established 'Special Procedures on thematic or country-specific issues and appoints mandate holders to these positions'.[119] Under the HRC, the normative content of the right to privacy has been developed by the Special Rapporteur on to privacy and the Special rapporteur on the promotion and protection of the right to freedom of opinion and expression. Therefore, the DRC, as a State party to the ICCPR, must comply with the requirements of the HRC.

2.3.3 Locating the right to privacy and data protection in human rights instruments adopted under the African Union

The African regional system for promoting and protecting human rights is set up in the AU Constitutive Act and other instruments.[120] This regional system sets out to reach first the objectives of human rights and subsequently to use human rights-based means and principles to accomplish human rights objectives.[121] On the continental level, the ACHPR is the principal treaty that guarantees peoples' fundamental human rights. However, the ACHPR, unlike other regional human rights instruments, contains no provision of the right to privacy explicitly. According to some commentators in this arena, the right to privacy may be implicit from other provisions of the Charter, particularly those related to human dignity, freedom from all forms of degradation and exploitation, as well as torture.[122]

Notwithstanding, the right to privacy is not guaranteed explicitly in the ACHPR, the African Commission on Human and Peoples' Rights (African Commission) has adopted the Declaration of principles on freedom of expression in Africa (Declaration) to complement the rights to freedom of expression as provided in Article 9 of the ACHPR. Even though it is not a binding instrument, this declaration provides the right to access his data, correct and update his personal data. In addition, the

https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf (access 18 September 2021).

[117] General Comment No 16 on the right to privacy.

[118] Article 16 CRC

[119] A Singh, 'The right to privacy in the digital age in Africa: Module 2 overview of the legal framework on privacy' Centre for Human Rights MOOC 2021 3.

[120] F Viljoen, *Internatinal Human Rights Law in Africa* (2012) 152.

[121] As above.

[122] K Yilma & A Birhanu, 'Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices', *Journal of Ethiopian Law* 26, 1 (2013): 106

Declaration under Part IV related to access to information on the internet and freedom of expression sets key principles on the protection of data privacy.[123] These principles include non-interference, internet intermediaries, internet access, privacy and data protection. Additionally, the right to privacy and data protection is explicitly guaranteed under the Principle 40 of the Declaration.[124]

In addition, on 4 November 2016, the African Commission has adopted a Resolution on privacy on the Internet in Africa. In this resolution, the Africa Commission declared that the online right to privacy is significant to realise the right to freedom of expression. [125] Further, it is crucial to realise other rights such as the right to peacefully assembly, freedom of expression, and freedom of opinion.[126]

Significantly, for the first time, the African Commission in this landmark Resolution has made a normative link between the right to privacy online and the right to privacy offline. Additionally, the African Commission made the connection between the right to privacy and the realisation of other rights, including the right to freedom of expression and the right to freedom of association. Besides, the African Charter on the Rights and Welfare of the Child (ACRWC) guarantees also, on the continental level, the right to privacy of children against unlawful or arbitrary interference.[127]

Most importantly, the AUCCSPD on the continental level is the only human rights treaty on data protection, which bind Sates outside of Europe.[128] This Convention is also called the 'Malabo Convention' because it was adopted on 27 June 2014 in Malabo (Equatorial Guinea). However, it has not yet come into force because of the lack of fifteen ratifications required. So far, only fourteen African countries out to fifty-five have signed the Convention, but five countries, namely Guinea, Senegal, Mauritius, Namibia and Rwanda, have ratified the treaty.[129] The Convention combines in one document three diverse subjects, unlike other regional treaties on privacy and data protection, including electronic transactions, data protection and cybersecurity. Moreover, the Convention constitutes the AU key human rights instrument in the digital age, considering the importance of data protection.[130] For these reasons, Greenleaf and Georges have declared that the enactment of the Convention was a significant step to the protection of personal data at the continental level.[131]

Concerning data privacy, it has enshrined its Chapter two on personal data protection, which obliges State members, including the DRC, to establish a legal framework that guarantees the right to

[123] Part IV of the African Declaration.
[124] Principle 49 African Declaration.
[125] Resolution 362 on the right to freedom of information and expression on the internet in Africa ACHRP/Res. 362 (LIX) 2016 available at https://www.achpr.org/sessions/resolutions?id=374 (access 18 September 2021).
[126] As above.
[127] Article 10 of the African Charter on the Rights and Welfare of the Child

[128] Makulilo (n 22) 5.
[129] African Union, List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection 2014, https://au.int/sites/DATA%20PROTECTION.pdf (accessed 18 September 2021).
[130] Abdurauf & Fombad (n 6) 8.
[131] G Greenleaf & M Georges 'The African Union's data protection Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws & Business International Report* 18-21.

data privacy particularly.[132] In addition, the AU has adopted the personal data protection guideline for Africa to implement the Malabo Convention with recommended actions for stakeholders.[133]

2.3.4 The normative content of privacy and data protection under the Constitution

When independence constitutions were being drafted in Africa, recognising the right to data protection as a subcategory of the right to privacy did not exist.[134] Hence, only a few African Constitutions such as Cape Verde[135], Mozambique[136] and Algeria[137] have incorporated data protection provisions in their Bill of rights separate from provisions related to privacy. All African Constitution's guarantee the right to privacy except Somalia.[138]

In most African constitutions, there is a provision on 'the right to privacy which is interpreted to give effect to data protection as a constitutional right'.[139] The DRC is among African states, like Malawi, whose Constitution guarantees the right to privacy with other various forms of communication prohibited from the State, including all forms of telecommunication.[140] Other African constitutions on the right to privacy simply protect 'privacy of correspondence' or communication or the 'secrecy of correspondence'[141] or 'telegraphic communication' or 'postal letters and communications made by means of telephones, telecommunication and electronic devices'.[142]

The DRC Constitution adopted on 18 February 2006 and revised on 11 January 2011 has consecrated in Title II on Human rights, fundamental freedoms and duties of citizen and State, the right to privacy. The provisions of the Constitution have a superior value than any other provisions of laws or case-law. Under the constitutional principle, every legislation must comply with this Constitution. It 'captures aspects of the right to privacy and ensures the prevention of unnecessary surveillance measures through telecommunications and other means of communication'.[143]

---

[132] Article 8 (1) Malabo Convention
[133] AU 'Personal data protection guidelines for Africa' available at https://www.internetsociety.org/wp content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed 18 September 2021).
[134] A Singh (n 119) 9.
[135] Article 45 of Cape Verde Constitution, available at THE CONSTITUTION OF THE EPUBLIC OF CABO VDE (into-sa.com) (accessed 4 October 2021).
[136] Article 71 of Mozambique Constitution, available at MZ004 : Other, Constitution, 1990, (2004) (parliament.am) (accessed 4 October 2021).
[137] Article 47 of Algeria Constitution available at (anonymous) (constituteproject.org) (accessed 4 October 2021).
[138] A Singh (n 119) 9.
[139] As above.
[140] Such as Guinea, Eritrea, Equatorial Guinea, Kenya, South Africa, South Sudan, Swaziland, Tanzania, Uganda, Tunisia and Zilbabwe.
[141] Such as Benin, Djibouti, Mali and Togo.
[142] Constitution on Ethiopia.
[143] T Makunya (n 107) 9.

This is the second time in the DRC the Constitution provision protects rights related to privacy and confidentiality of correspondence. For the first time, in DRC's framework, it appeared through the interim 2003 Constitution as indicated previously.[144] Article 31 states that:[145]

> All persons have the right to respect their private life and to the secrecy of their correspondence, of telecommunications, and any other form of communication. This right may only be infringed in the cases specified by the law.

The DRC's Constitution guarantees this right to all persons, like the Algerian Constitution.[146] The wordings 'all persons' means that every person, national or foreigner under Congolese jurisdiction, are guaranteed this right. It can only be infringed in some specific cases determined by law.

However, the DRC's Constitution does not determine the meaning of 'law' in which specific cases can violate the right to privacy. Therefore, it can be assumed that the law that the Constitution refers to includes laws of general application voted by parliament or decisions of administrative authorities.[147] They must be subject to their consistency with international human rights standards and the value and spirit underlying principles of 'democracy' and 'rule of law'.[148] Some commentators like Justine Limpitlaw argue that limiting the right to privacy, as provided under Article 31 of the Constitution, is to deny the enjoyment of this right.[149] She supports that this right is empty because the law limiting the right to privacy must be enacted after the Constitution comes into force.[150]

Furthermore, the protection of privacy under article 31 of the DRC Constitution is broader. It covers the protection of privacy as well as confidentially of correspondence through whichever means of telecommunication, unlike the Algeria Constitution, which protects only the confidentiality of correspondence and forms of private communications[151]. Similarly, the Cape Verde Constitution's privacy provision also covers the secrecy of correspondence and telecommunications.[152] It can only be limited 'by a judicial decision rendered under the terms of the law of criminal proceedings, interference, by public authorities'.[153] According to the 2020 ICT Act, telecommunication is 'a set of techniques used to process, transmit, and exchange information'.[154] Therefore, the protection of privacy under the DRC Constitution is wide in scope. In addition, Article 31 on privacy is connected with other constitutional

---

[144] Article 37 of the 2003 DRC Interim Constitution; Wetsh'Okonda, Marcel, *Les textes constitutionnels congolais annotés* (Campagne pour les Droits de l'Homme au Congo, 2011) 377. T Makunya (n 107).
[145] Article 31 DRC Constitution
[146] Article 47 (1) (2) of Algeria Constitution
[147] T Makunya (n 107) 9.
[148] As above.
[149] J Limpitlaw 'Manuel des droits des medias en Afrique australe, la République Démocratique du Congo' (2020) 15 available at https://www.kas.de/documents/285576/11521648/MLHSA+2021+Version+Fran%C3%A7aise+-+RDC+.pdf (accessed 6 October 2021).
[150] As above.
[151] Article 47 (2) Algeria Constitution.
[152] Article 44 Cape Verde Constitution.
[153] As above.
[154] Article 4 (93) of the 2020 ICT Act.

provisions that protect fundamental rights and without which the exercise of privacy and confidentiality of correspondence may seem unreal.

