THE PRICE OF EXCLUSION: AN ANALYSIS OF THE INADEQUATE INCLUSION OF CLEAR PROVISIONS ON DATA SHARING OF SENSITIVE PERSONAL DATA OF DATA SUBJECTS IN KENYA

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree,

Strathmore University Law School

By

Vanessa Sylvia Odhiambo

136311

Prepared under the supervision of

Mwangi Claude Kamau

February 2024

TABLE OF CONTENTS

Acknowledgments

I extend my heartfelt gratitude to my supervisor Mr. Claude Kamau, for his invaluable guidance, patience and support throughout this dissertation. I am deeply grateful to my family for their unwavering support.

Declaration

I, Vanessa Sylvia, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Works cited or referred to are accordingly acknowledged.

Signed:.....

Date: 4th | April | 2024

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed:

(Claude Kamau)

vi

Abstract

In Kenya, data sharing of sensitive personal data is provided for under sec 44 and 55 of the Data Protection Act (2019). The General Data Protection laws require that data subjects be accorded specific rights and interests while their sensitive personal data. However, there is a lack of a supporting framework to facilitate the inclusion of data subject's rights such as ownership and self-determination rights. Failure to include these rights and interests will expose their data to misuse and abuse of their rights and freedoms. Furthermore, the legislative framework surrounding data sharing of sensitive personal data fails to clearly provide for obligations that data processors have while handling sensitive personal data of data subjects. This study will attempt to deconstruct the concept of informational self-determination as a principle and as a right of data subjects. Building on the existing data subjects rights under sec 25 of the Data Protection Act, this study asks; *how can the principle of informational self-determination be incorporated in the legislative framework to ensure data sharing of sensitive personal data is effectively done without the misuse or abuse of the patient data*. Based on the review on the existing literature relating to data sharing of sensitive personal data in Kenya, there is currently an insufficient framework that is contradictory and unclear to its aims with relation to data sharing of sensitive personal data. Nonetheless, the results of this study indicate that a framework that encompasses fundamental rights such as informational self-determination, data ownership and personal autonomy rights will serve as useful in ensuring no privacy breaches in data sharing of sensitive personal data. Failure to incorporate these rights and ensuring clarification of the same in the legislative framework surrounding data sharing of sensitive personal data will result in abuse and misuse by data processors.

List of Abbreviations

1. SPD- Sensitive Personal Data
2. PLHIV- People Living with HIV and AIDS
3. ISD- Informational Self-determination

List of Cases

KELIN and 3 others v Cabinet Secretary Ministry of Health and 4 others [2016] Eklr

Data Protection commissioner v Facebook Ireland Limited (2018), High Court of Ireland.

List of Legal Instruments

1. Data Protection Act (2019)
2. Constitution of Kenya (2010)
3. Data Protection (General) Regulations (2021)

VT OMNES
VNVM SINT

CHAPTER ONE: INTRODUCTION

1.1 Background

1.1.1 Background to the Study

The debate around data sharing is complex with wide recognition that the type of data, who has access and how data will be used has the potential to generate context-specific ethical issues. [1]Data sharing is any operation involving the transfer and dissemination of data. Privacy, a necessity for this practice, empowers individuals to maintain control over their personal information by allowing data owners to know how their data is maintained, controlled and handled. Privacy is a notoriously vague term that is contextual in the sense that it entails that it is sensible to share an individual's data with a party or parties while maintaining confidentiality, and also defined as a situation whereby data relating to a person are either in a state of non-access, or in a state of managed access such that the person can decide whether and how they may be processed. [2]International Human Rights law provides that everyone has a right to privacy, and this exclusively applies to the processing of sensitive personal data of data subjects. [3]Sensitive personal data is data revealing racial or ethnic origin, biometric and genetic data as well as health data of a data subject. Data subjects in this context, are identifiable living individuals to whom personal data relates.[4] The concept of sensitive personal data has been a mainstay of data protection for a number of decades. The concept itself is used to denote several categories of data for which processing is deemed to

[1] Bainbridge, 'Processing personal data and the data protection directive. Information and Communications Technology Law', 1997, 17-40--< https://www.tandfonline.com/doi/abs/10.1080/13600834.1997.9965752> on 4 March 2023.

[2] Article 12, *Universal Declaration of Human Rights*, 10 December 1948, 999 UNTS 171.

[3] Quinn and Malgieri, 'The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework' *German Law Journal*, 2021,1583-> https://www.cambridge.org/core/journals/german-law-journal/article/difficulty-of-defining-sensitive-datathe-concept-of-sensitive-data-in-the-eu-data-protection-framework/5EC5932AAC5703E31D2C90045813F6C6> on 4 March 2023.

[4] Quinn and Malgieri, 'The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework' *German Law Journal*, 2021,1583-> https://www.cambridge.org/core/journals/german-law-journal/article/difficulty-of-defining-sensitive-datathe-concept-of-sensitive-data-in-the-eu-data-protection-framework/5EC5932AAC5703E31D2C90045813F6C6> on 4 March 2023.

pose a higher risk for data subjects than other forms of data, such risks are often perceived in terms of an elevated probability of discrimination, or related harms, to vulnerable groups in society. As a result, data protection frameworks have traditionally foreseen a higher burden for the processing of sensitive personal data than other forms of data. The sui generis protection of sensitive data 'stronger than the protection of non-sensitive personal data' can also seemingly be a necessity from a fundamental rights-based perspective, as indicated by human rights jurisprudence.

1.1.2 Background to the Problem

Kenya's fragile data protection regime lacks comprehensive and up-to-date legislation that aligns with international standards as earlier stated with relation to data sharing and this has resulted in the misuse and abuse of sensitive personal data of data subjects over the years. [5]In 2015, the Government of Kenya through the President issued a directive to all County Commissioners to collect up to date data and prepare an inter alia report on all school going children, guardians, and expectant and breastfeeding mothers living with HIV/AIDS, the sources of this data being government publications on research involving medical data. [6] The parties concerned, who were also unaware of their rights to disclose sensitive personal data, were irreparably harmed through stigma and discrimination after publication of reports with their data. There was also disclosure of the subject's HIV status to third parties on their health information without consent contrary to International Guidelines on HIV and AIDS. [7]In response, the High Court issued a ruling that the implementation of the directive violated the rights of the data subjects through the disclosure of their identities and medical status. [8]The fundamental right put to consideration by the court was the right to privacy which inter alia provides that every person has the right not to have information on their family and private affairs divulged or called for. The court noted this when it concurred with the petitioners that the implementation of the directive violated the best interests of the subjects. The Court also suggested amendment of the legislative framework surrounding the processing of sensitive personal data to include protection of data subject's rights while allowing

[5] KELIN and 3 others v Cabinet Secretary Ministry of Health and 4 others [2016] eKLR.
[6] KELIN and the Key Populations Consortium. "*Everyone said no": Biometrics, HIV and human rights,* A Kenya case study, 2018.
[7] KELIN and 3 others v Cabinet Secretary Ministry of Health and 4 others [2016] eKLR.
[8] Article 31, *Constitution of Kenya* (2010).

retention of general data for statistical purposes to be used in addressing the data subject's needs.[9]Shortly after this exercise in 2015, the Parliament passed the Data Protection Act, 2019 which set out provisions that still did not clarify certain rights to data sharing of sensitive personal data of data subjects.

From a legal standpoint, at the time of effecting this directive, the already precarious data regime had an insufficient legal framework for the processing of sensitive personal data, this is evident through the unclear provisions that directly speak on the grounds for processing of sensitive personal data, sec 44 and 45 of the DPA specifically are unclear and inconsistent with other provisions in the act. [10]The processing of sensitive personal data stated in sec 44 is silent on a number of things. Firstly, definitions under section 2 of the DPA are not clearly defined. The definition of 'sensitive personal data' has a couple of omissions including the commission or alleged commission of any offense, or any proceedings for any offense committed or alleged to have been committed, disposal of such proceedings or the sentence of any court in such proceedings. [11]Secondly, there are no considerations given in relation to sec 44(1) of the DPA with regards to shortcomings of sec 30 that provides for lawful processing of personal data. [12]The act fails to define what constitutes public interest in sec 30(1) (iv) and there exists no public interest ground provided for with relation to data sharing of sensitive personal data. This section is also very broad in terms of what the legitimate interests pursued by a data controller or data processor by a third party entails, therefore raising questions as to the intended purpose of the provision. The wording used in section 30 is open to abuse since if the provision is included and there exists doubt in the balancing exercise that is prejudice to the individual, then the presumption should be that the processing should not proceed. [13]The third unclear provision, sec 45, provides for grounds of processing sensitive personal data noting the complexity of the data generation and processing ecosystem and states that a data subject 'manifestly' making their data public is not a sufficient justification for indirectly processing the data without involving the data subject. [14]The ground

[9] Greenleaf and Cottier, '2020 ends a decade of 62 new data privacy laws', 2022,24-<https://www.austlii.edu.au/au/journals/UNSWLRS/2015/21.pdf> on 4 March 2023.

[10] Section 44, Data Protection Act, (Act No 24 of 2019).

