

https://dspace.org/

The Evolution of Privacy and Data Protection in Kenya

Antony Laibuta

https://hdl.handle.net/10539/43654
DHET

Downloaded from a DSpace repository. https://dspace.org/

juta



A Journal of Legal History · Volume 30 (1) 2024



FUNDAMINA

A Journal of Legal History • Volume 30 (1) 2024

Fundamina

Year of publication: 2024

© Juta and Company (Pty) Ltd

First Floor, Sunclare Building, 21 Dreyer Street, Claremont 7708

This journal is approved by the Department of National Education for SAPSE purposes

Fundamina is available on HeinOnline at *https://home.heinonline.org/*

Online ISSN 2411-7870

Typeset by Elinye Ithuba DTP Solutions

Fundamina

A Journal of Legal History

Volume 30 | Issue 1 | 2024

Online ISSN 2411-7870

ARTICLES

A HISTORICAL OVERVIEW OF LEGISLATIVE MEASURES TO CRIMINALISE SAME-SEX RELATIONS IN SELECTED AFRICAN COUNTRIES
John C Mubangizi 1

FROM JUDICIAL MANAGEMENT TO BUSINESS RESCUE: A CRITICAL ANALYSIS OF THE MEANING AND PURPOSE OF BUSINESS RESCUE IN SOUTH AFRICA SINCE 1926
Simphiwe P Phungula 36

BEYOND LEGALITY: THE HISTORICAL DISREGARD OF THE PRINCIPLE OF LEGALITY AND ITS IMPACT ON FORCED MARRIAGE PROSECUTION IN INTERNATIONAL CRIMINAL LAW
Julian Rebecca Okeyo and Emma Charlene Lubaale 68

THE EVOLUTION OF PRIVACY AND DATA PROTECTION IN KENYA
Mugambi Laibuta. 116

IN MEMORIAM: PROFESSOR DG KLEYN (1955–2024)
Emile Zitzke. 166

EDITORIAL COMMITTEE

Honorary Editor: LC Winkel LLM LLD (Amsterdam) LLD h c (Edinb)

Editor-in-Chief: SV Hoctor BA LLB LLM (Cape Town) DJuris (Leiden) PG Dip (Latin) (Wales Trinity Saint David)

Editors: L Wildenboer (BLC LLB (UP)); Giltaij (BA MA PhD (Rotterdam)); J Coetzee BA LLB LLM LLD (Stellenbosch); P Swanepoel MA(Hons) (St Andrews) LLB (Natal) MSc PhD (Edinburgh)

Typesetter: Elinye Ithuba DTP Solutions

Cover designer: Andri Steyn (BTech (Graphic Design))

Editorial Board: W Brauneder (Vienna); E Chevreau (Paris); S Corrêa Fattori (São Paulo); M Dan Bob (Cluj-Napoca); A Domanski (Johannesburg); PJ du Plessis (Edinburgh); T Finkenauer (Tübingen); A Földi (Budapest); CM Fombad (Pretoria); JF Gerkens (Liège); JJ Hallebeek (Amsterdam); G Hamza (Budapest); DG Kleyn (Pretoria); F Longchamps de Beriér (Krakow); F Lucrezi (Naples); C Masi Doria (Naples); TAJ McGinn (Nashville); P Pichonnaz (Fribourg); D Pugsley (Exeter); AM Rabello (Jerusalem); JM Rainer (Salzburg); M Skřejpek (Prague); K Tanev (Sofia); Ph J Thomas (Pretoria); K Tuori (Helsinki); JP van Niekerk (Pretoria); DH van Zyl (Cape Town); A Wacke (Cologne)

EDITORIAL POLICY

Fundamina. *A Journal of Legal History* is a peer-refereed journal that publishes legal-historical research. In this journal, academics and practitioners from South Africa and abroad have the opportunity to exchange ideas on a wide range of legal-historical issues. The focus is on the ancient and modern, external and internal legal history of all families of law and is not limited to South or southern African legal history. Articles written in English are acceptable; articles written in other languages will be considered. As a rule, articles that have been published elsewhere, either in full or in part, are not acceptable for publication and on submission, authors should inform the editors if a contribution has already appeared in another publication, or has been offered for publication elsewhere. The editors reserve the right to alter manuscripts accepted for publication in accordance with the journal's house style, to correct errors, and to improve clarity. *Fundamina* is published twice a year. It is the mouthpiece of the Southern African Society of Legal Historians. Membership of the Society is open to all who identify with the aims of the Society, as set out in its Constitution.