Foremost of these rights and principles are dignity and equality.[155] Therefore, the denial of one's own privacy and the failure to protect their personal data can be a violation of 'dignity' to its core, a rejection of their self-worth and self-esteem,[156] their ability to harmoniously live in the society according to their proper belief and participate in the democratic project.[157] Moreover, Article 31 of the DRC Constitution is connected to Article 14 on the obligation to combat discrimination against women; article 22 on freedom of thought, conscious and religion, Article 23 on freedom of expression; article 24 related to the right to information, Article 25 on freedom of assembly and Article 29 on the inviolability of domicile. The link between the DRC Constitution and international human rights treaties such as Article 17 of the ICCPR ratified by the DRC also increases the protection of the right to privacy.[158]

2.4 Legislative protection

Before the adoption of this Act on 25 November 2020, the protection of privacy, personal data and protection against unlawful surveillance were regulated under Act 013/2002 of 16 October 2002 on Telecommunications and Act 14/2002 of 16 October 2002, creating the ARPTC. Different actors have criticised these Acts as outdated, pro-security, and not considering the ICT sector developments.[159] They focused mainly on the telecommunications sector and could not cover cybersecurity and privacy, and data protection issues as required.[160] However, due to the failure of the two Acts to take into account the technological progress on rights accrued to individuals in the digital era and new technological infrastructures, they made them subject to criticism. In order to improve the protection of the right to privacy of personal data, to ensure the confidentiality of correspondence and to minimise the likelihood of unaccountable surveillance, the Congolese parliament enacted the ICT Act on 25 November 2020 to address the issues of privacy and data protection.

This Act guarantees to every person the secrecy of correspondence transmitted by means of telecommunication and ICTs. It defines confidentiality as 'maintaining the secrecy of information and transactions in order to prevent the unauthorised disclosure of information to non-recipients allowing the reading, listening, illicit copying of intentional or accidental origin during their storage, processing or transfer subject to public safety'.[161] This right can be derogated only on the public prosecutor's request or by the courts' permission in terms of legal investigation.[162] It means that there is no other situation

[155] Laurie Ackermann, *Human Dignity: Lodestar for Equality in South Africa* (2012). T Makunya (n 107) 10.
[156] *South African Police Service v Solidarity obo Barnard* [2014] (SACC) CCT 01/14, 35 para 173. T Makunya (n 107).
[157] Serges Djoyou Kamga, 'Cultural Values as a Source of Law: Emerging Trends of Ubuntu Jurisprudence in South Africa' (2018) 18 *African Human Rights Law Journal* 625. T Makunya (n 107) 10.
[158] T Makunya (n 107) 10.
[159] CIPESA, 'State of internet freedom, Democratic Republic of the Congo 2019, Mapping trends in Government internet controls 1999-2019' (2020) 9 available at https://cipesa.org/?wpfb_dl=408 (accessed 20 September 2021).
[160] As above.
[161] Article 4 (16) of the 2020 ICT Act.
[162] Article 126 of the 2020 ICT Act.

where this right can be derogated except in both cases as provided. This Act has a broader definition of personal data than the Mauritius Data protection law, which defines 'personal data' as 'any information relating to a data subject'.[163] The 2020 ICT Act does not refer to a data subject in defining personal data. It covers all information on a person well-identified or a person who can be identified by ID number or other specific factors, including social, economic, physiological, physical or genetic.[164]

Nevertheless, the South African POPIA Act has the broadest definition. It includes 'biometric information, any identifying number, symbol, e-mail address, personal opinions, views or preferences, information on their education, medical, financial, criminal or employment history.[165] Besides, the 2020 ICT Act defines the processing of personal data as : [166]

> any operation or set of operations carried out by means of automated or non-automated processes and applied to data, such as collecting, processing, recording, organising, storing, adapting, modifying, retrieving, saving, copying, consulting, using, communicating by transmission, disseminating or otherwise making available, matching or interconnecting, as well as blocking, encrypting, making effective or destroying personal data.

This definition is broader as well as defined in the Mauritius Data Protection Act (DPA)[167] and South Africa Protection of Personal Information Act (POPIA Act)[168]

Furthermore, the 2020 ICT Act guarantees and protects the confidentiality of personal data and obliges any process of personal data by the prior consent of the data subject or by the public prosecutor's request. Article 131 provides that: [169]

> the confidentiality of personal data is guaranteed and protected by law. The processing of personal data is carried out only with the consent of the person concerned or at the public prosecutor's request.

Significantly, it requires the prior authorisation of the data subject to collect, record, store, or transmit personal data, except for the competent public authority.[170] However, it does not explicitly state who is a competent public authority. Instead, it refers to Article 126, where the public prosecutor or Courts can infringe the secrecy of correspondence when dealing with judicial cases. Conversely, under the same article, the State's competent public services can also derogate to personal data subject's rights, but the Act does not define those State's public services. Therefore, this can lead to the violation of data subject's rights, where any public authority can claim to be competent to process personal data of any person.

---

[163] Part I (2) of the 2017 Mauritius Data Protection Act available at https://rm.coe.int/dpa-2017-maurice/168077c5b8 (accessed 6 October 2021).
[164] Article 4 (37) of the 2020 ICT Act.
[165] Chapter 1 (10) of the 2013 POPIA Act.
[166] Article 4 (95) of the 2020 ICT Act.
[167]The 2017 DPA Part I (2).
[168] Chapter 1 (30) of the 2013 POPIA Act.
[169] Article 131 of the 2020 ICT Act.
[170] Article 132 (1) of the 2020 ICT Act.

Moreover, the 2020 ICT Act prohibits the processing of personal data related to sexual life and those on racial origin, political opinions, religious or philosophical beliefs, and those on health conditions of individuals.[171] But there is no reason provided under the Act that justifies the prohibition of these kinds of data, and there is no exception to this provision. By contrast, the South African POPIA Act classifies those data as 'special personal information' and establishes some conditions for processing.[172] The same distinction of specific data is made in the Mauritius Data Protection Act under section 29, named 'special categories of personal data' where their processing conditions are provided.[173]

On the other note, under article 190 of the 2020 ICT Act, the processing of personal data without prior authorisation is punishable up to 100 000 000 Congolese Francs and imprisonment for the author. Apart from protecting personal data, privacy, the confidentiality of correspondence, prohibition of unlawful interceptions are equally provided for under the Act.[174] In addition, the Act prohibits, but unfortunately without providing any sanction, 'the interception, eavesdropping, recording, transcription and disclosure of correspondence sent by means of telecommunications and information communication, without the prior authorisation of the Court of Cassation Prosecutor's office'.[175]

By contrast, the Mauritius Data Protection Act establishes offences and penalties related to personal data, such as the unlawful disclosure of personal data. However, it states other violations for which no specific penalty is provided.[176] In the same vein, the South African POPIA Act is broader. It has devoted its Chapter 11 to offences, penalties and administrative fines related to personal data.

It should be noted that, despite the lack of provisions on offences and penalties in the Congolese 2020 ICT Act on privacy and data protection, some legislations cover several criminal offences on the right to privacy. This is the case of the Congolese criminal Act of 1940 that punishes the violation of the secrecy of letters. Under Article 71, every person who opens or deletes letters, postal cards are punished by paying a fine and imprisonment. In addition, the Criminal Act punishes imprisonment and payment of fines to every person who will reveal the existence or the content of a letter of postcards.[177]

Apart from the Criminal Act, Act No. 18-019 on payments and securities settlement systems deals with privacy and data protection issues as it devotes under Chapter II of Title VII specific offences and penalties for breaches of payment or automated data processing systems. It punishes for payment of fines, the lack of implementation of security measures on privacy.[178]

[171] Article 132 (2) of the 2020 ICT Act.
[172] Chapter 3 Part C of the 2013 POPIA Act.
[173] Section 29 of the 2017 DP Act.
[174] Article 127 of the 2020 ICT Act.
[175] Article 127 (2) of the 2020 ICT Act.
[176] Part VIII of the 2017 DP Act.
[177] Article 72 Criminal Act.
[178] Articles 117 to 119 of the Act on payment and securities settlement systems.

Finally, article 133 of the ICT Act states that a Minister's decree on the proposition of the Regulatory Authority should determine the conditions and modalities of the collection, recording, processing, storage and transmission of personal data. But unfortunately, until now, the minister has not yet taken this decree establishing those conditions and modalities.

2.5 Conclusion

This Chapter analysed the international and African regional standards on personal data applicable to the DRC. It showed the deficiency of protecting the right to privacy and personal data under the Congolese legal framework. Furthermore, it provided the nature and scope of the DRC's data protection legislation. It located international and regional human rights instruments applicable to the DRC. In addition, it explored the normative content of data protection under the DRC Constitution and the 2020 ICT Act. As a result, the DRC Constitution does not explicitly guarantee the right to personal data, like the Algerian, Mozambique and Cape Verde Constitutions.