[11] Section 44(1), Data Protection Act, (Act No 24 of 2019).

[12] Section 30 (1) (iv), Data Protection Act, (Act No 24 of 2019).

[13] Section 45, Data Protection Act, (Act No 24 of 2019)

[14] Section 45 (1) (c) (ii), Data Protection Act, (Act No 24 of 2019)

provided in sec 45 (1) (c) (ii) referring to 'rights of the controller' is contradictory as a data controller does not have rights in the same way as the owner of the data, a data subject, and if in any case legal obligations were being referred to in this provision, it is still very unclear. [15] Section 55 (2) which provides for the issuance of a data sharing code with relation to data sharing of sensitive personal data to government departments or public sector agencies. The predicament exists in interpreting the principle of autonomy and self-determination which is meant to ensure that the data subject has absolute control over their sensitive personal data. This act clearly suffers greatly from several shortcomings, vagueness and ambiguity with problematic contradictions.

1.2 Problem Statement

Section 55 (2) of the Data Protection Act [16]provides for the issuance of a data sharing code between public sector agencies to facilitate dissemination of sensitive personal data , however it fails to provide for the inclusion of the right to access, duty to inform and individual ownership of data which presents a risk to the freedoms and rights of the data subjects, undermining the procedure and hinders the promotion of the principle of informational self-determination.

1.3 Research Objectives

1. To examine the principle of informational self-determination and duty to inform and their role in data sharing of sensitive personal data
2. To examine whether the current framework on data sharing adequately complies with the principle of informational self-determination
3. To propose incorporation of the duty to inform and ownership rights of data subjects into the guidance note on sharing of health data provided by the Office of the Data Protection Commissioner.

[15] Section 55 (2), Data Protection Act, (Act No 24 of 2019)
[16] Section 55(2), Data Protection Act, (Act No 24 of 2019)

1.4 Research Questions

1. Whether sec 55(2) of the Data Protection Act is adequate in entrenching the principle of informational self-determination in data sharing of sensitive personal data?
2. Whether section 55(2) fails to adequately address the principle of informational self-determination by failing to provide a sufficient and clear framework for data sharing of sensitive personal data?
3. Should section 55 (2) of the Data Protection Act be amended to incorporate the inclusion of the duty to inform and ownership rights of a data subject?

1.5 Hypothesis

The following constitutes hypothetical answers to the research questions above

(a) The current legislative framework specifically sec 55 (2) of the Data Protection Act fails to provide for duty to inform and ownership rights of data subjects with relation to data sharing of their sensitive personal data.

(b) This exclusion presents a risk to the rights and interests of the data subjects as the section fails to adequately address the principle of informational self-determination by failing to provide a clear framework on data sharing of sensitive personal data.

(c) The incorporation of the duty to inform and data ownership rights will allow for incorporation of rights and interests of data subjects in data sharing of their sensitive personal data. The incorporation of a framework that provides for the duty to inform will contribute to the promotion of the principle of informational self-determination.

1.6 Justification

Data sharing in Kenya presents an underlying issue of maintaining trust of the wider public especially when sensitive personal data is handled without involving the data owners. Although risks are not easily quantifiable, there is a probability of generating negative implications when sensitive personal data is misused and abused. On the other hand, there is a potential infringement of the right to privacy as the processed data is misused by the processors with the claim that a data subject 'manifestly' makes their data public. Seemingly, the current legal provisions in Kenya regarding data sharing is silent on the rights of the data subject in processing of their sensitive personal data indirectly without their involvement. Therefore, there lies competing interests between the rights of the data subjects and obligations of data processors. This study will be useful to stakeholders such as data processors to enable them to be informed of their obligations to data subjects while processing their data. The data subjects will also be imparted with knowledge of their rights and freedoms with regards to processing of their data. Additionally, it will benefit policy makers, ministers of Health in Kenya who are drafting policies to address these similar gaps arising from data sharing. Addressing the question will also be helpful to adjudicators in dealing with cases of violations against data subjects arising before them.

1.7 Theoretical Framework

The theoretical framework behind this study will largely be from the point of view of personal autonomy.

1.7.1 Personal Autonomy

This study will be premised on the theory of personal autonomy. [17]Simply put, this theory describes a fact in context of the ability to choose and have absolute control with deliberation and it suggests a right which exercises that ability without external interference either by overt force or by lack of truthful information. [18]Personal Autonomy is therefore understood as a quality that all selves must

[17]Shell, SM, *Kant and the Limits of Autonomy*, Harvard University Press, Cambridge, 2009, 3.

[18] Guyer, '*Kant on the theory and practice of autonomy. Social philosophy and policy'*, 2003, 70-98<https://www.cambridge.org/core/journals/social-philosophy-and-policy/article/kant-on-the-theory-and-practice-of-autonomy/78DE2DC254F543F996798A5C48B8B978#> on 3 March 20223.

minimally possess and are presumed to insist on or deserve. [19]This theory has its origin in ethnic and political literature to explain liberty and rights of persons in the context of absolute control and self-determination of personal matters. [20]There is a strong presence of the above in the privacy and liberty of person's realm. This is because liberty presumes an autonomy of self that includes freedom of thought, expression and absolute control of private matters.[21]

Kant acknowledges the aspect of morality and reason placing people as moral agents responsible for their actions. [22]This theory calls for respect for other people in their treatment process especially those with sensitive conditions. [23]Personal Autonomy is key in analyzing the doctrine of privacy in the context of data sharing of sensitive personal data. This is so as it speaks to the instrumental nature of privacy and its relationship to autonomy as the two correlate and cannot be understood if one is absent. [24]Therefore, there is need for data subjects to be treated with application of informed consent meaning that they ought to understand every concept of data sharing as well as their rights and freedoms. This ultimately results in personal autonomy and absolute control over how their sensitive data is handled by data processors. Personal autonomy therefore is applicable when provisions that are specific to protect the rights of data subjects are in place and application of informational self-determination principle, thus avoiding unwarranted intrusions and privacy violations since the data subjects are aware of their rights in context of data sharing. [25]

This theory of personal autonomy will be used to critique Kenya's insufficient and unclear framework provisions on data sharing of sensitive personal data by looking into whether the existing legal framework allows data subjects to exercise personal autonomy over their personal

---

[19] Bielefeld, *'Autonomy and republicanism: Immanuel Kant's philosophy of freedom'. Political Theory*, 1997, 544-558-<https://journals.sagepub.com/doi/abs/10.1177/0090591797025004003?journalCode=ptxa> on 4 March 2023.

[20] Cooke, *'Private autonomy and public autonomy: Tensions in Habermas' discourse theory of law and politics' Kantian Review, 2020,*559-582-<https://www.cambridge.org/core/journals/kantian-review/article/private-autonomy-and-public-autonomy-tensions-in-habermas-discourse-theory-of-law-and-politics/22B5D3AFC7D37EF6EDA19DB98A9E9261> on 4 March 2023.

[21] Shell, SM, *Kant and the Limits of Autonomy*, Harvard University Press, Cambridge, 2009, 3.

[22] M.N.S Sellers, ' *An Introduction to value of autonomy in law'* 2007, 1-9-<https://link.springer.com/chapter/10.1007/978-1-4020-6490-6_1> on 4 March 2023.

[23] Brudner, 'Private Law and Kantian Right' *University of Toronto Law Journal*, 2011, 279-311-<https://www.utpjournals.press/doi/abs/10.3138/utlj.61.2.279 >on 4 March 2023.

[24] Osuji, '*African traditional medicine: Autonomy and informed consent*', Vol 3, Springer Cham, 2014,1-8.

[25] Kombe, Mwalukore, Bull, Parker, Kamuya, Molyneux, Marsh, '*Research stakeholders' views on benefits and challenges for public health research data sharing in Kenya: the importance of trust and social relations'. PloS one,2015,10-*< https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0135545>on 4 March 2023.

data. Firstly, it will be used to gauge whether the insufficient and unclear provisions on data sharing of sensitive personal data allows the application of the principle of informational self-determination and personal autonomy on the data subjects and whether they are conversant with their rights with regards to handling their sensitive personal data. This will be useful in assessing whether the current legal provisions on data sharing allows application of personal autonomy of the data subjects. Secondly, is whether the current legal framework recognizes the principle of informational self-determination of data subjects. The existing legal framework presents a contradiction between the provisions and exposes data subjects to privacy violations since there exists no duty to inform them with regard to how these government agencies handle their data, and the data subjects lack absolute control over their data and this eventually results to data misuse and abuse**.**

1.8 LITERATURE REVIEW

The ongoing academic discourse surrounding the research problem has veered off in different directions quite distinct to this study. So far, the literature on data sharing of sensitive personal data has mostly focused on introducing the general issues, addressing the problem of privacy violations and the proposed solutions to evade risks relating to data sharing by enhancing the favorable risk benefit ratio. Although White and Lisa have touched on the research problem in one paragraph, the scholars discussed the concept of individual autonomy and stated that it must be justified in terms of the obligation of public health to improve population health, reduce inequities, attend to the health of vulnerable and systematically disadvantaged persons, and prevent harm. In addition, they discuss that data collected without consent must represent the minimal necessary interference, lead to effective public health action, and be maintained securely.