For information on how to become a member of the Society or subscribing to *Fundamina*, please visit *www.legalhistory.org.za*

Annual membership fees: **R700,00** per year (Africa); **$90,00** or **€75,00** (elsewhere).

Correspondence and applications for membership should be sent to:

The Secretary, Southern African Society of Legal Historians, e-mail: *SASLH@unisa.ac.za*

GUIDELINES FOR AUTHORS

Contributions for publication and all correspondence should be sent to *svhoctor@sun.ac.za*. Authors are requested to submit manuscripts in the style set out below. The author of a contribution must please supply details of their professional or academic status for publication.

HOUSE STYLE

Language: Any contributions written in English must adhere to the UK language rules for spelling and grammar.

Format: All contributions must be submitted electronically. The text must be justified and typed in double spacing and in font Times New Roman and font size 12. Footnotes must be justified, typed in single spacing and in font size 10.

Abbreviations: Abbreviations should be avoided in the text, but used as extensively as possible in footnotes. The normal language rules apply to abbreviations, but no full stops are used.

Quotations: Quotations should be used sparingly and correctly. Quotations of less than forty words are indicated in the text by means of double quotation marks. All quotations exceeding forty words should be placed in a separate paragraph in font size 11 and indented without quotation marks. Single quotation marks are used for a quotation within a quotation. Alterations to quotations should be indicated by square brackets. Quotations are not italicised.

Headings: All headings should be numbered consecutively with Arabic numerals. No full stops are used after headings.

Italics: Quotations (including those in Latin) are not italicised. All foreign words and expressions are italicised, for example *Grundgesetz*, *fait accompli* and *dolus*.

Numbers: Write out numbers of up to one hundred. Use numerals for units of measurement, monetary values and percentages. Examples: fifty-five sheep, 3 metres, £10, R20, €10, 7 kilograms, 7 per cent.

KEYWORDS, BIBLIOGRAPHY AND ABSTRACT

All articles must be accompanied by a list of **Keywords**, a **Bibliography** and an **Abstract** in English (appr 300 words).

(1) All research materials (except cases and legislation) appear in an integrated Bibliography and are listed alphabetically: (a) ***Books***: surname/s and names/initials of the author/s, date of publication in brackets, title of book in italics, accompanied by the place of publication in brackets. Example: Cairns, J & P du Plessis (2010) *The Creation of the Ius Commune* (Edinburgh). (b) ***Articles***: surname/s and names/initials of the author/s; date of publication in brackets; title of article in double quotation marks; name of the journal written in full (except for *LJ*, *LR* and *Univ*) in italics; numbers of volumes and issues; starting and ending page numbers. Example: Benson, John (1997) "The origins of Roman legal science" *Howard LR* 34(2): 194–220. (c) ***Websites***: Example: Ndulo, B (2006) "African Economic Community and the promotion of intra-African trade" available at *http://www.einaudi.cornell.edu/Africa/ outreach/pdf/African_Economic_Community.pdf* (accessed 19 Nov 2018).

(2) ***Cases*** (listed separately and according to jurisdiction, in alphabetical order): The name of the case is italicised, and words such as "and another" are omitted. Examples: *Smit v Smit* 1977 (2) SA 304 (AD); *United Democratic Movement v President of the RSA (1)* 2002 (11) BCLR 1179 (CC). The English references to pre-1947 cases are also used in Afrikaans texts. Example: *Fennell v Bosch* 1934 NPD 142. References to English cases dating to before 1865 must include the ER reference. Please contact the editor for further details in this regard.

(3) ***Legislation*** (listed separately and according to jurisdiction, in alphabetical order): The title of a statute is not italicised. Example: Internal Security Act 74 of 1982. Only primary legislation is listed in the Bibliography. In the case of subordinate legislation, the basic form changes to the following: Procl R138 in *GG* 8331 of 6 Aug 1982.

(4) ***Archival materials and classical texts***: These do not appear in the Bibliography. References to such materials in the footnotes are in full. Please contact the editor for further details in this regard.