Moreover, the 2020 ICT Act has devoted mainly only three articles on personal data protection, which are not broader, unlike the 2017 DPA and the POPIA, the comprehensive legislation with more provisions on issues related to data protection. As a result, there are several issues that the 2020 ICT Act does not cover, such as the establishment of a Data Protection Office with Commissioners, the transfer of personal data outside of the DRC or the trans-border information flows, the rights of data subjects, obligations of controllers and processors. As a result, Congolese data remain unprotected because of the lack of specific comprehensive legislation.

CHAPTER 3 MAJOR PRINCIPLES GOVERNING PERSONAL DATA PROTECTION

3.1 Introduction

The previous Chapter provided the DRC's background and approaches to personal data protection. However, it demonstrated the lack of specific comprehensive data protection legislation. This Chapter examines the major data protection processing principles and compares principles provided under the 2020 ICT Act with international standards and practices in African countries, including Mauritius and South Africa. In addition, it determines the weaknesses of the 2020 ICT Act with regard to the international standards and best practices.

3.2 Overview of international principles governing personal data protection

The overview states the principles that can be identified in all successful data protection legislation within one form or another. This section provides the importance of those principles and the exceptions and exemptions applicable to the principles.

3.2.1 Nature and types of principles

As scholars have noted, certain basic data protection principles have become more or less universal despite diversities in language, culture, social values and legal traditions.[179] These principles are fair and lawful processing, purpose specification, minimality, openness or transparency, data subject participation, sensitivity, security and confidentiality, and accountability.[180] They can be found in any data protection legislation, in one form or another.[181] For example, these principles are provided in Article 5 of the GDPR; Chapter II of the Convention 108; Part 2 of the OECD Guidelines; the Guidelines for the regulation of computerised personal data files; article 13 AU Convention and Principle 42 (2) of the African Declaration. However, not all legislations have the whole principles or have the same wordings.[182] Then again, rigid distinctions can be made between the principles. As a result, some of them overlap to some extent.[183]

[179]Bennett Regulating privacy: data protection and public policy in Europe and the United States (1992) 23; Blume 'An EEC policy for data protection' 1992 Computer/Law Journal 399; Bygrave Data protection law: approaching its rationale, logic and limit (2002) at 125 et seq; Flaherty Protecting privacy in surveillance societies-the Federal Republic of Germany, Sweden, France, Canada, and the United States (1989) xiii; Hondius Emerging data protection in Europe (1975) 2; Trubow 'The European harmonization of data protection laws threatens US participation in trans-border data flow' 1992 North-western Journal of International Law and Business 159 161; Neethling et al & Visser Neethling's law of personality (2005), A Roos 'Core prinicples f data protection law' (2006) 107*Journal of Souther Africa*, available at https://www.jstor.org/stable/23253014?seq=1#metadata_info_tab_contents (accessed 1 October 2021).

[180] Roos (n 179) 107.

[181] As above.

[182] Roos (n 66) 481.

[183] As above.

Fair and lawful processing

According to this principle, 'personal data shall be processed lawfully, fairly, and transparently concerning the data subject'.[184] Abdulrauf and Fombad argue that this principle is important in all data protection instruments around other principles.[185]In the same way, Bygrave argues that this principle 'denote[s] the pith and basic of a set of legal rules'.[186]

Concerning this principle, the processing of personal data must be done following the law. In other words, it is not authorised to process personal data without complying with the law. Furthermore, Bygrave affirms that the principle of fair and lawful processing of personal data is fundamental because it affects other core principles of data protection laws.[187] It means that the application of all data processing principles will lead to fairness and lawfully.[188] Moreover, Roos submit that the insurance lawful processing of personal data is the ultimate aim of any data protection law.[189]

Under article 6(1), the GDPR provides conditions and the extent that should apply for the lawful processing of personal data. Therefore, to be considered as lawful processing of personal data, one of the following conditions must be applicable:[190]

> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

With regard to the above conditions, Roos argues that they can be resumed as the conservation and continuance of interests, either public or private.[191]

[184] Article 5 (1) (a) GDPR
[185] Abdurauf & Fombad (n 6) 10.
[186] LA Bygrave *Data protection law: Approaching its rational, logic and limits* (MIT Press, 2002) 57, (n4).
[187] Bygrave Data protection law: approaching its rationale, logic and limit (2002) 58, Roos (n 66) 111.
[188] As above.
[189] Roos (n 66) 22.
[190] Article 6 (1) GDPR.
[191] Roos (n 179) 110.

Purpose specification

This principle is also called 'finality' principle or concept.[192] Under Article 5(1)(b), the GDPR provides that: [193]

> Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

With regard to this principle, personal data must only be processed for a purpose that is specified. It means that the collection, use, and disclosure of personal data must be specified and must comply with the purpose of data processing.[194] However, some data protection instruments, such as the AUCSSPD, provide that the data processing purposes must be 'lawful' whilst others, like the GDPR and the Convention 108, use the concept 'legitimate'.[195] In this regard, Bygrave affirms that the concept 'legitimacy' refers to the social acceptability of processing personal data as social norms must be considered.[196] Furthermore, Bennett highlights that the purpose specification principle is the cornerstone of data protection provision, around which, turn other principles.[197]

Moreover, Byragve adds that three principles should be gathered with the purpose specification principle:[198]

- The purpose(s) for which data are processed must be specified or defined;
- The purpose(s) for which data are processed must be determined at the time collection, and must be made known to the data subject at that time.;
- The purpose(s) for which data are processed must be lawful. This principle follows from the first data protection principle that personal data must processed fairly and lawfully. Data processing cannot be done lawfully if it does not serve a lawful purpose;
- the purpose(s) for which the data are further processed may not be incompatible with the purposes for which the data were first collected.

In the same vein, Roos confirms that, the lawful processing of personal data ensures the application of the purpose processing principle as it justifies why data are processed. In addition, the application of this principle provides a close definition of the limits of this ground of justification.[199]

[192] Bennett (n 179) 4, Roos (n 179) 111.
[193] Article 5(1)(b) GDPR.
[194] Roos (n 179) 111.
[195] As above.
[196] Bygrave (n 179) 61.
[197] Bennett (n 179) 4.
[198] Bygrave (n 179) 61.
[199] Roos (n 179) 113.

Minimality

The minimality principle also called 'data minimisation', is provided under article 5(1)(c) of the GDPR, which states that: 'personal data shall be adequate, relevant and limited to what is necessary concerning the purposes for which they are processed'.[200]

In line with this principle, personal data collected must only be restricted to the requirement or purpose they were collected.[201] This principle also implies that data should be erased or expressed anonymously when they no longer serve or the purpose for which they were collected.[202] Thus, the principle of minimality of data protection intends to ensure that personal data collected for a specific objective are satisfactory or suitable for their purpose but not beyond the reason of the collection.[203]

Quality

This principle is also called the 'accuracy principle'. Article 5(1)(d) of the GDPR provides that :[204]

> Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

In conformity with this principle, personal data must be accurate, relevant, and keep updated considering their purpose.[205] It means that, in order to comply with the data processing quality principle, the data controller, namely the body or organisation entitled to determine the data purpose, must make sure that the data are relevant, accurate and up to date.[206]

In this regard, personal data are relevant when they relate to the purpose for which they are processed and the purpose they have to be used.[207] Furthermore, they are accurate when they are correct or do not mislead as to any matter of fact.[208] Moreover, they are up to date when they give updated information for which they were processed.[209]

Nevertheless, when they are no longer up to date, they are considered 'obsolete' and need to be erased by the data controller. In the same way, Neethling mentions that the purpose of collecting

[200] 5(1)(c) GDPR.
[201] Article 5 (c) Convention 108.
[202] Article 5 (e) Convention 108.
[203] Roos (n 179) 113.
[204] Article 5(1) (d) GDPR.
[205] As above 114.
[206] Roos (n 179) 115.
[207] As above.
[208] As above.
[209] As above 116.

personal data is infringing when data are not relevant or updated.[210] Consequently, the processing of that kind of data is not reasonable.[211] Additionally, the OECD Guidelines explain that the obligations of relevance, accuracy and update are the fundamental characteristics of the quality principle, and they have to be connected to the objective of data processing.[212] Their requirements must not be broader than their purposes.[213]

Openness or transparency

This principle requires that personal data have a general rule of openness related to best practices, developments, and policies.[214] With regard to the OECD Guidelines, the principle of openness can respect different ways such as consistent information from data controllers to data subjects, publication of information on activities related to the data processing; data controllers must register public bodies.[215]

Data subject participation

In line with this principle, persons with whom data relate must be implicated in processing their data and have more control over them than other individuals or organisations.[216] In other words, data subjects have to be legally entitled to control their data records directly.[217] Furthermore, this principle involves some aspects including, the right for data subjects to have access to their personal data at reasonable intervals and without delay or expense; the right to request rectification, erasure or blocking of incomplete, inaccurate personal data; the right to object to the processing of their personal data; the right to object to the processing of personal data for direct marketing purposes.[218]

Sensitivity

According to this principle, 'the processing of certain types of data which are regarded as especially sensitive for data subjects, should be subject to more stringent controls than other personal data'.[219] However, the group of experts drafting the OECD Guidelines found it was not possible to define a universal criterion of sensitive data.[220] Furthermore, there were two opposing views, one supporting the enumeration of sensitive data and another supporting that they could not be enumerated.[221] Finally, the Group of Experts concluded that it was impossible to determine universal sensitive data criteria. As a result, they only recommended general standards limited to personal data collection.[222]

[210] Neethling (n 179) 121.
[211] As above.
[212] OECD Guidelines Explanatory Memorandum (1981).
[213] As above
[214] As above para 12.
[215] As above
[216] Article 8 Convention 108
[217] Neethling (n 179) 152.
[218] Article 8 (d) Convention 108
[219] Article 6 Convention 108
[220] Roos (n 179) 112.
[221] As above.
[222] OECD Guidelines (n 212) 29.