1.8.1 The proposed solutions to evade data breaches of data owners in Public health surveillance

Public Health Surveillance is the ongoing, systematic collection, analysis, and interpretation of health-related data with the purpose of preventing or controlling disease or injury, or of identifying unusual events of public health importance, followed by the dissemination and use of information

for public health action. The following are major ethical issues captured in existing literature regarding public health surveillance of data subjects. [26]

i Informed Consent

As Gerald Dworkin points out, the doctrine of informed consent is a 'creature of law'; it has been developed in various legal domains in which one party sanctions another to perform 'some course of action to which the consented party would otherwise have no moral right'. The fundamental idea that we aim to capture when we claim that 'A moral right to obtain B's informed consent to A's doing x to B', is that the moral permissibility of A's doing x to B. [27]Akinyi on the other hand, describes informed consent as the pertinent information given to patients before they participate in any medical activity or research. [28]Regarding public health surveillance, it is expected that the patients understand the probability of the general public accessing their personal data and the data subjects ought to have granted those individuals permission to access their medical information. [29]This pertains to their rights to autonomy and privacy.[30] Some scholars such as Mystakidou and Efi have addressed the ethical and practical aspects of informed consent in HIV research. [31]Their major argument was that informed consent is the cornerstone of biomedical

[26] Gunderson, M, 'Justifying a principle of informed consent: A case study in autonomy-based ethics. Public Affairs Quarterly',1990, 249-<https://www.jstor.org/stable/40435751> on 5 March 2023.
[27] Barbara Akinyi, 'laws, policies and the right to privacy for PLHIV in Kenya' Unpublished LLB Dissertation, University of Nairobi, Nairobi,2019,40.
[28] Ioannidis, J.P, 'Informed consent, big data, and the oxymoron of research that is not research', *The American Journal of Bioethics*.2013-<https://www.tandfonline.com/doi/abs/10.1080/15265161.2013.768864?journalCode=uajb20 >on 5 March 2023.
[29] Peto, Fletcher and Gilham, *'Data protection, informed consent, and research' BMJ, 2004, 1029-1030.* <*https://www.bmj.com/content/328/7447/1029.short*> on 5 March 2023.
[30] Mystakidou, Panagiotou, Katsaragakis, Tsilika, and Parpa, '*Ethical and practical challenges in implementing informed consent in HIV/AIDS clinical trials in developing or resource-limited countries' SAHARA: Journal of Social Aspects of HIV/AIDS Research Alliance*, *6*(2), 2009, 46-57-<https://journals.co.za/doi/abs/10.10520/EJC64406> on 5 March 2023.
[31] Woodsong and Karim, *'A model designed to enhance informed consent: experiences from the HIV prevention trials network. American journal of public health'* 2005, 412-419.<https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2004.041624> on 5 March 2023.

research and lack of the same results is a major contribution to privacy violations of data subjects.[32] Ronald Bayer on the other hand argued that written informed consent for groups with sensitive personal data such as PLHIV patients has been subjected to furious debate over what a rational and ethical screening policy entails. [33]Bayer based his argument on the view of abolition of written informed consent with maintenance of the oral one since according to him personal medical information requires oral consent by data subjects which is sufficient. The weakness of this concept is that there is often an inherent power imbalance between individuals and the entities conducting surveillance, such as governments or large corporations. This power asymmetry can pressure individuals into consenting to surveillance even when they may not feel comfortable or fully informed. Applicability of the informed consent concept to the research questions in this study is that it ensures transparency and accountability in data sharing practices. By providing individuals with clear and comprehensive information about how their sensitive personal data will be used, shared, and stored, data processors demonstrate respect for the principle of informational self-determination and promote transparency in their data sharing activities.

1.8.2 Autonomy-Based Justifications of informed Consent

Faden and Beauchamp establish an unbreakable connection between consent and the idea of respect for autonomy by characterizing the granting of consent as a particular type of autonomous action in the first meaning. [34]This institutionalization of informed consent in the legal domain does, in fact, provide formidable obstacles to any philosophical study of the subject. [35]The law demands more tangible conceptions that can be evaluated and consistently applied in litigation, as noted by Ashcroft. The relationship between informed consent and autonomy is straightforward; to provide informed consent entails making a certain kind of autonomous decision, a decision to authorize a

---

[32] Bayer, Philbin, and Remien, R.H, '*The end of written informed consent for HIV testing: not with a bang but a whimper' American journal of public health*, *2017*,1259-1265-<https://ajph.aphapublications.org/doi/abs/10.2105/AJPH.2017.303819> on 5 march 2023.

[33] Wing, *'Effects of written informed consent requirements on HIV testing rates: evidence from a natural experiment. American journal of public health', 2009*,1087-1092-<https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2008.141069> on 5 March 2023

[34] Kennedy, Goggin and Nollen, 'Adherence *to HIV medications: Utility of the theory of self-determination. Cognitive therapy and research*' *2004*, 611-628-<https://link.springer.com/article/10.1023/B:COTR.0000045568.95219.e2>on 5 March 2023.

[35] Lynam, Catley, Goggin, Rabinowitz, Gerkovich, Williams, Wright, and MOTIV, 'Autonomous regulation and locus of control as predictors of antiretroviral medication adherence' *Journal of health psychology*, *2009*, 578-586-<https://journals.sagepub.com/doi/abs/10.1177/1359105309103577?journalCode=hpq> on 5 March 2023.

particular medical treatment or data sharing. [36]The positive obligation imposed by the requirement to obtain informed consent can be understood to amount to an obligation to aid in facilitating autonomous decision-making, and the negative obligation to ensure that medical interventions do not involve the infringement of rights that have not been waived by their holders. [37]Thus, insofar as the process of informed consent aids in people's ability to determine whether to approve medical operations therefore, informed consent in its original sense may endorse autonomous decision-making.

1.9 RESEARCH METHODOLOGY

The nature of research in this study will be qualitative. The main sources of data will be secondary sources such as books, articles and reports. The study will also utilize primary sources such as the Data Protection Act (2019), Data Protection General Regulations, ODPC guidance note on the processing of Health Data and relevant case law [38]to showcase the practicality of the gap in the application of the principle of informational self-determination. In general, a deductive approach will be preferred with the chapters thus setting up a premise, from which the claim will be derived. Following this, the first chapter seeks to explain the origin and rationale behind the principle of informational self-determination and autonomy and whether sec 45 of the DPA applies it. This rationale will thus be the basis in analyzing the rights of data subjects to attain absolute control of their sensitive personal data and whether it maintains the aim of this principle.

I intend to analyze the origin and rationale behind the principle of informational self-determination through a historical analysis. This will mainly be done through articles, books and other scholarly sources that have an account of this history. [39]This study will then proceed to showcase why the unclear legislative framework on data sharing of sensitive personal data contributes to misuse and

[36] Kennedy, Goggin and Nollen, 'Adherence *to HIV medications: Utility of the theory of self-determination. Cognitive therapy and research*' *2004*, 611-628-<https://link.springer.com/article/10.1023/B:COTR.0000045568.95219.e2>on 5 March 2023.

[37] Barbara Akinyi, 'laws, policies and the right to privacy for PLHIV in Kenya' Unpublished LLB Dissertation, University of Nairobi, Nairobi,2019,40.

[38] Gunderson, M, 'Justifying a principle of informed consent: A case study in autonomy-based ethics. Public Affairs Quarterly',1990, 249-<https://www.jstor.org/stable/40435751> on 5 March 2023.

[39] Gunderson, M, 'Justifying a principle of informed consent: A case study in autonomy-based ethics. Public Affairs Quarterly',1990, 249-<https://www.jstor.org/stable/40435751> on 5 March 2023.

abuse of the data resulting to violations of rights and freedoms. In order to do so, an analysis of the legislative framework surrounding data sharing will be utilized. This will also entail an analysis and critique of the determined cases where the legislative framework was insufficient and resulted in violation of rights and freedoms of data subjects. Additionally, scholarly interpretation of the said cases will be analyzed to showcase the gaps and shortcomings of the legal provisions surrounding data sharing of sensitive personal data. This will therefore follow a discussion on the MIDATA model which has been used by jurisdictions such as the UK to evade privacy problems and ensure control over personal data.

Finally, this study will, in general, utilize the deductive approach with the first two chapters setting up a premise each, from which the main claim will be derived.

1.10 CHAPTER BREAKDOWN

Chapter one is an introductory part of the study. It lays down the research objectives and subsequent research questions.

Chapter two will discuss the aim or justification of section 55 (2) of the DPA with relation to data sharing of sensitive personal data. This Chapter will also discuss the relevant laws proximate to the research problem. The second part of this chapter will answer the first research question. This will further illustrate the need for the provision of informational self-determination principle in the Data Protection Act 2019. This Chapter will conclude by proposing to institutional actors, specifically the legislature and the Ministry of Health a sound definition of personal autonomy with regards to data sharing of sensitive personal data. This will be partnered up with chapter three that will seek to delve into the duty to inform as a pre-requisite for application of the principle of informational self-determination in the legislative framework.