FOOTNOTES

In view of the fact that the Bibliography contains full particulars, abbreviated references appear in the footnotes: the author's name/authors' names, date of publication and relevant page numbers (Ankum 2014: 34). In the case of more than one publication of the same author published during the same year, "a", "b", etc are added (Silver 1987a: 18–19; Silver 1987b: 327–329).

ARTICLES

THE EVOLUTION OF PRIVACY AND DATA PROTECTION IN KENYA

Mugambi Laibuta*

ABSTRACT

The contribution looks at the right to privacy within Kenya's legal system by setting out the constitutional, legislative and jurisprudential framework on this right, as well as the right to data protection. The evolution of the rights to privacy and data protection in Kenya have been marked by significant milestones, reflecting global trends and local imperatives. The right to privacy in Kenya has featured in the constitutional text since Kenya gained independence from colonial rule. Conversations during the clamour for constitutional reforms shaped the current constitutional text that provides for an individual right to privacy and has been the springboard for the promulgation of legislation regarding data protection rights. The enactment of the Data Protection Act, 2019 was a pivotal moment, providing a legal framework for the protection of personal data. The Act emphasises the rights of individuals regarding their personal data, including the rights to be informed about the processing thereof, to access it and

* LLB (Moi University) LLM (London School of Economics and Political Sciences) PhD (University of the Witwatersrand). Advocate of the High Court of Kenya; Certified Information Privacy Manager. This contribution is based on ch 2 of my PhD thesis entitled *Adequacy of Data Protection Regulation in Kenya* (2023, University of the Witwatersrand). E-mail: *Mugambi@laibuta.com*

https://doi.org/10.47348/FUND/v30/i1a4

to its rectification. The Act also provides for baseline data protection principles and grants the Office of the Data Protection Commissioner powers to enforce data subject rights and data protection principles. Other legislation, such as the Children Act and the HIV and AIDS Prevention and Control Act, also provide privacy safeguards. For decades, the Kenyan courts have ruled in favour of the right to privacy. However, despite legislative developments, some statutes regulating national security organs still contain provisions limiting the right to privacy. This contribution describes the past and present status of the rights to privacy and of data protection in Kenya.

Keywords: Kenyan law; data protection; right to privacy; Kenyan Constitution; Data Protection Act

1 Introduction

This contribution focuses on the evolution of the right to privacy in Kenya. The approach of this study is descriptive, analytical and partly historical. It provides an exploration of the current privacy-law and, by extension, the data-protection framework in Kenya. This historical contribution matters for two main reasons. The first relates to the general importance of the study of legal history. The second relates to the gap in historical research on privacy and data protection in Kenya in particular.

It has been said that "history gives a better understanding of the background in which any idea or institution or system originated, the purposes for which they emerged, their working, factors of their success or failure, and reasons for the same".[1] This contribution therefore looks at the way in which the rights to privacy and data protection has evolved in Kenya and provides a contextual background of the constitutional and statutory origins of these rights. Hopefully, this will allow for a better understanding of how the right to privacy has been construed in Kenya since its independence from colonial rule. As argued by one scholar, "historical legal research exposes the social transformation dimension of law and gives clues for understanding the present law".[2]

A historical understanding of the right to privacy provides clarity on the state of data protection regulation in Kenya.[3]

1 Bhat 2019: 201.
2 *Idem* at 206.
3 *Idem* at 205.

https://doi.org/10.47348/FUND/v30/i1a4

This is especially relevant for the current generation of law makers, scholars, jurists and legal practitioners responsible for crafting laws that aptly fit prevailing circumstances.[4] As has been said, the present is a culmination of the past,[5] but the future must be recalibrated with an understanding of the past and of the present.[6]

It is important to note that no academic analysis has yet been done regarding the Kenyan constitutional right to privacy, the provisions of the Kenyan Data Protection Act 24 of 2019, and how they relate to the statutory provisions described below. This contribution hopes to fill this void. In addition, this study points out potential problems in the current privacy-law scheme in that country.