With regard to the Convention 108+:[223]

> personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, or relating to criminal convictions, may not be processed automatically unless the domestic law provides appropriate safeguards.

On the other side, the GDPR list a category of personal data considered to have a sensitive nature and consequently profit bit the processing of this kind of data unless there is a reason or a circumstance that justifies processing them.

According to article 9 (1) under the title 'Processing of special categories of personal date':[224]

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited

In addition, concerning the processing of personal data on criminal records, the GDPR makes a special obligation to process this kind of data. It provides that an official authority must control the processing of all personal data related to convictions, criminal offences and security measures.[225] However, national legislation may derogate this rule with appropriate and specific security measures.[226]

Security and confidentiality

In line with the OECD Guidelines, personal data have to be protected by suitable measures against any risk such as access without authorisation, the use, destruction, modification or divulgation of personal data beyond their purpose.[227] In the same vein, the GDPR under Article 5(1)(f) provides that: [228]

> Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Indeed, this principle obliges that data controllers ensure that security measures are put in place to guarantee personal data protection.[229] Those security measures can be physical, for example, identifications cards, locked doors; they can be organisational like the use of access codes for a category of person; they can also be informational, for example, the inclusion of enciphering or monitoring of unusual activities.[230]

---

[223] Article 6 Convention 108.
[224] Article 9 (1) GDPR
[225] Article 10 GDPR
[226] As above.
[227] OECD Guidelines para 11.
[228] Article 5(1)(f) GDPR.
[229] Roos (n 179) 125.
[230] As above.

With regard to the security of the processing of personal data, Roos points out that the responsible party of data processing has an obligation of implementing all adequate measures that ensure the security of data against all the forms of unlawful processing, such as the access without autorotation, the modification, loss or destruction of data. [231] Moreover, considering the confidentiality of personal data, she emphasises that the State must authorise the processing of data by the data processor or any legislation or policy to justify the confidentiality of data processing. [232]

Accountability

According to this principle, the data controller must be responsible for any other measures or principles of processing personal data. [233] In this regard, the OECD Guidelines state that: [234]

> given that the data processing activities are carried out for the benefit of the data controllers, the controllers should be accountable under domestic law for complying with privacy protection rules and should not be relieved of this accountability merely because data processors are carrying out the data processing activities on their behalf.

In addition, Roos asserts that the principle of accountability should be included in any data protection law in order to make strong et effective the obligations imposed by law.[235]

3.2.2. Importance of the principles

The principles governing the processing of personal data are important for these reasons: firstly, they are located at the heart of any data protection legislation, which must comply with them to ensure adequate protection. secondly, as they are placed at the beginning of the data protection legislation, they influence the following provisions to comply with the essence of the principles and build a solid block for data procedures.[236] Thirdly, they make the new purposes of data easier, such as security measures and restrictions, which are an obligation for data processing.[237]

In other words, all data processing principles aim to prevent the data subject from abuses created by new information and communication technologies. Nevertheless, in the same sense, they remain significant.[238] Therefore, these principles are important and must be included in any data protection law to ensure adequate protection of personal data.

---

[231] Roos (n 179) 125.
[232] As above.
[233] Article 5(2) of the GDPR.
[234] OECD Guidelines (n 212) 32.
[235] Roos (n 179) 127.
[236] Cloudian 'Data protection guides' available at https://cloudian.com/guides/data-protection/data-protection-regulations/ (accessed 15 October 2021)
[237] D Korff & M Georges 'The DPO Handbook: Guidance for data protection offices in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation' (2019) 16.
[238]As above.

3.2.3 Exceptions and exemptions of the principles

Principles governing personal data have exceptions or exemptions, which are usually provided for by data protection laws. However, these exceptions or exemptions may be totally or partially from data protection law. Generally, exceptions and exemptions to data processing principles may cover two circumstances, including when there are relatively small risks on the interests of data subjects and when the interests of others derogate the interests of data subjects in privacy.[239]

Minimal risk

There is a minimal risk when the processing of personal data relates to some activities which are exclusively important for home use or personal use.[240] Considering that their risk is very small, they can be relieved from the space of data protection legislation.[241] For example, this is the case of a notebook of addresses of friends and their telephone numbers kept at home for use, which should not need to be regulated by data protection legislation.[242] In the same vein, when data are exclusively processed for a scientific research purpose or for a short period necessary for the unique purpose of establishing statistics, there is obviously no risk of violating the privacy of data subject, the data subject's right to access to his personal data can be restricted.[243]

Overriding interests

The restriction of data protection principles may occur in protecting the data subject's interests or protecting the interests of others or safeguarding specific public interests.[244] Indeed, data subjects' interests can be protected by denying them access to personal data. This could be the case, for example, where sensitive data subject's health can affect him negatively.'[245] The other interests may be the case when data subject information are linked to third-party information. Therefore, the data subject may be denied access to his information in order to protect others.[246] Finally, public interests may justify the restriction of data protection principles when provisions make partial or total limitations necessary.[247]

3.3 Principles governing personal data protection under Congolese legislative frameworks

3.3.1 Meaning, nature and scope

The previous section provided principles that can be found in any data protection legislation. This section will provide data processing principle under the 2020 ICT Act.

[239] As above.
[240] As above.
[241] Roos (n 179) 128.
[242] As above.
[243] As above .
[244] Article 49 GDPR
[245] Roos (n179) 128.
[246] As above
[247] As above

As stated previously, there is no specific data protection legislation in the DRC. However, certain principles governing personal data can be found in the 2020 ICT Act, including the principle of consent, confidentiality, and sensitivity.

Principle of the consent of data subject

This principle is provided under Article 131(2), which states that any processing of personal data must be done only with the consent of data subject or with the requisition of a public minister officer. But, the Act does not define the consent of data subject, unlike the GDPR or the AU Convention. The GDPR defines the consent of data subject as: [248]

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The AU Convention does not use the same wordings, consent of data subject means: [249]

> any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing.

Nevertheless, the consent is of the conditions of the principles of lawful processing of personal data in the GDPR.[250] Neither the GDPR nor the Convention 108+ makes a specific principle of data subject consent. Conversely, the AU Convention states a particular principle of consent under principles governing the processing of personal data. It makes a difference between the principle of consent of personal data and the lawfulness of personal data.[251] Abdulrauf & Fombad argue that this definition obliges AU member States to provide for a regime of acceptance of consent rather than its exclusion.[252] In addition, they assert that this is in accordance with current data protection regulations' best practice[253]

Furthermore, the 2020 ICT Act does not state the conditions applicable to the consent and the consent form. Ultimately, in contrast to the GDPR, the 2020 ICT Act does not provide for a child's consent data processing. The GDPR provides that the child's consent is required when they have the age of 16 years.[254] When the child's age is under 16, consent must be given by a person who has parental responsibility over the child.[255]

[248] Article 4 (11) GDPR
[249] Article 1 AU Convention.
[250] Article 6 (1) (a) GDPR
[251] Article 13 AU Convention
[252] Abdurauf & Fombad (n6) 13.
[253] As above.
[254] Article 8 (1) GDPR.
[255] As above.

Principle of confidentiality

This principle is guaranteed under Article 131 (1) of the 2020 ICT Act, which provides that 'the confidentiality of personal data is guaranteed and protected by the present Act.'[256] The 2020 ICT Act defines confidentiality as 'maintaining the secrecy of information and transactions to prevent the unauthorised disclosure of information to non-recipients, allowing it to be read, listened to or copied unlawfully, whether intentionally or accidentally, during its storage, processing or transfer, subject to public safety.'[257] This definition is broader as the 2020 ICT Act covers most telecommunications and technology of information and communication than personal data.

Furthermore, the 2020 ICT Act does not combine the principle of confidentiality with the principle of security like the AU Convention. As a result, the security of personal data is not guaranteed under the 2020 ICT Act because this principle imposes the data controller to undertake security measures to protect data privacy.[258] Under article 13, principle 6, the AU Convention obliges States member to undertake appropriate measures that ensure security and confidentiality when the processing of personal data go beyond their jurisdiction.[259]

On the other hand, the GDPR combines the principle of confidentiality with the principle of the integrity of processing personal data. It provides that personal data shall be processed to ensure suitable security measures such as protection from destruction, unlawful and unauthorised processing.[260] In the same way, the Convention 108, use the wording 'data security.'[261] It makes an obligation on States parties to take appropriate measures that require data controllers to protect security measures ensuring the protection of personal information from unauthorised access, accidental access, use, divulgation, destruction, loss of personal data.[262] With regard to the principle of confidentiality and security of data processing, Abdulrauf and Fombad submit that the Convention 108 provides more explanation than the AU Convention.[263]

Principle of sensitivity

This principle is guaranteed under Article 132 (2) of the 2020 ICT Act. It provides that:[264]

> The collection and processing of personal data reveals racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic data, or, more generally, data concerning the person's state of health are prohibited.