Chapter four will discuss the legislative attempts made to ensure facilitation of data sharing of sensitive personal data. This will include a comparative analysis of the UK's data protection framework through a discussion of the problem of asymmetrical access of personal data between consumers and businesses. The discussion will be followed by an analysis of the adoption of the MIDATA model by the UK government to reduce misuse and abuse of sensitive personal data.

Chapter five will entail a brief overview of the research in totality. It will also involve a summary of the findings, recommendations and conclusion to the study.

CHAPTER TWO: WHAT IS THE CONCEPTUAL FOUNDATION OF THE PRINCIPLE OF INFORMATIONAL SELF-DETERMINATION IN THE LEGAL FRAMEWORK IN KENYA?

2.1 Introduction

This Chapter intends to answer the first research question that relates to discussing the principle of informational self-determination in data sharing of sensitive personal data. The first section will highlight the applicable laws in this case by pointing out the legislative texts under which this discussion falls under. Consequently, it will attempt to analyze sec 55(2) of the DPA and determine whether it entrenches the informational self-determination principle adequately through a brief analysis of excluded rights such as ownership and right to access. Then, it will highlight other discussions that attempt to define fundamental concepts that are backbone to the principle of informational self-determination such as personal autonomy. This will be followed by a brief discussion of these concepts. Lastly, it will conclude the discussion.[40]

2.2 Applicable laws

Article 31 of the Constitution of Kenya recognizes the right to privacy as a fundamental human right in Kenya, protecting individuals from unwarranted intrusions into their personal affairs. It also sets out the circumstances under which limitations on this right may be permissible, provided they are prescribed by law and necessary in a democratic society for specified purposes such as public safety or the protection of rights and freedoms. [41]The DPA on the other hand under section 31, outlines various provisions aimed at safeguarding individuals' privacy rights in relation to the processing of personal data. It covers aspects such as the requirement for lawful and fair processing of personal data, limitations on data sharing, and measures to ensure data security and confidentiality. [42] The DPA under sec 45 further states grounds for processing sensitive personal data of data subjects mentioning a requirement of consent to ensure protection

[40] Article 31, *Constitution of Kenya* (2010).
[41] Section 31, Data Protection Act (Act No 24 of 2019).
[42] Thouvenin, '*Informational Self-Determination: A Convincing Rationale for Data Protection Law*?' 2021, 246-< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4521552#:~:text=Florent%20Thouvenin,-University%20of%20Zurich&text=European%20data%20protection%20law%20rests,convincing%20and%20promising%20at%20first> on 10 August 2023.

of the data owners privacy. However, the Act does not seem to expressly clarify on the justification for indirectly processing the data without involving the data subject. There exists no inclusion of specific rights of the data subjects in this provision to ensure absolute control of their sensitive personal data. This is because the Act only provides a generalization of grounds for processing of sensitive personal data with exclusion of mandatory rights such as informational self-determination of the data subjects. [43] Section 55 (2) provides for a data sharing code that is issued between public sector agencies, this excludes the involvement of data subjects in consenting to the sharing of their data.

Lastly, there exists exclusion of fundamental principles in the legal provision on data sharing which will be discussed in subsequent parts of this Chapter.

2.3 DECONSTRUCTION OF INFORMATIONAL SELF-DETERMINATION

2.3.1 Informational self-determination as a principle

Informational Self-determination is an underlying rationale of the fundamental right to the protection of sensitive personal data. [44]Acknowledging such a right essentially means that the state may not require citizens to provide information about themselves and government institutions or agencies may not use such information without a sound legal basis. This ideally results in no misuse and abuse of sensitive personal data processed by these public actors. [45]In Kenya for instance, most data sharing activities by public and private actors are not based on data subjects consent but on the legitimate interests of the controller. [46]This is clearly seen in sec 45 of the DPA which provides grounds of processing sensitive personal data stating that the act of a data subject 'manifestly' making their data public is sufficient reason to allow indirect processing of their data without their involvement. [47]In addition to this, the section continues to

[43] Section 55 (2), Data Protection Act (Act No 24 of 2019).
[44]Thouvenin, '*Informational Self-Determination: A Convincing Rationale for Data Protection Law*?' 2021, 246-< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4521552#:~:text=Florent%20Thouvenin,-University%20of%20Zurich&text=European%20data%20protection%20law%20rests,convincing%20and%20promising%20at%20first> on 10 August 2023.
[45] Section 45, *Data Protection Act* (Act No 24 of 2019).
[46] Section 45, *Data Protection* Act (Act No 24 of 2019).
[47] Section 45, *Data Protection Act* (Act No 24 of 2019).

provide for data controllers rights which is contradictory as a data controller does not have rights in the same way as the data subject but rather has obligations to ensure no violation of their rights and freedoms in processing of their data. The data relation between data subjects and private/public actors is hardly ever based on exercising the principle of informational self-determination. This chapter will provide a normative analysis which demonstrates that informational self-determination principle can be reconciled with the personal autonomy principle and there exists a resulting need to provide a justification for granting data subjects a right that requires the actors to control how they process their data. Even though data is a public good, informational self-determination ought to be awarded to data subjects with sensitive personal data as a fundamental right to ensure non violation of their rights and freedoms. The next section will discuss individual agency as a concept that encompasses the ability of data subjects to exercise control over their data through incorporation of personal autonomy and privacy rights.

2.4 Individual Agency

This overarching concept encompasses the ability of data subjects to exercise control over their sensitive personal data and make autonomous decisions regarding its processing. This concept is further categorized into personal autonomy and privacy. Personal autonomy emphasizes individuals' rights to self-determination and freedom of choice, while privacy concept focuses on protecting individuals from unauthorized intrusion into their personal data.

2.4.1 What is the relationship between Personal Autonomy and informational self-determination principle?

This part explores the concept of personal autonomy in the context of patients' control over their data, emphasizing the ethical, legal, and practical aspects of this vital principle and relates it to informational self-determination principle. Personal Autonomy is an individual’s ability to

conduct activities without concern of or actual observation. [48]This concept has its origin in ethnic and political literature to explain liberty and rights of persons in the context of absolute control and self-determination of personal matters. Liberty presumes an autonomy of self that includes freedom of thought, expression and absolute control of private matters. Personal autonomy of data subjects in relation to data sharing is a fundamental ethical concept. It emphasizes the rights of individuals to have control over their own health information and plays a crucial role in ensuring patient privacy, trust, and informed decision-making.

Healthcare stakeholders such as data processors have an obligation of upholding these principles to build and maintain trust with data owners and to ensure ethical and patient-centered care. [49]Personal autonomy is critical in understanding the principle of informational self-determination. [50]This is due to the instrumental character of informational self-determination principle, as the two are inextricably linked and cannot be comprehended without the other. Personal autonomy is thus only applicable when specific provisions to protect data subjects' rights are in place, thereby avoiding unwarranted intrusions and privacy violations because the data subjects are aware of their rights in the context of data sharing. In an age where medical information is increasingly digital and processed among various stakeholders, it is crucial to uphold the autonomy of patients regarding their health data.

2.4.2 Data Ownership

In the digital age, data has emerged as a crucial asset, driving innovation, commerce, and societal development. With the proliferation of data-driven technologies, the question of data ownership has become increasingly pertinent. Data ownership rights delineate the rights and responsibilities of individuals and entities regarding the data they generate, collect, and use. In Kenya, the Data

[48] Guyer, '*Kant on the theory and practice of autonomy. Social philosophy and policy*', 2003, 98-< https://www.cambridge.org/core/journals/social-philosophy-and-policy/article/abs/kant-on-the-theory-and-practice-of-autonomy/78DE2DC254F543F996798A5C48B8B978> on 11 August 2023.

[49] Habermas, 'Human rights and popular sovereignty: The liberal and republican versions' *Ratio Juris*, 1994, 13-< https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-9337.1994.tb00162.x> on 12 August 2023.

[50] Habermas, 'Human rights and popular sovereignty: The liberal and republican versions' *Ratio Juris*, 1994, 13-< https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-9337.1994.tb00162.x> on 12 August 2023.