Privacy may be construed as either a moral or a legal right, or as both, depending on the relevant jurisdiction. Moral and legal rights to privacy have been explained as "since by nature a person has a fundamental interest in particular facets of [their] personality (such as [their] body, good name, privacy, dignity, et cetera), these interests exist autonomously *de facto*, independently of their formal recognition *de jure*".[7] This contribution focuses on the written law (*de jure*) only or, put differently, on the formal recognition of elements of the right to privacy in Kenya. The written law includes the constitutional text, legislation and judicial decisions that contain elements of the right to privacy and data protection. This study does not look at the cultural construct of privacy in Kenya, nor does it discuss privacy as a purely moral right. Kenyan society is not an ethnically homogenous one; it consists of more than forty-three ethnic groups that preserved their laws and customs through oral narratives. The scope of this study simply does not allow for an in-depth look at the various ethnic laws and customs.[8]

4 *Idem* at 207.
5 Boorstin 1941: 430.
6 Dubber 1998: 159.
7 Neethling 2005: 19.
8 Boshe, Hennemann & Von Meding 2022: 34 give a glimpse of privacy in the African context, stating that the communal nature of the African context mostly does not focus on individuals as right bearers. In other words, the allusion is that privacy may be regarded by some as an un-African concept. While this hypothesis about privacy in the African context is relevant to understanding how privacy laws are formulated in certain African contexts, one should be conscious of the problem of treating Africa as a uniform entity with no diversity. In this regard, Silungwe 2014: 28 laments the futility of a purist notion of African legal theory because of the internal contradictions

https://doi.org/10.47348/FUND/v30/i1a4

This contribution describes the development of the right to privacy within the Kenyan legal system by setting out the constitutional, legislative and jurisprudential framework that is instrumental in interrogating data protection regulation there. The purpose of this study is to provide a better understanding of the way in which the rights to privacy and data protection may ideally be protected, respected and promoted. It does so by first highlighting the constitutional provisions related to the right to privacy after Kenya became independent from colonial rule in 1963. Secondly, it identifies current legislation that protects the right to privacy or elements of the latter right. The Data Protection Act is afforded special focus as it refines privacy rights by outlining data subject rights, data protection principles, as well as the lawful processing of personal data. Thirdly, the contribution then looks at the approach of the Kenyan courts on the right to privacy.

2 The constitutional protection of privacy in Kenya since independence

Kenya won its independence from Britain in 1963. In the same year, Kenya promulgated a new Constitution, also known as the independence Constitution. Prior to that, the indigenous communities living in Kenya did not have written legal provisions on the right to privacy. Like most Commonwealth constitutions, the Kenyan independence Constitution was drafted in Lancaster in the United Kingdom and had similar provisions to the constitutions of other Commonwealth countries seeking independence after World War II.[9] It is perhaps for this reason that the right to privacy found its way into Kenya's first independent Constitution as it did in the case of other Commonwealth countries' constitutions.

There have been three constitutions governing Kenya since its independence, namely the independence Constitution enacted in 1963;[10] the post-independence Constitution that endured

that exist within African communities. This view holds that there is no singular version of what it means to be African or, for purposes of this contribution, what an African approach to privacy may involve.

9 Dale 1993: 67–83.

10 The independence Constitution endured twenty-eight amendments until its repeal in 1997. See, also, Muigai 2001: *passim*; Muigai & Juma 2022: *passim*.

https://doi.org/10.47348/FUND/v30/i1a4

decades of amendments;[11] and the current Constitution, which was promulgated on 27 August 2010. This part of the discussion demonstrates that elements of the right to privacy have become entrenched in the constitutional text since 1963.

Section 14 of the independence Constitution provided for protection of the right to privacy, while section 20 provided for protection from arbitrary search and entry. Section 14 read:

> Whereas every person in Kenya is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, tribe, place of origin or residence or other local connexion, individual, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely–
>
> (a) life, liberty, security of the person and the protection of the law;
>
> (b) freedom of conscience, of expression and of assembly and association; and
>
> (c) *protection for the privacy of his home and other property* and from deprivation of property without compensation,
>
> the provisions of this Chapter shall have effect for the purpose of affording protection to those rights and freedoms subject to such limitations of that protection as are contained in those provisions, being limitations designed to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest. [emphasis added]

On the other hand, section 20 stipulated:

> (1) Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on against his premises.
>
> (2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision–
>
> (a) that is reasonably required in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development and utilization of mineral resources, or the development or utilization of any other property in such a manner as to promote the public benefit;

11 The post-independence Constitution was repealed on 27 Aug 2010.

https://doi.org/10.47348/FUND/v30/i1a4

(b) that is reasonably required for the purpose of promoting the rights or freedoms of other persons;

(c) that authorizes an officer or agent of the Government of Kenya, or of a Region, or of the East African Common Services Organization, or of a local government authority, or of a body corporate established bylaw – for public purposes, to enter on the premises of any person in order to inspect those premises or anything thereon for the purpose of any tax, rate or due or in order to carry out work connected with any property that is lawfully on those premises and, that belongs to that Government, Region, Organization, authority or body corporate, as the case may be; or

(d) that authorizes, for the purpose of enforcing the judgment or order of a court in any civil proceedings, the entry upon any premises by order of a court,

and except so far as that provision or, as the case may be, anything done under the authority thereof is shown not to be reasonably justifiable in a democratic society.