[256] Article 131 (1) ICT Act.
[257] Article 4 (16) ICT Act.
[258] Roos 516
[259] Article 13 AU Convention, Principle 6.
[260] Article 5 (1) (f) GDPR.
[261] Article 7 (1) Convention 108
[262] As above/
[263] Abdurauf & Fombad (n6) 15.
[264] Article 132 (2) ICT Act.

This category of sensitive data is also provided under article 9 of the GDPR, article 6 of the Convention 108 and article 14 AU Convention. However, in comparison to the GDPR and the Convention 108, the 2020 ICT Act did not include in the list of sensitive data, personal data on security measures, offences, biometrical data, criminal proceedings, and convictions. Furthermore, the Convention 108 in its explanatory report, states that the list of sensitive data as provided under article 6 is not exhaustive. Every State party can add to the list other sensitive data in its domestic legislation.[265]

On the other hand, the 2020 ICT Act, unlike the GDPR, the Convention 108 and the AU Convention, did not allow exceptions where sensitive data could be processed. Instead, it has just been limited to prohibiting the processing of sensitive data without stating which sensitive data might be processed. As a result, other sensitive data are left unprotected, including biometrical data on criminal offences and convictions.

3.4 Weaknesses of the 2020 ICT Act

The 2020 ICT Act applies to every processing of personal data of a physical or a legal person.[266] In addition, it is considered by the Congolese legislator as innovative by establishing mechanisms in the protection of personal data.[267] However, although it pretends to regulate the data protection area, it does not cover all the sectors, including the principle governing data protection, considered the heart of any data protection legislation.[268] In the few provisions dedicated to data protection in the 2020 ICT Act, some principles governing the processing of personal data are confidentiality, consent, and sensitive data. However, these principles are not defined and explained in the 2020 ICT Act.

Nonetheless, article 133 of the 2020 ICT Act provides that the Minister of ICT should enact a ministerial decree by the proposition of the ARPTIC. That decree will determine the conditions and modalities under which the collection, recording, processing, storage and transmission of personal data should be done. Unfortunately, more than two years after the enactment of the ICT Act, no efforts have been undertaken to enact that ministerial decree. As a result, the protection of data protection remains ineffective. Nevertheless, the 2020 ICT Act does cover all data protection principles. However, the following are notable gaps:

3.4.1 Principle of lawful and fairness

The principle of lawful and fairness is usually the first principle in most legislations and data protection instruments. This is because it justifies the reasons for personal processing data in every legislation. However, although to be the legal basis of data protection legislation, this principle is not set out in the

[265] Explanatory Report to the Convention 108, para 55, available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (accessed 15 October 2021).
[266] Article 2 (2) ICT Act.
[267] ICT Act, Explanatory statement, Point 11.
[268] Abdurauf & Fombad (n 6) 12.

2020 ICT Act, which pretends to be innovative in regulating personal data. Therefore, the lack of this principle in the 2020 ICT Act can confirm that the processing of personal data is unlawful as it has no ground that justifies the processing. In addition, it is unfair since fairness is considered to be part and parcel of lawfulness.[269]

3.4.2 Principle of finality (purpose specific)

While the finality principle is considered the cornerstone of data protection, it is not provided under the 2020 ICT Act. In this way, Roos argues that personal data must not be processed not only for specified and lawfully or legitimate purposes, but they must also be processed in a compatible way with their purposes.[270] The purposes which justified the data processing are important considering every aspect of data protection, including the nature, origin, duration of data collected. In addition, the processing that has to be done and divulgations to the third parties justify the processing.[271]

However, the 2020 ICT Act does not provide the purpose of the finality for which personal data can be processed. It neither specifies, determine or define the purpose for which personal data must be processed. Therefore, this situation confirms unlawful data processing because the purpose principle ensures that the legal basis or the reason for the processing of data exist.[272] Furthermore, it ensures also that the scope of this reason is closely defined.[273]

3.4.3 Principle of minimality (particular purpose)

Although this principle is important as it requires that data processing be limited only to its intended purpose, the 2020 ICT Act does not provide for it. As a result, the processing of personal data can go beyond its particular necessarily purpose. Then, the minimality principle is infringed because the particular purpose exceeds what is necessary to fulfil the purpose of the processing. This amounts to unlawful processing as it relates to unnecessary data processing.[274]

3.4.4 Principle of quality

The 2020 ICT Act does not cover this principle, which obliges personal data to be kept updated, accurate, complete, and relevant to the processed objectives. The lack of this principle under the 2020 ICT Act makes the processing of persona data irrelevant because its purpose is not relevant, accurate, and updated to their use. Moreover, there is no requirement in the 2020 ICT Act on keeping updates, accuracy and relevant personal data. Therefore, the lack of this principle infringes the principle of data quality.

[269] Bygrave (n 53) 23.
[270] Roos (n 179) 112.
[271] As above.
[272] Roos (n 179) 123.
[273] As above.
[274] Neethling (n 179) 276.

3.4.5 Principle of transparency and openness

The 2020 ICT Act does not include any general or particular policy of openness related to development best practices and policies in the data protection area, as this principle is required. Furthermore, it does not provide how data subjects might be awarded on how their personal data are being processed, the purposes of the processing, recipients' identities, and the data controller's residence, as required by this principle. Consequently, the processing of data in DRC infringes this principle.

3.4.6 Principle of data participation

The 2020 ICT Act did not provide how a data subject could participate in processing their personal data. As a result, the lack of this principle in the 2020 ICT Act denies the data subject the right to access his personal data within a reasonable time and without expense and delay, as required by this principle. Furthermore, the 2020 ICT Act denies several data subjects' rights. These rights are, for example, the right to receive confirmation whether or not his when his data are probing processed, the right to obtain his data undergoing processing and their source, and the right to receive information on the underlying logic of the automated data processing.[275]

3.4.7 Principle of accountability

Despite its importance of being considered 'an umbrella principle which covers a myriad of obligations' and committing a data controller to set up necessary mechanisms to ensure compliance with all other principles, the 2020 ICT Act has ignored it. Furthermore, the lack of this principle in the 2020 ICT Act denies the data subject the right to know who is responsible for the unlawful processing of their personal data. In addition, it denies him the right to judicial or administrative remedy, the right to receive compensation from the controller damage caused by unlawful data processing. Therefore, the accountability could be incorporated in the 2020 ICT Act in order to give effect to other obligations and data processing principles.

3.4.8 Lack of an Independent Regulatory Authority

As Flaherty argues that 'the lack of oversight body is the major weakness in privacy Act'.[276] In addition, the supervisory authority must have the power of advising and authorisation. In particular cases, it is entitled to receive complaints from natural persons and bring infringements of data protection legislation to the judicial authorities and engage in legal proceedings without prejudice of prosecutorial authorities.[277] Furthermore, the GDPR provides that this kind of power also has to include the power to oblige a provisional or absolute limitation, for example, a prohibition on processing.[278]

[275] Roos (n 179) 122.
[276] Flaherty 'Surveillance societies' 305, A Roos 'The law of data (privacy) protection: a comparative and theoretical study' (2009) University of South Africa. available at http://hdl.handle.net/10500/1463 (accessed 16 October 2021).
[277] As above.
[278] Asa bove.

However, the 2020 ICT Act does not establish an independent Regulatory Authority. Under article 12 of the 2020 ICT Act, the Regulatory Authority is placed under the tutelage of the Minister of ICT. As a result, the independence is of the Regulatory Authority is not guaranteed as it is subject to the control of the Minister of ICT.

3.5 Lessons from other data protection legislation (Mauritius & South Africa)

The DRC can learn some lessons from Mauritius and South African data protection legislation. Indeed, Mauritius has comprehensive data protection legislation which set out all the principles governing the processing of personal data. Furthermore, the 2017 Data Protection Act (2017 DPA) establishes the Data Protection Office (DPO), an independent and impartial administrative Institution of privacy enforcement.[279] The Commissioner chaired the DPO, who must be a barrister of at least five years' standing.[280] In addition, the DPA states the ICT Tribunal to hear and determine appeals from the Data Protection Officer (Commissioner).[281]

In the same vein, the DRC can also learn from the South African Protection Of Personal Information Act (POPIA). As stated previously, it is the newest data privacy law worldwide.[282] Additionally, it is a comprehensive data protection legislation that broadly explains data processing principles, and data rights are clearly outlined in the first part of the Act.[283] Furthermore, the POPIA establishes an Information Regulatory, a supervisory body whose members are subject only to the Constitution and accountable to the National Assembly.[284]

Therefore, the DRC should also establish an independent and impartial Regulatory body whose members should be qualified in the sector of data protection or ICT, like in Mauritius. Then again, the Regulatory Authority should be subjected only to the Constitution and accountable to the National Assembly, like in South Africa. In addition, a special tribunal should be established to handle the appeals from decisions of the Regulatory Authority, as is the case in Mauritius. Doing so will guarantee genuine protection of personal data.