Protection Act of 2019 provides a legal framework for data protection, but the issue of data ownership remains inadequately addressed, particularly in Section 55(2) of the Act. Data ownership refers to the legal rights and control individuals or entities have over data that they create, possess, or control. It encompasses the right to determine how data is collected, processed, stored, and shared. Data ownership rights typically include the right to access, modify, transfer, and delete data. These rights are essential for safeguarding individual autonomy, privacy, and dignity in an increasingly data-centric society.[51] This concept asserts that individuals have the right to ensure control over their data including sensitive personal data. Data ownership is the manifestation of personal autonomy, empowering individuals to assert control over their personal information.[52] Patients have the right to make informed decisions about their healthcare, and this right hinges on their ability to control access to their medical data. Furthermore, data ownership aligns with the ethical principles of privacy and confidentiality. Patients share sensitive medical details with healthcare providers, trusting that their information will remain confidential. Respecting data ownership ensures that this trust is upheld, fostering open and honest communication between patients and providers. [53]Data ownership upholds individuals' rights to control their health information, make informed decisions about their healthcare, and maintain the privacy and confidentiality of their medical records. Ethical principles, legal protections, and practical measures all converge to safeguard data ownership and, by extension, personal autonomy in healthcare. [54]

The Legislative framework surrounding data sharing of sensitive personal data however fails to accord data subjects individual data ownership rights. The DPA outlines grounds for processing sensitive personal data while excluding the duty to inform the data subjects of the processing of their sensitive data. This exposes the data subject to risks of misuse and abuse of their data. The DPA further in sec 55(2) provides for a data sharing code that is issued between public actors and government departments and this undermines the data subject's ownership rights as their

[51] Fracassi, '*C. and Magnuson, W. Data autonomy*',2021,327< https://scholarship.law.vanderbilt.edu/vlr/vol74/iss2/6/> on 13th December 2023.
[52] Fracassi, '*C. and Magnuson, W. Data autonomy*',2021,327< https://scholarship.law.vanderbilt.edu/vlr/vol74/iss2/6/> on 13th December 2023
[53] Fracassi, '*C. and Magnuson, W. Data autonomy*',2021,327< https://scholarship.law.vanderbilt.edu/vlr/vol74/iss2/6/> on 13th December 2023
[54] Sec 55(2), Data Protection Act (Act No 24 of 2019).

sensitive personal data is shared between these agencies without their involvement. This exclusion of data ownership rights from the Data Protection Act has significant implications. Firstly, it leaves a legal vacuum concerning the rights and responsibilities of data stakeholders, potentially leading to conflicts of interests and exploitation. Without clear data ownership rights, individuals may lose control over their sensitive personal data, exposing them to privacy violations. Furthermore, the absence of data ownership undermines innovation and economic growth by disincentivizing data sharing. Inadequate protection of data ownership rights discourages individuals and organizations from investing in data-driven initiatives, fearing unauthorized use or misappropriation of their data.

Stakeholders involved in data sharing face uncertainty regarding their rights and responsibilities. Data processors may be unsure about the extent to which they retain control over their data once shared, while data subjects may be uncertain about their rights to use and process the shared data. This uncertainty can result to disputes, reluctance to share data and inhibit collaboration among stakeholders. There also exists the risk of data exploitation and misuse. Data shared without clear ownership rights outlined in the Act may be used for purposes not originally intended or in ways to violate the privacy rights of data subjects.

2.4.3 What is the role of Privacy?

Privacy ensures that individuals can exercise control over their personal information, including their health data. When it comes to healthcare, patient data often comprises sensitive details about a person's physical and mental well-being. [55]Protecting the privacy of this data is paramount to respecting an individual's autonomy. Respecting patient privacy is not merely a legal or technical requirement; it is deeply rooted in ethical principles. Moreover, privacy also links to the ethical principles of beneficence and non-maleficence. It is essential to balance a patient's autonomy with the duty of healthcare professionals to provide the best possible care. Striking this balance often

[55] Makulilo, ' Privacy and data protection in Africa: a state of the art. International Data Privacy Law' 2012,163-178-< https://www.researchgate.net/publication/273026565_Privacy_and_data_protection_in_Africa_a_state_of_the_art> on 12 August 2023.

leads to shared decision-making, where patients are active participants in their healthcare choices, thus reinforcing their autonomy.

Privacy is an indispensable concept of informational self-determination principle that ensures individuals retain control over their health data, allowing them to make informed decisions about their healthcare. Ethical principles, legal protections, and practical measures all converge to safeguard patient privacy and, by extension, their autonomy. [56]Public and private actors, policymakers, and society at large must continue to prioritize privacy to maintain the trust and dignity of patients in an increasingly data-driven healthcare landscape.

[57]Transparency is a concept relating to privacy that intersects with informational self-determination in the handling of sensitive personal data. It emphasizes the importance of clear and honest communication about data practices. Data subjects have the right to know how their data is collected, stored, and used, as well as who has access to it. [58]Transparency ensures that data subjects are informed and can make decisions in line with their values and preferences. Furthermore, transparency extends to data breaches and security measures. Data subjects should be promptly informed if their sensitive data is compromised, allowing them to take necessary actions to protect themselves. Transparency is the principle of making information readily accessible and understandable to individuals. It is a cornerstone of personal autonomy, particularly when it comes to personal sensitive data. Within the healthcare sphere, transparency implies that patients have the right to know how their medical data is collected, processed, stored, and shared. It ensures that individuals have a comprehensive understanding of the processes involved, thereby enabling them to make informed decisions about their data.[59]

---

[56] Guyer, '*Kant on the theory and practice of autonomy. Social philosophy and policy*', 2003, 98-< https://www.cambridge.org/core/journals/social-philosophy-and-policy/article/abs/kant-on-the-theory-and-practice-of-autonomy/78DE2DC254F543F996798A5C48B8B978> on 11 August 2023.

[57] Hert and Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' *Privacy and the criminal law*,2006,61-104-< https://research.tilburguniversity.edu/en/publications/privacy-data-protection-and-law-enforcement-opacity-of-the-indiviual> on 20 August 2023.

[58] Hert and Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' *Privacy and the criminal law*,2006,61-104-< https://research.tilburguniversity.edu/en/publications/privacy-data-protection-and-law-enforcement-opacity-of-the-indiviual> on 20 August 2023.

[59] Guyer, '*Kant on the theory and practice of autonomy. Social philosophy and policy*', 2003, 98-< https://www.cambridge.org/core/journals/social-philosophy-and-policy/article/abs/kant-on-the-theory-and-practice-of-autonomy/78DE2DC254F543F996798A5C48B8B978> on 11 August 2023.

The principle of autonomy on the other hand underscores that individuals have the right to make decisions about their own healthcare. This principle hinges on having access to accurate information and the assurance that their personal health data will remain confidential. Both autonomy and privacy concepts are foundational to respecting individual rights, dignity, and self-determination across various domains of human interaction. Interpretations of these concepts evolve as societies grapple with new challenges posed by technological advancements and changes in social norms, requiring ongoing dialogue and thoughtful considerations. Autonomy frequently highlights an individual's right to make independent judgments. Self-determination, on the other hand, may encourage a more collaborative approach, in which public and private actors participate in a dialogue with patients to understand their values and preferences, developing a shared decision-making paradigm. [60] In the Kenyan context, the right to privacy of personal data is primarily addressed in Section 31 of the DPA. This section outlines various provisions aimed at safeguarding individuals' privacy rights in relation to the processing of personal data. It covers aspects such as the requirement for lawful and fair processing of personal data, limitations on data sharing, and measures to ensure data security and confidentiality. [61] While the latter provision may not provide a cut-clear direction as to the privacy of sensitive personal data specifically, it can be said that the privacy of data subjects extends to all actors and stakeholders in data sharing who ought to have obligations to ensure protection of the subjects rights and freedoms.

2.5 Conclusion

This Chapter has a brief introduction to attempt to delineate the legal conflict. The Chapter demonstrates the non-inclusion of major concepts in the legal provision to ensure non violation of rights and freedoms of data subjects with regards to data sharing. It then attempts to analyze the fundamental principle of informational self-determination that is lacking in the legal provision. The Chapter continues to discuss rights arising from this principle such as privacy and personal autonomy. Under this discussion, it is noted that privacy and personal autonomy rights are key concepts in ensuring effectiveness of informational self-determination principle. Lastly, it speaks on the possible effect of non-inclusion of these fundamental principles of informational self-

[60] Section 31, Data Protection Act, (Act No 24 of 2019).
[61] Section 31, Data Protection Act, (Act No 24 of 2019).

determination in the DPA. The following chapter will seek to delve into the conceptual proposition of informational self-determination rights in the legislative framework and effects of non-incorporation.

CHAPTER THREE

3.1 Introduction

The previous Chapter analyzed the principle of Informational Self-determination and fundamental concepts pertaining to it. This Chapter will respond to the second research question and will cover the conceptual proposition of Informational self-determination rights with an aim to determine whether section 55(2) fails to entrench this right due to the insufficient/unclear framework addressing data protection of sensitive personal data. Afterwards, it will analyze the effect of incorporation of concepts into the insufficient legislative framework. This will contribute to the discussions surrounding data protection of sensitive personal data in the Kenyan context. The analysis will be done in the last part before concluding.

3.2 Applicable laws and regulations

The Data Protection Act allows for processing of sensitive personal data if it necessary for the performance of a legal obligation. [62]It outlines the permitted grounds for processing sensitive personal data through establishing of a legal framework to ensure data sharing is done effectively. The provisions of the DPA are intended to serve as a cornerstone of data protection regulation with an aim of providing a robust framework for processing of sensitive personal data.[63] A framework that fails to put the data subject first will likely result in violations of their rights and freedoms. Since there exists insufficient inclusion of concepts such as obligation to inform, the adoption of this obligation will cure the problem of non-recognition of data subject's interests. It is important to include clearly in the legislative framework the obligations of a processor as well as the data subject's rights and interests. [64]A similar approach was taken in the Ireland High Court case of Data Protection commissioner v Facebook Ireland Limited and Maximillian Schrems, where the Court held that the data controller is under an obligation to inform the data subject of any action involving processing of their data. [65]The court concluded that there ought to exist an adequate level of protection that is binding and relevant for purposes of assessing obligations of the controller to the subject.