Similarly, section 70 of the post-independence Constitution provided for protection of the privacy of the home and other property, while section 76 provided protection against arbitrary search and entry. These latter provisions therefore mirrored the provisions under the independence Constitution.

While there are no academic commentaries on these provisions, and none on the right to privacy in particular, the courts were often called upon to determine the constitutionality of searches and seizures. For example, in *Standard Newspapers Limited v Attorney General*,[12] where a search and seizure had been carried out against the petitioner, the High Court ruled "that the petitioners' rights under sections 76 and 79 of the post-independence Constitution were violated by the respondents' action of arbitrary search and seizure". In *Heiwua Auto Kenya Limited v The Office Commanding Police Division Central Police Station*,[13] the court recognised the fact that a search could be carried out within the confines of the law, referring to the same constitutional section 76. In both these cases, the courts held that where searches and seizures were carried out contrary to provisions of the criminal procedure code and police procedures, it violated the constitutional right against arbitrary

12 [2013] eKLR para 63.
13 [2010] eKLR.

https://doi.org/10.47348/FUND/v30/i1a4

searches and seizures. The two decisions demonstrate that the right to privacy were protected by the constitutional provisions and by the courts. This is notwithstanding the fact that that Constitution did not provide for an express individual right to privacy. Instead, its provisions offered protection for the privacy of individuals' home and property, as well as protection against arbitrary searches and seizures.

It was not until Kenya's clamour for constitutional change during the early 2000s that the express and broader individual right to privacy gained traction. It is not clear what caused this shift to an individual right to privacy in the constitutional text. It is submitted that the Kenyan constitutional drafters may have been influenced by the fact that international human rights instruments contain a broader right to privacy, covering more than just privacy regarding property. Hence, they may have been persuaded to include constitutional provisions that mirror such international human rights instruments. The drafters may also have been inspired by progressive constitutional frameworks on the African continent, such as the Constitution of the Republic of South Africa, 1996, which contains an individual right to privacy. Section 14 of South Africa's Constitution states:

> Everyone has the right to privacy, which includes the right not to have–
>
> a. their person or home searched;
> b. their property searched;
> c. their possessions seized; or
> d. the privacy of their communications infringed.

The phrasing of this latter provision was mirrored almost word-for-word in various draft constitutions debated in Kenya, as well as in the current constitutional provision on the right to privacy. It is submitted that international cosmopolitanism and comparative constitutional architecture may be another reason why Kenya currently has a broad constitutional provision on the right to privacy.

The 2005 final report on protection of privacy by the Constitution of Kenya Review Commission recommended that such "provision should also give general protection to privacy of the home, person, correspondence and other forms of communication. This is relevant to the behaviour of law enforcement agencies, and of fellow citizens".[14] This recommendation resulted in the

14 Constitution of Kenya Review Commission 2005: 122.

https://doi.org/10.47348/FUND/v30/i1a4

inclusion of an individual right to privacy in the various draft constitutional texts.

Since independence, Kenya has considered several draft constitutions in its quest for constitutional reform. Without fail, all these draft constitutions provided for an express individual right to privacy. They included: clause 43 of the Constitutional Amendment Bill proposed by the report of the Constitution of Kenya Review Commission in 2003;[15] clause 47 of the Constitutional Amendment Bill proposed by the National Constitutional Conference in 2004; and clause 47 of the Proposed New Constitution of Kenya, 2005 which was rejected by voters in the 2005 referendum.[16] As there was never any debate on the right to privacy clauses, it was uncertain whether the right to privacy would be included in the final constitutional text.

However, in the run up to the promulgation of the Constitution of Kenya, 2010, the proposed text on the right to privacy finally came up for debate. When the Committee of Experts on Constitutional Review submitted a proposed draft constitution to the National Assembly for consideration, the Assembly flagged the proposed clause 31, which provided for the right to privacy. The National Assembly wanted the following clauses deleted:

> Every person has the right to privacy, which includes the right not to have–
>
> (a) their person, home or property searched;
>
> (b) their possessions seized.