3.5.1 Mauritius

Mauritius is chosen in this analysing for many reasons. Firstly, consider its role in data protection reforms in Africa and its internationalised data protection systems.[285] Secondly, Mauritius was among the first countries in Africa to enact Data protection legislation according to international data protection standards.[286] Thirdly, it was the first African country to pass the 2004 Data Protection Act (2004 DPA),

[279] Section 4(2) 2017 DPA
[280] Section 4(3) 2017 DPA
[281] Article 51 2017 DPA
[282] Cookietbot (n 51)
[283] Section 5 POPIA
[284] Section 39 POPIA
[285] A Makulilo (n20) 2.
[286] ALT ADVISORY 'Data protection in Africa Factsheet : Mauritius' (2020) 1.

which established and operationalised the Data Protection Commissioner.[287] In addition, it replaced the 2004 DPA with the 2017 Data Protection Act (2017)[288], which is an updated and comprehensive data protection legislation modelled on the EU GDPR.[289]

Indeed, the Mauritian 2017 DPA, like the Congolese 2020 ICT Act, provides principles of personal processing data under section 21 (a). However, the 2017 DPA, unlike the 2020 ICT Act, is broader. It sets out six principles, while the 2020 ICT Act can be found only three principles as analysed above. Furthermore, the latter's scope is limited to the processing of some category of personal data. In contrast, the scope of the former is not limited as it applies to all kinds of personal data. As provided in the 2017 DPA, the principles are the copy-paste of those provided in the GDRP. The only difference is the last principle on the rights to the data subject, which is not listed under data processing principles in the GDPR and replaced by the principle of integrity and confidentiality in the GDPR.[290]

With regard to the principle of consent, both the 2020 ICT Act and the 2017 DPA provide the principle of data subject consent. However, the 2017 DPA is broader than the 2020 ICT Act. Firstly, it defines consent[291]. Secondly, it sets out conditions under which a data subject consent for processing their data. Thirdly, it guarantees the right to the data subject to withdraw his consent any time, without affecting the lawfulness data processing.[292]

Both acts guarantee the right to data subject related to sensitive data even though the 2017 DPA uses the wordings 'special categories of personal data.' However, the DAP, unlike the 2020 ICT Act, includes in this category personal data about: [293]

> sexual orientation, practices or preferences; genetic data or biometric data uniquely identifying a person; commission or alleged commission of an offence by a person; proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in the proceedings such other personal data as the Commissioner may determine to be sensitive personal data.

Consequently, the list of sensitive under the DPA is broader than one provided under the 2020 ICT Act. In addition, the latter list is exhaustive, while the former is not, because the Mauritian Commissioner can add on the list sensitive data. The future DRC's Data Protection legislation should incorporate data on biometric, sexual orientation and criminal offences. Also, it should provide for a non-exhaustive list of sensitive data, like the 2017 DPA, to ensure the protection of this kind of data.

[287] As above.
[288] Avalable at https://rm.coe.int/dpa-2017-maurice/168077c5b8 (accessed 10 September 2021).
[289]As above.
[290] Article 5 (1) (f) GDPR.
[291] Section 2 of 20 17 DPA
[292] Section 24 2 (e) of 2017 DPA
[293] Section 2 of 20 17 DPA

3.5.2 South Africa

South Africa is also chosen for the following reasons: first, like Mauritius, South Africa has a data protection legislation that is more comprehensive.[294] Second, it has been recognised as suitable for protecting personal data.[295] Third, it was passed after many types of research that drew perceptions from different countries worldwide.[296] Third, it was principally influenced by European Union Directives and the GDPR, which, at that time, was still in draft form.[297]

Indeed, the POPIA, like the 2020 ICT Act, provides for principles for processing personal data. But the POPIA is broader than the 2020 ICT Act, as it dedicated its Chapter 3 on conditions for lawful processing of personal information.

Concerning the principle of consent, both the POPIA and the ICT Act guarantee data subject processing consent. However, the POPIA has an extensive explanation of this principle, unlike the 2020 ICT Act. First, it defines as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.'[298] Second, it guarantees the right to the data subject to withdraw their consent at any time.[299] Third, it sets out exceptions to the data processing principle of consent.[300] In addition, unlike the 2020 ICT Act, it provides that a child's consent must be expressed by a competent person, even though it does not specify who the competent person is.[301]

With regard to the principle of sensitivity, both the 2020 ICT Act and POPIA guarantee this principle. However, unlike the 2020 ICT Act, which only prohibits the processing of sensitive data, the POPIA devotes the whole Part B of its Chapter 3 on lawful conditions of personal processing data. Furthermore, unlike the ICT Act, it includes the data on criminal behaviour in the list of sensitive data. It provides exceptions to the processing of sensitive data for each kind of sensitive data.

With regard to the principle of confidentiality, it is provided by both legislations but the POPIA as a broader scope. It provides several measures related to the principle of integrity and the principle of confidentiality of personal data.[302] It provides that: [303]

> a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable and technical and organisational

[294] Makulio (n 60)163.
[295] As above.
[296] As above.
[297] P Stein, 'South Africa's EU-style Data Protection Law' (2012) 10 Without Prejudice 48.
[298] Section 1 POPIA
[299] Section 11 2 b POPIA
[300] Section 12 1 (a) POPIA
[301] Section 11 2 (a) POPIA
[302] section 9 POPIA
[303] Section 19 1 (a) (b) POPIA

measures to prevent loss of, damage, unauthorised destruction of personal information; and unlawful access to or processing of personal information.

Furthermore, unlike the 2020 ICT Act, it strengthens the data subject's right to confidentiality by preventing him from the publicity that could not guarantee integrity and confidentiality.[304]

3.6 Conclusion

This Chapter examined the major principles governing the processing of personal data. It started by providing an overview, nature, and type of core principles governing data protection in light of international standards. Subsequently, in assessing their applicability to the DRC context, it was noted that the 2020 ICT Act does not cover all principles. In its provisions, only three principles can be identified: the principle of consent, confidentiality, and sensitivity. Then again, the 2020 ICT Act does not explain these principles, unlike the international standards and data protection legislation of some African countries, including Mauritius and South Africa.

Ultimately, this Chapter stated some lessons that the DRC can learn from Mauritius and South Africa regarding their comprehensive data protection legislation modelled on international standards. The DRC should adopt a comprehensive data protection legislation with all data protection principles and ensure the enforcement of that legislation by the establishment of an independent and impartial Regulatory which will not be subject to the control or direction of any other authority.

[304] Section 22 (6) POPIA

CHAPTER 4: FINDINGS AND RECOMMENDATIONS

4.1 Introduction

The preceding Chapters analysed the background, approaches and principles governing the processing of personal data in the DRC with regard to international standards. They sought to demonstrate to what extent the principles provided under the 2020 ICT Act comply with international and regional data protection standards. Thus, the following questions guided the reflection: What are the international and African regional standards on personal data protection applicable to the DRC? To what extent has the legal framework on personal data protection in the DRC complied with the international and regional standards?

This Chapter presents the findings after assessing the gaps of the 2020 ICT Act. It states the extent to which the 2020 ICT Act covers principles governing the processing of personal data and gives the principles that are not covered by the 2020 ICT Act. Furthermore, it compares with some African countries on mechanisms that must be established by the 2020 ICT Act to ensure the protection of personal data. Ultimately, it gives recommendations in order to ensure genuine protection of personal data in the DRC, which comply with international standards.

4.2 Findings

The study demonstrates the weaknesses of the 2020 ICT Act, which does not provide principles governing personal data in the light of international standards. In addition, it does not establish an independent body to ensure the enforcement of data subject's rights. Also, it does not establish security measures to ensure the transfer of personal data outside the DRC, as recommended by international standards.

4.2.1 Principles of processing personal data

The 2020 ICT Act does not cover all principles governing the processing of personal data. First, it provides data subjects' confidentiality and personal consent and the prohibition of processing sensitive data without stating how these principles should be applied to data subjects. Second, the 2020 ICT Act ignores other core principles on the processing of personal data, including lawful and fairness, purpose specification, minimality, quality, openness and transparency, data participation and accountability. Third, the 2020 ICT Act states that the Minister of ICT should enact ministerial decree by the proposition of the ARPTIC, which determines the conditions and modalities for 'collection, recording, processing, storage and transmission of personal data.'[305] However, the 2020 ICT Act is silent about when should the ICT Minister enact that decree. As a result, personal data are not protected due to the lack of that ministerial decree.

[305] Article 133 ICT Act.

4.2.2 Enforcement mechanisms

In order to ensure the effective processing of personal data, the enforcement mechanism must be established by the data protection legislation. According to the GDPR, the supervisory authority established to ensure monitoring and enforcement of data protection legislation must be independent in exercising its powers in general, including the power to investigate, correct, and sanction.[306]

However, under Article 13 (6), the 2020 ICT Act has empowered the Authority of Regulation of Posts and Telecommunications and Information (ARPTIC) to 'regulate and control personal data protection.'[307] But, it has established the ARPTIC under the wing of the Ministry of telecommunications and ICT.[308] Also, the 2020 ICT Act does not state how should appoint members of the ARPTIC. Therefore, this situation cannot guarantee the independence of ARPTIC in protecting the processing of personal data subjects, and then bring to the valuation of subject data rights.