[62] Section 55, Data Protection Act (Act No 24 of 2019).
[63] Section 55, Data Protection Act (Act No 24 of 2019).
[64] Data Protection commissioner v Facebook Ireland Limited (2018), High Court of Ireland.
[65] Data Protection commissioner v Facebook Ireland Limited (2018), High Court of Ireland.

3.3 THE CONCEPTUAL INCORPORATION OF INFORMATIONAL SELF-DETERMINATION RIGHTS IN REGULATING SENSITIVE PERSONAL DATA PROTECTION IN KENYA

The conceptual proposition of Informational Self-determination rights cannot be limited to a mere recognition as a conceptual category. [66]There needs to be explicit inclusion and expression of informational self-determination rights in the process of construction of norms as a means to improve the effectiveness of fundamental rights such as privacy in the context of data sharing of sensitive personal data. [67]These rights (privacy and personal autonomy) assume greater importance especially when combined in the context of infringement of sensitive personal data sharing. [68]The current legal provisions do not meet the reasonable expectation of privacy as a general rule by not allowing the full exercise of rights such as personal autonomy of the data subject in processing of their sensitive personal data. Data sharing under the current legal framework, is an act that, priori, violates rights and freedoms of the data subjects. This section discusses conceptual incorporation of provisions that are clear, direct and sufficient discussing a number of essential things. Firstly, the interpretive criteria of what sensitive personal data in its entirety means, a list of data subjects rights in a broad sense, provisions establishing functioning of a competent autonomous authority and lastly requisitions and processing of penalties in the event the norms or rules are transgressed by data stakeholders**.** These precepts that aid effectiveness of informational self-determination rights are discussed as follows;

3.3.1 Obligation/ Duty to Inform

Data processors and controllers must adhere to strict data protection principles and ensure that personal data is processed: lawfully, fairly and in a transparent manner; that the minimum necessary data is collected and processed and for the specified purposes only; accurately; kept for

[66] Fortes, '*The right to privacy and personal data protection in Brazil: time for Internet privacy rights?*' Brussels Privacy Hub, Working Paper 2 (5), 2016, 13-< https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N5.pdf> on 12 February 2024.

[67] Fortes, '*The right to privacy and personal data protection in Brazil: time for Internet privacy rights?*' Brussels Privacy Hub, Working Paper 2 (5), 2016, 13-< https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N5.pdf> on 12 February 2024

[68] Section 55, Data Protection Act (Act No 24 of 2019).

no longer than necessary; and appropriately safeguarded. Transparency is a key principle of data protection law and the obligation to inform is key to ensuring transparency. The purpose of this obligation is to provide data subjects with information that allows them to assess the compliance and trustworthiness of the data controller. Despite the benefits of categorizing sensitive personal data for this purpose, a coherent and consistent approach to doing so under the obligation to inform has not emerged. It is unclear what a 'category' of sensitive personal data is and when this information must be provided. This results in reduced transparency for data subjects and uncertainty for data controllers regarding their legal obligations, defeating the purpose of this obligation. However, as the de facto method of compliance with the obligation to inform (which mandates the provision of certain information about sensitive personal data sharing to individuals), privacy policies have continuously been criticized in their ability to make processing transparent. This problem makes the study of how to increase the transparency of sensitive personal data in the context of providing information to individuals about the processing of their personal data. The obligation to inform is therefore a mandatory requirement in the legislative framework on data protection of sensitive personal data. The addition of this obligation in the DPA will be essential in distinguishing the rights and interests of data subjects as well as the duties of the data processors. This ought to be clearly stated in the provision with inclusion of both data subject's rights and interests. The exemption of this mandatory concept will result in mistrust by data subjects since there is no clarity in the obligations of data controllers towards the data owners. Therefore, a framework that lacks clear inclusion of such a concept will likely be insufficient and silent in expending fundamental rights of data subjects.

3.4 Contextual Integrity Model

This subsection will discuss the contextual integrity model which focuses on how contextual factors affect the appropriateness of data sharing. The frictionless flow of health data in today's digital ecosystem has revolutionized healthcare, research, and public health activities. [69] Nissenbaum's Contextual Integrity Model emerges as a strong framework for understanding and protecting privacy in the context of health data. The Contextual Integrity Model is based on the

[69] Barth, Datta, Mitchell, J.C. and Nissenbaum's, '*Privacy and contextual integrity: Framework and applications*'. In 2006 IEEE symposium on security and privacy, 2016,15-< https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1624011&casa_token=4BOVN0kZjysAAAAA:11zehljYF96O3NbEy8NRN1jkidCMZMC4tKiDCBbPp1CDQYzp1seNVo2QPje-Ahk0veYA7bVC2g&tag=1> on 12 February 2024

premise that privacy rules vary depending on the circumstance. [70]In other words, the acceptability of data sharing is determined by their context. According to Nissenbaum's, privacy is more than just limiting data sharing; it is also about ensuring that data sharing conforms with society norms and expectations within certain situations. [71]The Contextual Integrity Model assures that data sharing follows contextual standards, balancing the requirement for data sharing with patient privacy protection. [72]This model presents a nuanced and adaptable approach to data privacy by considering the relevance of context in setting privacy expectations. In the area of health data, where sensitivity and confidentiality are crucial, using the Contextual Integrity Model preserves data subject privacy while enabling the appropriate use of data for healthcare improvements.

In legislative terms, the contextual integrity model may influence the drafting and interpretation of data protection laws that have unique requirements and considerations when it comes to the processing of sensitive personal data. The law may provide tailored provisions or guidelines for each context to ensure that sensitive personal data is handled appropriately and in accordance with the specific needs and expectations of data subjects. This model is essential in the Kenyan data protection legislation as adoption of it will result in incorporation of laws relevant in data protection of sensitive personal data.

3.5 Effect of the conceptual incorporation of these precepts on legislative framework

Given the previous discussions on the principle of informational self-determination and concepts pertaining to it, it is clear that the rights and interests of data subjects ought to be put into

[70] Nissenbaum's, 'Privacy as contextual integrity'. 2004, 119-< https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/> on 12 February 2024

[71] Barth, Datta, Mitchell, J.C. and Nissenbaum's, '*Privacy and contextual integrity: Framework and applications*'. In 2006 IEEE symposium on security and privacy, 2016,15-< https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1624011&casa_token=4BOVN0kZjysAAAAA:11zehljYF96O3NbEy8NRN1jkidCMZMC4tKiDCBbPp1CDQYzp1seNVo2QPje-Ahk0veYA7bVC2g&tag=1> on 12 February 2024

[72] Grodzinsky, and Tavani, *'Privacy in" the cloud" applying Nissenbaum's theory of contextual integrity*. Acm Sigcas Computers and Society,2006,38-47-< https://www.academia.edu/73971427/Privacy_in_the_cloud_applying_Nissenbaum_s_theory_of_contextual_integrity?ri_id=55243> on 12 February 2024.

consideration to avoid an overlap between the obligations of data processors. There is a requirement to ensure the clarification of these obligations of the data processors in the legislative framework to ensure that rights and freedoms of data subjects are not violated. Subsequently, there have been academic discussions on relevant models such as the contextual integrity model that have been used by jurisdictions to ensure effectiveness of data protection frameworks. Nissenbaum, for example, argues that privacy is more than just limiting data sharing and that it involves ensuring that data sharing conforms with society norms and expectations within certain situations. As such, there is an over emphasis on discussions surrounding the protection of sensitive personal data through incorporation of models that enhance the development of data protection laws. This also includes adoption of specific concepts in the legislative framework to ensure no violation of data subjects rights and interests.

3.6 Conclusion

In Conclusion, this Chapter has analyzed the conceptual incorporation of informational self-determination rights in regulating sensitive personal data protection in Kenya. It first started by providing an analysis of relevant and applicable laws. With this, it analyzed the obligation or duty to inform as a requirement in the data protection legislative framework. This discussion was followed by a brief overview of the contextual integrity model and its legal nature with relation to data protection of sensitive personal data. The discussion was then concluded by a detailed analysis of the effects of the incorporation of these concepts in the legislative framework.

CHAPTER 4: AN APPROPRIATE FRAMEWORK TO BE ADOPTED FOR INTERPRETATION OF PRINCIPLE OF SELF-DETERMINATION AND AUTONOMY

4.1 Introduction

Having looked at the conceptual incorporation of self-determination rights in the legislative framework in Chapter 3, this Chapter will look at the legislative attempts made to ensure facilitation of data sharing of sensitive personal data. This analysis will begin by discussing why UK is a proper comparator to Kenya. This will include a detailed analysis with reasons of why UK is relevant in the comparative analysis. The Chapter will continue to discuss the problem of privacy violations in data sharing faced by both Kenya and UK. This will be followed by a discussion on the Data Sharing Statutes in Kenya and UK and their impact.