According to the National Assembly, "[c]lause (a) would affect security measures with regard to searches, especially in this era of terrorism" and "[c]lause (b) would complicate financial transactions as collateral for loans would be rendered useless".[17] These objections did not receive the margin of support required for adoption.[18] The proposed clause on privacy at the time read:

15 The draft Constitutional Amendment Bill was revised to come up with the Proposed New Constitution subjected to the 2005 referendum.

16 The 2004 Bill informed the text of the Constitutional Amendment Bill proposed by the report of the Constitution of Kenya Review Commission in 2003.

17 Committee of Experts on Constitutional Review 2010: 139.

18 *Idem* at 137. The Constitution of Kenya (Amendment) Act, 2008 required that for any amendment to the proposed Constitution to be adopted, it had to be supported by 65 per cent of the members of the National Assembly.

https://doi.org/10.47348/FUND/v30/i1a4

> Every person has the right to privacy and that this right includes the right to every person not to have–
>
> (a) their person, home or property searched;
> (b) their possessions seized;
> (c) information relating to their family or private affairs unnecessarily required or revealed; or
> (d) the privacy of their communications infringed.

The failure to delete clauses (a) and (b) was a good thing, since their removal would have resulted in a much watered-down constitutional right to privacy.

It should be noted that the National Assembly did not oppose the right to privacy in general terms, perhaps since the right had already formed part of the independence Constitution and the text repealed by the current Constitution.[19]

However, the current constitutional right to privacy is not absolute. For one, the right is not listed in article 25 that lists fundamental rights and freedoms that may not be limited.[20] More recently, the Constitutional (Amendment) Bill of 2020 sought to amend, among other constitutional provisions, article 31 on the right to privacy to include a provision stating that "every person has the right to privacy, which includes the right not to have their personal data infringed".[21] Had the Constitutional (Amendment) Bill been ratified, personal data protection would have been an express constitutional right. However, both the High Court[22] and the Court of Appeal[23] declared the adoption of the Bill to be unconstitutional for not having followed constitutional procedures;

19 The current Constitution was promulgated on 27 Aug 2010 after having been ratified by way of a referendum on 4 Aug 2010. More than 68 per cent of the voters approved the constitutional text, which included art 31 containing the right to privacy.

20 On limitations, art 19(3) states that "the rights and fundamental freedoms in the Bill of Rights are subject only to the limitations contemplated" in the Constitution. Article 24(1) provides that a right or fundamental freedom "shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom".

21 Constitutional (Amendment) Bill, 2020, available at *http://kenyalaw.org/kenyalawblog/wp-content/uploads/2020/10/Constitution-of-Kenya-Amendment-Bill-25-11-2020.pdf* (accessed 10 Mar 2022).

22 *David Ndii v Attorney General* [2021] eKLR.

23 *Independent Electoral and Boundaries Commission v David Ndii; Kenya Human Rights Commission* [2021] eKLR.

https://doi.org/10.47348/FUND/v30/i1a4

for not having been subjected to comprehensive public participation; and, generally, for amending what the courts deemed to be the basic structure of the Constitution. The Supreme Court eventually declared the latter constitutional amendment process to have been unconstitutional.[24]

The Constitution remains the main source of this right and has been described as "a form of scaffolding",[25] although the constitutional text is not sufficient by itself, even with a robust Bill of Rights.[26] The constitutional text ought to be supported by a rule-of-law culture, by political accountability and by an effective bureaucracy.[27] The rule-of-law culture ensures that any state action is sanctioned by the law; applies equally to all citizens and to the ruling elite; is reasonable; and is supported by the constitutional text.[28]

However, in addition to a rule-of-law culture, political accountability and effective bureaucracy, legislation plays a key role in giving effect to constitutional provisions.[29] Legislation is critical in implementing a constitution.[30] Thus, statutes on privacy are critical. Even where legislation gives effect to constitutional provisions, such legislation ought to be construed "to promote the spirit, purport and objects of both the Bill of Rights, and the specific constitutional provision(s) to which more concrete effect is given".[31] As such, statutes should "not be allowed to decrease the protection that a constitutional right affords or to infringe any other constitutional right".[32]

The next part takes a look at the Kenyan statutes promoting the spirit of the right to privacy.