In the line of the GDPR, the Mauritian 2017 DPA has established a Data Protection Officer with a Data Protection Commissioner at the head, assisted by public officers in necessity cases.[309] The Commissioner has different powers, including receiving and investigating complaints, requiring information, preserving orders, enforcing notice, seeking assistance, undertaking search, and other powers.[310] Furthermore, the 2017 DPA enforcement mechanism is strengthened by establishing ICT Appeal Tribunal, established by the Information and Communication Technologies Act 2001 under section 35.[311] This tribunal is entitled to hear and determine appeals of decisions held by the commissioner.[312] Also, appeals from the ICT tribunal are heard by the Mauritian Supreme Court.[313]

Makulilo mentions that it is fascinating that the Court of last resort in data protection issues in the United Kingdom Privy Council is entitled to handle appeals on data privacy from the Supreme Court.[314] The only case reached to the UK Privy Council on privacy is *Madhewoo v The State of Mauritius and another.*[315] With regard to the enforcement mechanisms, the South African 2020 POPIA has also established the Information Regulatory under Chapter 5. It is independent, impartial, subject only to the Constitution and law, and exercises its powers without fear, favour, or prejudice.[316] Also, it is accountable to the National Assembly, and the President appoints its members on the recommendation of the National Assembly.[317]

---

[306] Para 128 GDPR.
[307] Article 13 (6) ICT Act.
[308] Article 12 ICT Act
[309] Section 4 of the 2017 DPA
[310] Section 5 of the 2017 DPA
[311] Makulilo (n20) 20.
[312] Section 51 of the 2017 DPA
[313] Makulilo (n20) 21.
[314] As above.
[315] As above.
[316] Section 39 POPIA
[317] Section 42 (2) (a) POPIA

4.2.3 Transborder data flow

The security principle of data processing requires that a State have appropriate measures to ensure the security of personal data beyond its jurisdiction. Indeed, the protection of personal data has been challenged by globalisation and rapid technological developments.[318] With the development in the ICT sector, the collection and processing of personal data have significantly increased. ICTs allow private actors and public authorities to use more personal data than on a record scale. With this technological development, both economy and social life could have facilitated the free flow of data within countries.[319] Then, the third country must have data protection legislation that ensures a high level of protection.

According to the GDPR, the transfer of personal data in a third country or an international organisation must ensure a satisfactory level of personal data protection.[320] In addition, it provides that the adequacy of the level of protection must consider several elements such as the respect of fundamental freedoms, the respect of human rights, the rule of law, the existence of adequate legislation, and the establishment of an independent regulatory body.[321] Regarding the transfer of personal data outside the country, the 2017 DPA and the 2020 POIPA have also required adequate protection in the third country, like the GDPR.[322]

However, the 2020 ICT Act does not have any provision in this regard. Although, in contrast, many foreign companies in DRC process personal data, including the transfer of personal data outside the country, the 2020 ICT Act is silent on that issue. As a result, the transfer of personal data outside the DRC is not protected by the 2020 ICT Act.

4.3 Recommendations

In order to ensure the protection of personal data in the DRC with international standards, the following recommendations should be applied:

4.3.1 Ratification of the AU Convention

The DRC government must ratify the African Convention on Cyber Security and Personal Data Protection to ensure the promotion and protection of personal data by making individuals derive from it.

[318] Para 6 GDPR.
[319] As above.
[320] Article 44 GDPR
[321] Article 44 GDPR
[322] Section 36 DPA & section 72 POPIA

4.3.2 Recognition and constitutionalise the right to data privacy

Regarding the importance of personal data in the age of technological development, there is a crucial need to integrate the right to data privacy, separately from the right to private life, in the bill of rights of the DRC Constitution. As a fundamental law in DRC, recognising the right to data privacy in the Constitution will ensure the genuine protection of personal data like Algeria, Cape Verde and Mozambique. In doing so, the right to data privacy will acquire a superior status over other national Congolese laws as the DRC Constitution is a supreme law from which other laws have sources.

4.3.3 Enactment of a comprehensive data protection legislation

With regard to the increasing data processing activities that threaten and imperil people's rights, there is an urgent need for the DRC to enact comprehensive data protection legislation in light of the GDPR, which set out the international standards. That legislation must be drafted comprehensively and explicitly, which will be understood by everyone. The 2020 ICT Act is a small step in ensuring personal data recognition, but is limited considering the weaknesses above. All principles governing personal data must be incorporated in the Act and defined and explained in the light of international standards.

4.3.4 Enactment of the ICT ministerial decree

Considering the rigorous process of the amendment of the DRC Constitution and the long process of enactment of laws by Congolese Parliament, the ARPTIC should urgently propose to the Minister of ICT the decree provided under article 133 of the 2020 ICT Act. This decree should cover the gaps of the ICT Act, including setting out all data processing principles which are not included in the 2020 ICT Act in the light of international standards. Furthermore, it should define the principle of consent, provide its conditions, and determine a child's consent modalities. In addition, it should explain the principle of confidentiality and associate it with the security principle; include in the list of sensitive data, biometrical data, data on criminal offence, proceedings and convictions.

4.3.5 Establishment of an Independent Regulatory Authority

The data protection legislation should establish a regulator authority independent from the Minister of TIC to ensure that he plays the role of a regulatory body without threats. In order to ensure its independence, the Act should clearly determine that the Regulatory Authority will be only subject to the Constitution and the law, like in the South African POPIA. In addition, its members must be appointed or elected in a specified procedure. They must be qualified and have experience in the domain of data protection in particular or ICT in general. Furthermore, the regulator authority must have in its obligations the raising of awareness and educate Congolese on data protection; advising private and public entities on the requirements provided in the Act; establishing mechanisms to audit the processing of data system and treatment of complaints provided under the Act.

4.3.6 Recognition of data subject's rights

The Data Protection Act should recognise the rights of the data subject with the international standards, including the right to be notified of the collection, accession or acquisition by an authorised person to their personal data; the right to request the correction, destruction or deletion of their personal data; the right to object the processing of their data when there is no reasonable ground of justification; the rights to object the processing of their data for the purposes of direct marketing; the right to object the processing that will make them subjected to automated decision making; the right to have the remedy.

4.3.7 Raise awareness on data protection

Considering that data protection issues are novel and ignored by most Congolese, civil society organisations, the regulator authority, Public authorities, telecommunication companies, members of the press, the academia and community leaders must raise awareness on data protection issues. In addition, they must influence the Parliament to adopt comprehensive data protection legislation on international standards. In the meantime, before enacting that data protection legislation, the ICT Minister must cover the gap by enacting the ministerial decree proposed by the ARPTIC, on conditions and modalities of data processing.

Furthermore, judicial authorities and lawyers must be trained in active litigation before courts to ensure that the regulatory authority, security services, and government comply with international data protection standards. Also, the Congolese Human Rights Commission, human rights activists, civil society, and pro-democracy activists must step up their efforts to protect personal data and privacy. Ultimately, with regard to the lack of research on Congolese data protection, scholars, academia, students should research personal data from diverse perspectives. Implementing all the above recommendations will arguably allow the DRC to ensure the protection of personal data and privacy in light of international standards.

5 Conclusion

This study sought to assess the principles governing personal data protection in the DRC by examining the extent to which the Congolese legislation (ICT Act) complied with the international standards of data protection principles. It started by demonstrating how the development of technology in the current age has impacted all human activities with digitalisation. The increase of computers and the development of ICT facilitate the transfer of information between computer systems and boost personal data collection and processing. Also, the emergence of new technologies has created new challenges that require new solutions. With the collection of personal data by public and private entities, data subjects' rights can be infringed. Many risks could lead to the violation of the data subject. Furthermore, the processing of his personal data poses a threat to his privacy. Therefore, there is a need for an effective legal regime that regulates personal data according to internationally accepted principles, namely fair

and lawful processing, purpose specification, minimality, openness or transparency, data subject participation, sensitivity, security and confidentiality, and accountability.

Furthermore, the study demonstrated how worldwide, particularly in Africa, countries are adopting and updating data protection legislation and policies. This is because States want to ensure privacy and attract foreign investments, especially from Europe. For these reasons, they must have comprehensive legislation that guarantees adequate protection of personal data as the free flow of personal data goes beyond countries' jurisdiction. Therefore, adequate legislation that guarantees personal data protection in a third country is a principal condition.

However, despite the emerging data protection legislation in Africa, the protection regime in the DRC is deficient, and these gaps must be addressed. The 2020 ICT Act does not cover all principles governing personal data. It just refers to some principles without giving further explanation. Only three relevant principles can be identified in the whole Act, namely principles of consent, confidentiality and sensitivity. In addition, the ministerial decree that could try to cover the gap by determining the modalities and conditions under which personal data should be collected, processed and stored is not yet enacted by the ICT Minister on the proposition of the ARPTIC. Also, the oversight mechanism established by the 2020 ICT Act to regulate and control the protection of personal data is not independent as it is placed under the tutelage of the ICT Minister.

Therefore, after analysing principles governing the processing of personal data in the 2020 ICT Act in the light of international standards and other African countries with comprehensive data protection legislation modelled on international standards, the study proposes recommendations in order to ensure that the DRC comply with international standards. These are namely: the ratification of the African Convention on Cyber Security and Personal Data Protection; the recognition of the right to data privacy under the Constitution different to the right to private life and secrecy of correspondence; the enactment of a comprehensive data protection legislation with all data procreation’s principles and subject’s rights; the establishment of an independent Regulatory Authority; the outreach of data protection.