4.2.1 Why UK is a proper comparator to Kenya

Information Technology has advanced over the years resulting to easier processing of personal data. Data sharing of sensitive personal data has been recognized to encompass common problems of distrust among data subjects across the globe. Therefore, the issue of Data protection of sensitive personal data has attracted necessitated reactions from both Kenya and UK besides their slight political and legal differences. UK enjoys benefits such as full compliance with EU Data protection laws with willingness to enter into a legally binding agreement to guarantee effective future enforcement of rules and regulations. This poses a great advantage since UK is committed to similar high standards of Data protection as the European Union. This jurisdiction is therefore comparable to the Kenyan regime.

4.2.1.1 The problem of privacy violations in data sharing as faced by both Kenya and UK

The development of Information Technology has raised a common set of fears among states that are crucial to individual rights and liberties being compromised. Research shows that sensitive personal data has been misused and abused by data processors in Kenya due to the insufficiency in the legislative framework on data protection. [73] The issue became greatly prevalent in 2015 when a directive was issued by the President to collect and process sensitive personal data of data subjects with HIV/AIDS. Shortly after, Kenya passed the DPA which provided for relevant

[73] KELIN and 3 others v Cabinet Secretary Ministry of Health and 4 others [2016] eKLR

requirements of data sharing of sensitive personal data under sec 55 (2) of the act. This section lists the grounds of processing sensitive personal data but is contradictory and unclear on the rights of the data subjects and obligations of data processors to the data owner.

The global concerns around data protection of sensitive personal data increased and the UK joined in the list of governments across the word that advanced the legislative framework surrounding data protection of sensitive personal data. [74] In 2017, Google's Artificial Intelligence Company, DeepMind, was exposed to having obtained sensitive personal data records of 1.6 million patients on an inappropriate legal basis meaning that the patient record/processing was not for direct care. The Information Commissioner's Office in UK determined that the legislative framework on data protection ought to be amended to avoid violations of rights and freedoms of data subjects.

4.2.1.2 Data Sharing statutes in Kenya and UK

Kenya's response to exposure of data subject's sensitive personal data after the 2015 incident was section 55 (2) of the DPA. The section seeks to provide listed grounds for processing of sensitive personal data through establishing of a legal framework to ensure data sharing is done effectively. The listed grounds however [75]have been criticized widely for their vague nature and inconsistent with international principles of data protection .

In UK, with the rise in public complaints on data violation of personal data, a legislative framework was introduced to reduce violations of data subject's rights and freedoms and allowed absolute control of personal data by the data owners. The Information Commissioner's Office stated that the law surrounding data protection ought to provide inclusion of the rights of the data subject and clearly outline the obligations of the data processors.

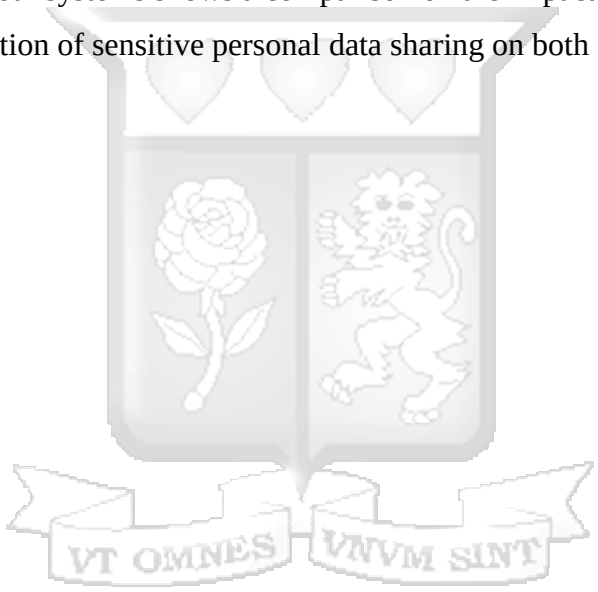
4.2.1.3 The impact of Data Sharing statutes in Kenya and UK

The Kenyan Data Protection Regime has resulted in a number of opposition and criticism for its insufficiency and inaccuracy. The relevant sections provided in the DPA are deemed contradictory

[74] Hodson, '*DeepMind and Google: the battle to control artificial intelligence*' *The Economist, ISSN*, pp.0013-0613, 2019-< https://www.economist.com/1843/2019/03/01/deepmind-and-google-the-battle-to-control-artificial-intelligence> on 13 February 2024.
[75] Section 55, Data Protection Act (Act No 24 of 2019).

and unclear to their aims. [76] An illustration is section 30(1) which fails to define what constitutes public interest in the processing of personal data, while sec 45 on the other hand fails to outline clear grounds to enforce the protection of sensitive personal data.[77] The High Court stated that the legislative framework is contradictory and would result to more violations. On the other hand, UK Government advocated for new forms of data sharing laws that guarantees the data subject absolute control over their sensitive personal data and this involved incorporation of a system known as the MIDATA model in the legislative framework. This model is designed with transparency and modularity characteristics that ensures that the data subjects is able to monitor how their data is processed by public and private actors.

The difference between both systems shows a comparison on the impact of insufficient legislative framework on data protection of sensitive personal data sharing on both countries and how Kenya is lacking.



[76] Section 30, Data Protection Act (Act No24 of 2019).

[77] KELIN and 3 others v Cabinet Secretary Ministry of Health and 4 others [2016] eKLR

CHAPTER FIVE: CONCLUSION

5.1 Introduction

This Chapter reflects the findings of the study as developed in the previous Chapters. Two recommendations will be made in this Chapter that will improve the legislation of Data Sharing. This Chapter will then conclude the research paper.

5.2 Summary of Findings

5.2.1 Chapter 1

Chapter one formed the basis of the research with establishing a clear understanding of these principles. The Chapter also laid out objectives of the research, establishing specific research questions to be researched, reviewed relevant literature, and laid out the conceptual framework of the study. The first research question ought to discuss whether the provisions of the Data Protection Act 2019 are sufficient and adequate with relation to protection of data subject's sensitive personal data.

5.2.2 Chapter 2

Chapter two discussed the relevant laws proximate to the research problem. The Chapter attempted to discuss the legal problem of whether the legislature surrounding data sharing of sensitive personal data was sufficient. The chapter further examined sec 45 and 55(2) of the DPA and attempted to determine whether it is inadequate on data sharing of sensitive personal data. This Chapter has a brief introduction to attempt to delineate the legal conflict. The Chapter demonstrates the non-inclusion of major concepts in the legal provision to ensure non violation of rights and freedoms of data subjects with regards to data sharing. It analyzes the fundamental principle of informational self-determination that is lacking in the legal provision. The Chapter continues to discuss rights arising from this principle such as privacy and personal autonomy. Under this discussion, it is noted that privacy and personal autonomy rights are key concepts in ensuring effectiveness of informational self-determination principle. The Chapter concluded the discussion by speaking on the possible effect of non-inclusion of these fundamental principles of informational self-determination in the DPA. This Chapter further determined that there is non-

inclusion of self-determination principles in the legal provisions surrounding data sharing of sensitive personal data therefore exposing data subjects to violations of their rights and freedoms.

5.2.3 Chapter 3

Chapter three examined the second research question and covered the conceptual proposition of Informational self-determination rights with an aim to determine whether section 55(2) fails to entrench this right due to the insufficient/unclear framework addressing data protection of sensitive personal data. The Chapter also analysed the effect of incorporation of concepts into the insufficient legislative framework. This Chapter responded to the second research question and determined that the insufficient legislative framework has resulted to non-incorporation of informational self-determination rights in data sharing provisions.

5.2.4 Chapter 4

Chapter 4 discussed the legislative attempts made to ensure facilitation of data sharing of sensitive personal data. This analysis began by discussing why UK is a proper comparator to Kenya. This included a detailed analysis with reasons of why UK is relevant in the comparative analysis. The Chapter also discussed the problem of privacy violations in data sharing faced by both Kenya and UK. This was followed by a discussion on the Data sharing statutes in Kenya and UK and their impact. This Chapter responded to the third research question and determined that there is need for amendment of the legislative framework surrounding data sharing of sensitive personal data in Kenya.

5.3 Recommendations

5.3.1 Legislative Recommendations

I. Firstly, at the legislative level, there is need to revisit the Data Protection Act 2019 in a bid to reflect the proposed interpretation of informational self-determination as a right and personal autonomy right. This is because this legislature is silent on interpreting what these rights means with relation to data sharing of sensitive personal data and the surrounding framework to ensure data is protected. The legislature should therefore adopt and apply these proposed principles given in the first recommendation in the interpretation section of the Data

Protection Act 2019. The inclusion of this will address the problem of uncertainty and lack of clarity as it will serve as a guiding framework which the legislature can use in determining how the sensitive personal data of data subjects will be handled.

II The second recommendation at this level is the inclusion of clear provisions on the grounds of processing sensitive personal data. This includes incorporation of the duty/obligation to inform in the provision. This is essential to distinguish clearly the rights data subjects have against the obligations of data processors. This will assist in recognition of the rights of data subjects by the data processors and will ultimately result in reduced breaches. These obligations also demonstrate accountability and transparency in data sharing practices. This includes maintaining records of data sharing activities, conducting regular audits and assessments, and providing clear and accessible information to data subjects about data sharing arrangements, risks, and safeguards.