24 *Attorney General v Ndii; Prof Rosalind Dixon (*amici curiae*)* [2022] KESC 8 (KLR).
25 Woolman 2016b: 283–295. See, also, Woolman 2016a: 156–183.
26 Woolman 2016b: 285.
27 *Ibid*.
28 *Idem* at 291.
29 Du Plessis 2011: 92–99.
30 *Idem* at 97.
31 *Ibid.*
32 *Ibid*.

https://doi.org/10.47348/FUND/v30/i1a4

3 Legislating privacy in Kenya

This part of the discussion looks at the legislation dealing with any aspect of the right to privacy. These statutes bear witness to the fact that Kenya has been experiencing continuous reinforcement of the right to privacy. The discussion also identifies those statutes containing provisions that limit the right to privacy.

3 1 Legislation promoting the right to privacy

3 1 1 The Data Protection Act 24 of 2019

The Data Protection Act, when read together with article 31 of the Constitution, forms the foundation for the right to privacy. The Act is the first to give effect to article 31 in a comprehensive manner. Before its implementation, legal principles with regard to privacy could only be derived from a few provisions of select statutes and judicial decisions.

The Data Protection Act is divided into eleven parts. Part 1 contains the preliminary provisions. Part 2 provides for the establishment of the Office of the Data Protection Commissioner. Part 3 regulates the registration of data controllers and data processors. Part 4 sets out principles and obligations of personal data protection. Part 5 provides for grounds for the processing of sensitive personal data. Part 6 regulates the transfer of personal data outside Kenya. Part 7 stipulates exemptions to the Act. Part 8 provides for enforcement provisions. Part 9 concerns financial provisions. Part 10 provides for the enactment of regulations and Part 11 sets out miscellaneous provisions.

i The purpose of the Act

Section 3 of the Data Protection Act provides the object and purpose of the Act as follows, namely–

> (a) to regulate the processing of personal data;
>
> (b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25;
>
> (c) to protect the privacy of individuals;
>
> (d) to establish the legal and institutional mechanism to protect personal data; and
>
> (e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

https://doi.org/10.47348/FUND/v30/i1a4

With regard to the first object and purpose, namely the regulation of the processing of personal data, the Act provides further details. The term "personal data" is defined under section 2 of the Act as "any information relating to an identified or identifiable natural person". Section 2 further states that a data subject is "an identified or identifiable natural person who is the subject of personal data". The same section also defines "processing" as "any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means". The Act identifies data controllers and data processors as engaging in personal data processing. Section 2 defines a data controller as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data". A data processor is defined as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller". This means that the Act applies to both public and private sector actors.

Regarding the second object and purpose, namely that data processing should be guided by the provisions laid out in section 25 of the Act, it is necessary to take note of the wording of the latter provision itself. Section 25 outlines the principles of data protection as follows:

> Every data controller or data processor shall ensure that personal data is–
>
> (i) processed in accordance with the right to privacy of the data subject;
>
> (ii) processed lawfully, fairly and in a transparent manner in relation to any data subject;
>
> (iii) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
>
> (iv) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
>
> (v) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
>
> (vi) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

https://doi.org/10.47348/FUND/v30/i1a4

(vii) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

(viii) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Any public or private sector actor processing personal data may therefore only do so in line with these outlined principles. Paragraph v below takes a closer look at these principles and at the lawful processing of personal data as regulated by section 30 of the Act.[33]

With regard to the third object and purpose of the Act relating to the protection of the right to privacy of individuals, section 26 of the Act expands the right to privacy by providing for the rights of data subjects as follows:[34]

A data subject has a right–

(a) to be informed of the use to which their personal data is to be put;

(b) to access their personal data in custody of data controller or data processor;

(c) to object to the processing of all or part of their personal data;

33 Lawful processing relates to the circumstances under which a public or private sector actor may process personal data. Section 30 states as follows: "(1) A data controller or data processor shall not process personal data, unless– (a) the data subject consents to the processing for one or more specified purposes; or (b) the processing is necessary– (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; (ii) or compliance with any legal obligation to which the controller is subject; (iii) in order to protect the vital interests of the data subject or another natural person; (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (v) the performance of any task carried out by a public authority; (vi) for the exercise, by any person in the public interest, of any other functions of a public nature; (vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or (viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research."