(Word Count 19 860)

Bibliography

Books

- Bennett *Regulating privacy: data protection and public policy in Europe and the United States* (1992)
- Bygrave, LA *Data privacy law: An international perspective* (Oxford University Press, 2014)
- Bygrave, LA *Data protection law: Approaching its rational, logic and limits* (MIT Press, 2002)
- Bygrave, LA *Data protection law: approaching its rationale, logic and limit* (2002)
- Flaherty, *Protecting privacy in surveillance societies-the Federal Republic of Germany, Sweden, France, Canada, and the United States* (1989)
- Hondius *Emerging data protection in Europe* (1975)
- Kodjo, A *Les droits des télécoms et du numériques : Profil africain et congolais, prospective comparée d'Europe et de France*, L'Harmatan (2019)
- Miller, A *The Assault on* Privacy: *Computers, Data Banks and Dossiers* (UMP 1971)
- Viljoen, F *International Human Rights Law in Africa* (2012) Oxford University Press
- Westin, A *Privacy and Freedom* (Bodley Head 1970)
- Wetsh'Okonda, M *Les textes constitutionnels congolais annotés* (Campagne pour les Droits de l'Homme au Congo, 2011)

Journal articles

- Blume 'An EEC policy for data protection' 1992 *Computer/Law Journal*
- Bygrave, L 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *International Journal of Law and Information Technology*
- Currie, I & De Waal, J *The Bill of Rights Handbook* (6th edn, Juta 2013)

- Greenleaf, G 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) *International Data Privacy Law*

- Greenleaf, G & Georges, M 'The African Union's data protection Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws & Business International Report*

- Harris, A and others 'Privacy and security concerns associated with mobile money application in Africa' (2013) 8 *Washington Journal of Law, technology*

- Kandolo wa Kandolo, B 'Réseaux sociaux : réflexion sur l'émergence d'une nouvelle forme de gouvernance des droits de l'homme en République Démocratique du Congo' *Revue générale de Droit et Interdisciplinaire de Likasi* (2018) 338 available at https://www.leganet.cd/Doctrine.textes/Decon/Reseauxsociauxetdroitsdelhomme.pdf (accessed 8 October 2021).

- Korff, D & Georges, M 'The DPO Handbook: Guidance for data protection offices in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation' (2019).

- Makulilo, A 'The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius' (2020), *The International Journal of Human Rights* available at https://doi.org/10.1080/13642987.2020.1783532 (accessed 10 August 2021).

- Makulilo, A'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) *International Data Privacy Law* 163, 176

- Neethling J and others Neethling's *law of personality* (2005),

- Roos, A 'Core prinicples f data protection law' (2006) 107*Journal of Southern Africa*, available at https://www.jstor.org/stable/23253014?seq=1#metadata_info_tab_contents

- Singh & Power 'The Privacy awakening: The urgent need to harmonize the right to privacy in Africa' (2019) NUMBER OF THE ISSUE *African Human Rights Yearbook*, 202

- Stein, P 'South Africa's EU-style Data Protection Law' (2012) 10

- Trubow 'The European harmonization of data protection laws threatens US participation in trans-border data flow' 1992 *North-western Journal of International Law and Business* 159 161;

- Van der Sloot, B 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 307

- Yilma, K & Birhanu, A 'Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices' (2013) 1 *Journal of Ethiopian Law* 26, 106

Theses and dissertations

- C Nyemba 'Right to Data Privacy in the Digital Era: Critical assessment of Malawi's Data Privacy protection regime' LL M Dissertation HRDA University of Pretoria (2019)

- Karanja, SK 'Schengen Information System and Border Control Cooperation: A Transparency and Proportionality Evaluation', PhD Thesis, Faculty of Law, University of Oslo, (2006) 86

- Roos, A 'The law of data (privacy) protection: a comparative and theoretical study' (2009) University of South Africa, PhD Thesis, available at http://hdl.handle.net/10500/1463 (accessed 16 October 2021).

United Nations instruments and documents

- Universal Declaration of Human Rights 1948.

- International Covenant on Civil and Political Rights 1966.

- General Comment No. 16: Article 17 (Right to Privacy) 1988.

- Resolution on the Right to Privacy, Human Rights Council (2015).

- OECD Guidelines Explanatory Memorandum (1981).

- UN Guidelines for the regulation of computerized personal data files (1990).

- United Nations Conference on Trade and Development 'Data Protection and Privacy Legislation Worldwide' 2020 available at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed 28 August 2021).

European Instruments

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) available at (europa.eu) (accessed 30 May 2021).

- Convention for the protection of individuals with regard to the processing of personal data 2018 (Convention 108+) available at 1613477197639c73z8n12ay.pdf (guardint.org) (accessed 30 May 2021).
- Explanatory Report to the Convention 108, para 55, available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

African Instruments

- African Charter on Human and Peoples' Rights (1981/1986)
- African Union Convention on Cyber Security and Personal Data Protection (2014).
- Declaration of principles on freedom of expression in Africa (2002), available at Microsoft Word - Declaration2.doc (refworld.org) (access 18 September 2021).
- Resolution 362 on the right to freedom of information and expression on the internet in Africa ACHRP/Res. 362 (LIX) 2016 available at https://www.achpr.org/sessions/resolutions?id=374 (access 18 September 2021).
- African Charter on the Rights and Welfare of the Child (1990/1999)
- AU 'Personal data protection guidelines for Africa' (2018) available at https://www.internetsociety.org/wp content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed 18 September 2021).

Congolese legislation

- Constitution of the Democratic Republic of Congo (2006) as amended in 2011.
- Constitution of Transition (2003).
- Act 20/017 Telecommunications and Information and Communications Technology.
- Act 013/2002 of 16 October 2002 on Telecommunications in the Democratic Republic of Congo available at http://www.droit-afrique.com/upload/doc/rdc/RDC-Loi-2002-13-cadre-telecom.pdf (accessed 18 August 2021).
- Act 14/2002 of 16 October 2002 on the creation of the post and telecommunications regulatory authority available at https://www.droitcongolais.info/files/7.35.11.-Loi-du-16-

octobre-2002_Autorite-de-recgulation-de-la-poste-et-des-telecommunications.pdf (accessed 18 August 2021).

- Act No. 18-019 on payments and securities settlement systems .
- The Criminal Act 1940

Other Constitutions & national legislations

- Cape Verde Constitution (1980 amended 1992), available at THE CONSTITUTION OF THE EPUBLIC OF CABO VDE (into-sa.com) (accessed 4 October 2021).
- Mozambique Constitution (2004 amended 2007), available at MZ004 : Other, Constitution, 1990, (2004) (parliament.am) (accessed 4 October 2021).
- Algeria Constitution (2020) available at (anonymous) (constituteproject.org) (accessed 4 October 2021).
- Act No. 20 of 2017 The Data Protection Act 2017 available at https://rm.coe.int/dpa-2017-maurice/168077c5b8 (accessed 6 October 2021).
- Act No. 4 of 2013 Protection of Personal Information (POPIA)

Reports

- CIPESA, 'State of internet freedom, Democratic Republic of the Congo 2019, Mapping trends in Government internet controls 1999-2019' (2020) 9 available at https://cipesa.org/?wpfb_dl=408 (accessed 20 September 2021) (accessed 10 August 2021).
- International ICT Policy for East and Southern Africa, 'Etat des lieux des libertés sur Internet en République Démocratique du Congo : Les stratégies des gouvernements africains pour étouffer les droits numériques des citoyens' 2016
- Makunya, T 'Digital space and protection of freedom and association and peaceful assembly in Africa: Report of CIPESA on the Democratic Republic of Congo' (2021)

Case law

- *Social and Economic Rights Action Centre and Another v. Nigeria* (2001) AHRLR 60 (ACHPR 2001).

Websites

- ALT ADVISORY 'Data protection in Africa Factsheet : Mauritius' (2020) 1 available at https://rm.coe.int/dpa-2017-maurice/168077c5b8 (accessed 10 September 2021).

- ALT ADVISORY 'Data protection in Africa Factsheet : South Africa' (2020) 1 https://dataprotection.africa/wp-content/uploads/2020/08/South-Africa-Factsheet-updated-20200803.pdf (accessed 17 October 2021)

- ARPTC' the DRC global rate of cell phone penetration and internet' available at https://deskeco.com/2021/09/03/rdc-larptc-situe-le-taux-de-penetration-global-de-la-telephonie-mobile-471-et-celui-de-linternet (accessed 6 October 2021).

- Cookietbot 'POPIA South Africa's Protection of Personal Information Act, enforcement update July 2021' available at https://www.cookiebot.com/en/popia/? (accessed 29 October 2021).

- Banisar, D 'The right to information and privacy: balancing rights and managing conflicts' 2011 6 available at https://openknowledge.worldbank.org/handle/10986/23022 (accessed 30 September 2021).

- Information Commissioner's Office 'Guide to the General data protection regulation (GDPR)' available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=248%23link2#link3 (accessed 30 September 2021).

- Woodward, M '16 countries with GDPR-like Data Privacy Laws' (2021) https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws (accessed 26 August 2021)

- Thales 'Beyond GDPR: Data protection around the world' (2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world (accessed 26 August 2021)

- Abdulrauf L & Fombad, C 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' 2016 2, available at https://repository.up.ac.za/bitstream/handle/2263/60613/Abdulrauf_African_2016.pdf? (accessed 6 August 2021).

- Privacy International 'Data Protection' available at https://privacyinternational.org/learn/data-protection (accessed 28 August 2021).

- Explanatory Report to the Convention 108, para 55, available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (accessed 15 October 2021).

- Cloudian 'Data protection guides' available at https://cloudian.com/guides/data-protection/data-protection-regulations/ (accessed 15 October 2021)

- Limpitlaw, J 'Manuel des droits des medias en Afrique australe, la République Démocratique du Congo' (2020) 15 available at https://www.kas.de/documents/285576/11521648/MLHSA+2021+Version+Fran%C3%A7aise+-+RDC+.pdf (accessed 6 October 2021).

- International Telecommunication Union (ITU) 'Support for harmonisation of the ICT Policies in Sub-Saharan Africa' 2021 available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx (accessed 18 September 2021).

- Data Protection: Southern African Development Community (SADC) Model law https://www.itu.int/en/ITUD/Projects/ITU ECACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed 18 September 2021).

- African Union, List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection 2014, https://au.int/sites/DATA%20PROTECTION.pdf (accessed 18 September 2021).