III The final recommendation at this level is that there is need to revisit the General Data Protection Guidelines and adopt several data subject's rights. This is essential to ensure that the data subject is aware of their right in the handling of their sensitive personal data**.** The amended legislation should reinforce core data protection principles, such as data minimization, accuracy, integrity, and confidentiality, in the context of data sharing activities involving sensitive personal data. Data controllers and processors should be required to adhere to these principles throughout the data sharing lifecycle, from collection to deletion or disposal.

5.3.2 Judicial Recommendations

The judiciary should interpret the existing data protection laws, such as the Data Protection Act of Kenya 2019, to clarify the legal obligations of data controllers, processors, and recipients when sharing sensitive personal data. This includes defining the scope of sensitive personal data and outlining specific requirements for obtaining consent, ensuring data security, and implementing safeguards to protect individuals' privacy rights. Judicial decisions should establish precedents that reinforce the importance of protecting sensitive personal data in accordance with constitutional rights to privacy and data protection. Precedents can provide clear guidance on legal standards and principles governing data sharing practices, deterring unlawful

or negligent conduct by data stakeholders and promoting accountability. The judiciary should also enhance its capacity to adjudicate data protection disputes effectively by providing specialized training to judges, magistrates, and legal practitioners on data protection laws, emerging technologies, and international best practices. This will enable the judiciary to adjudicate complex data protection cases with competence and expertise, ensuring fair and impartial resolution of disputes.

5.3.3 Administrative Recommendations

Administrative authorities should require organizations to conduct robust Data Protection Impact Assessments (DPIAs) before engaging in data sharing activities involving sensitive personal data. DPIAs should assess the potential risks to individuals' privacy and data protection rights, evaluate the necessity and proportionality of data sharing, and propose measures to mitigate risks and enhance compliance with data protection laws. Administrative bodies should also establish standardized data sharing protocols and procedures to facilitate secure and compliant sharing of sensitive personal data among authorized entities. These protocols should outline requirements for data governance, access control, encryption, data anonymization, and audit trails to ensure transparency, accountability, and data security throughout the data sharing lifecycle.

5.3.4 Institutional Recommendation

The DPA, in collaboration with relevant stakeholders, should develop sector-specific guidelines and standards for data sharing practices involving sensitive personal data. These guidelines should provide clear and practical guidance tailored to specific industries, outlining legal requirements, best practices, and risk mitigation strategies to ensure compliance with data protection laws. The DPA should promote the adoption of Privacy Impact Assessments (PIAs) by organizations engaged in data sharing activities involving sensitive personal data. PIAs should assess the potential privacy risks and impacts of data sharing initiatives, identify measures to mitigate risks and enhance compliance with data protection laws, and involve stakeholders in the decision-making process. Organizations involved in data sharing activities should designate Data Protection Officers (DPOs) responsibility for overseeing data protection compliance and facilitating communication with regulatory authorities and data subjects.

5.4 Conclusion

In summary, this study has found that there is a lack of understanding of the duty to inform, informational self-determination and personal autonomy rights. This is further illustrated in the provisions of the Data Protection Act 2019 that outlines rules governing data sharing. This study has also identified various concepts that can be used to understand the fundamental rights and principles in the data sharing sphere. From this, it is evident that adoption of the recommendations will result in a reduction if not completely resolving the problem of data sharing of sensitive personal data without their consent, and eventually reduce misuse and abuse by private and public actors.

BIBLIOGRAPHY

Journal Articles

Makulilo, A.B. Privacy and data protection in Africa: a state of the art. International Data Privacy Law, 2(3), 2012, pp.163-178.

Guyer, P.' Kant on the theory and practice of autonomy. Social philosophy and policy', 20(2),2003, pp.70-98.

De Hert, P. and Gutwirth, S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. Privacy and the criminal law,2006, pp.61-104.

Guyer, P.' Kant on the theory and practice of autonomy. Social philosophy and policy', 20(2), 2003, pp.70-98.

Fracassi, C. and Magnuson, W. Data autonomy. Vand. L. Rev., 74, 2021, p.327.

Sandman, L. and Munthe, C. *'Shared decision-making and patient autonomy'. Theoretical medicine and bioethics*, *30*, 2009, pp.289-310.

Falagas, M.E., Korbila, I.P., Giannopoulou, K.P., Kondilis, B.K. and Peppas, G. 'Informed consent: how much and what do patients understand?'. *The American Journal of Surgery*, *198*(3), 2009, pp.420-435.

Habermas, J. Human rights and popular sovereignty: The liberal and republican versions. Ratio Juris, 7(1) 1994, pp.1-1

Rashad, A.M., Phipps, F.M. and Haith-Cooper, M. 'Obtaining informed consent in an Egyptian research study. *Nursing ethics', 11*(4),2004, pp.394-399.

Fisher, P. Ethics in qualitative research: *'Vulnerability', citizenship and human rights. Ethics and Social Welfare, 6*(1), 2012, pp.2-17.

Lee L. M Heilig, CM and White, Ethical Justification for conducting public health surveillance without patient consent, The American Journal of Public Health, 2012.

Ioannidis, J.P, Informed Consent, big data and the oxymoron of research that is not research. The American Journal of Bioethics, 2013.

Woodsong, C and Karim, a model designed to enhance informed consent, experiences from the HIV prevention trials network, American Journal of Public Health, 2003.

Jomin George, Takura Bhila, Security, confidentiality and privacy in Health of Health Care Data, published in International Journal of Trend in Scientific Research and Development, Volume 3, 2019.

Thacker, SB Berkelman, The Science of Public Health Surveillance, Journal of Public Health policy, 1989.

Bayer R, Philbin M and Remien, the end of written informed consent for HIV testing, not with a bang but a whimper, American Journal of Public Health,2017.

Wing C, Effects of written informed consent requirements on HIV testing rates, evidence from a natural experiment, American Journal of Public Health, 2009.

La Guardia, J G Ryan and Deci, Within-person variation in security of attachment, a self-determination theory perspective on attachment, need fulfillment and wellbeing, Journal of Personality and social psychology, 2000.

Lwin, M Wirtz, J and Williams, Consumer Online Privacy concerns and

responses, a power responsibility equilibrium perspective. Journal of the Academy of Marketing Science,2007

Di Lorio, CT, Azzopardi, V Beck, Privacy impact assessment in the design of transnational public health information system. Journal of Medical Ethics, 2009.

Books

Shell, SM, *Kant and the Limits of Autonomy,* Harvard University Press, Cambridge, 2009, 3.

Lisa M Lee and Others, Principles and Practice of Public Health Surveillance, 3rd ed, Oxford Academic, 2010

Anna C. Mastroianni, Jeffrey P. Kahn, Nancy E. Kass, The Oxford Handbook of Public Health Ethics, 2019

Suji, '*African traditional medicine: Autonomy and informed consent*', Vol 3, Springer Cham, 2014,1-8.

Statutes

Constitution of Kenya (2010)

Data Protection Act (2019)

Data Protection (General) Regulations (2021)

Dissertations and Thesis

Barbara Akinyi, 'laws, policies and the right to privacy for PLHIV in Kenya' Unpublished LLB Dissertation, University of Nairobi, Nairobi,2019,40.

Working Papers

Fortes, '*The right to privacy and personal data protection in Brazil: time for Internet privacy rights?*' Brussels Privacy Hub, Working Paper 2 (5), 2016, 13-< https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N5.pdf

Bill

Data Protection Bill (2019)

Online Articles

Peto, Fletcher and Gilham, *'Data protection, informed consent, and research' BMJ, 2004, 1029-1030.* <*https://www.bmj.com/content/328/7447/1029.short*>

Thouvenin, '*Informational Self-Determination: A Convincing Rationale for Data Protection Law*?'2021, 246-< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4521552#:~:text=Florent%20Thouvenin,-University%20of%20Zurich&text=European%20data%20protection%20law%20rests,convincing%20and%20promising%20at%20first

Barth, Datta, Mitchell, J.C. and Nissenbaum, '*Privacy and contextual integrity: Framework and applications'*. In 2006 IEEE symposium on security and privacy, 2016,15-< https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1624011&casa_token=4BOVN0kZjysAAAAA:11zehljYF96O3NbEy8NRN1jkidCMZMC4tKiDCBbPp1CDQYzp1seNVo2QPje-Ahk0veYA7bVC2g&tag=1> on 12 February 2024

Grodzinsky, and Tavani, *'Privacy in" the cloud" applying Nissenbaum's theory of contextual integrity*.AcmSigcas ComputersandSociety,2006,38-47-<

https://www.academia.edu/73971427/Privacy_in_the_cloud_applying_Nissenbaum_s_theory_of_contextual_integrity?ri_id=55243>

Chapters in a book

Anna C. Mastroianni, Jeffrey P. Kahn, Nancy E. Kass, The Oxford Handbook of Public Health Ethics, 2019

Suji, '*African traditional medicine: Autonomy and informed consent*', Vol 3, Springer Cham, 2014,1-8.

Case Law

KELIN and 3 others v Cabinet Secretary Ministry of Health and 4 others [2016] Eklr

Data Protection commissioner v Facebook Ireland Limited (2018), High Court of Ireland.