34 Section iv *infra* discusses these rights in greater detail.

https://doi.org/10.47348/FUND/v30/i1a4

(d) to correction of false or misleading data; and
(e) to deletion of false or misleading data about them.

In order to provide for the fourth object and purpose, namely the implementation of the legal and institutional mechanism to protect personal data, section 5 of the Act establishes the Office of the Data Protection Commissioner as a body corporate. Section 8 lists the functions of the Office, which are to ensure the implementation and enforcement of the Act. Section 9 grants the Data Commissioner certain powers, which include conducting investigations, facilitation of alternative dispute resolution and imposing administrative fines.

With regard to the fifth object and purpose relating to remedies, section 56 enables an individual aggrieved by any decision made in relation to matters regulated by the Act to lodge a complaint with the Office of the Data Protection Commissioner. The Commissioner may issue enforcement notices (s 58); issue administrative fines (s 63); order for compensation of a data subject (s 65); or make other orders that would remedy the data subject's predicament. There are therefore statutory consequences for public and private sector actors who process personal data in violation of provisions of the Data Protection Act.

ii The Data Protection Regulations

To give effect to the Act, on 31 December 2021, the Cabinet Secretary, Ministry of Information, Communication, Technology, Innovation and Youth Affairs published three sets of Regulations in terms of section 71 of the Act. These are the Data Protection (General) Regulations, 2021;[35] the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021;[36] and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.[37]

The Data Protection (General) Regulations, 2021 enable the rights of a data subject by providing for restriction on the commercial use of data; listing the obligations of data controllers and data processors; identifying the elements for implementing data protection by design and by default; describing the processes

35 Published as LN263 *Kenya Gazette* 236 of 31 Dec 2021.
36 Published as LN264 *Kenya Gazette* 236 of 31 Dec 2021.
37 Published as LN265 *Kenya Gazette* 236 of 31 Dec 2021.

https://doi.org/10.47348/FUND/v30/i1a4

for notification of personal data breaches; regulating the transfer of personal data outside Kenya; requiring data protection impact assessment; and listing those circumstances exempted from the Data Protection Act. The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 outline the procedure for the lodging and admission of complaints, the available responses thereto, as well as enforcement provisions. Aptly named, the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 provide for the registration of data controllers and data processors.

iii The scope and application of the Act

In a 2021 case, *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology Ex Parte Katiba Institute; Immaculate Kasait, Data Commissioner (Interested Party)*,[38] the High Court confirmed that the Act applies retrospectively, despite the fact that the Act was enacted two years earlier, in November 2019. The court stated:[39]

> Reading the preamble to the Act together with section 3 thereof on the Act's object and purpose, it is clear that the Act was intended to be retrospective to such an extent or to such a time as to cover any action taken by the state or any other entity or person that may be deemed to affect, in one way or the other, the right to privacy under Article 31(c) and (d) of the Constitution. … Needless to say, the need to protect the constitutional right to privacy did not arise with the enactment of the Data Protection Act; the right accrued from the moment the Constitution was promulgated.

However, the High Court was clear that it is not the statutes enacted post-2010 that provide for the right to privacy, but that the right to privacy accrued "from the moment the Constitution was promulgated". It is not yet clear whether this decision will be appealed.

The Data Protection Act amended several existing statutes. For example, after its amendment, the Births and Deaths Registration Act[40] now states that the register of births and deaths in Kenya "shall be maintained in accordance with the principles of data protection

38 [2021] eKLR.
39 *Idem* at 99–100.
40 Births and Deaths Registration Act, cap 149.

https://doi.org/10.47348/FUND/v30/i1a4

set out in the Data Protection Act".[41] Section 25 of the Independent Electoral and Boundaries Commission Act[42] was amended to state that "the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters". Furthermore, section 61 of the Employment Act[43] was amended to require that "where an employer maintains such a register [of children in their employment], the register shall be maintained in accordance with principles of data protection set out in the Data Protection Act". In total, the promulgation of the Data Protection Act has resulted in the amendment of nine other statutes.[44]

It is submitted that these amendments to ensure conformity to data protection principles are curious. The Act applies automatically to all instances where personal data is processed by individuals and/or entities in public and private sectors. It is not clear why Parliament sought to single out these twelve statutes for amendment as such amendment provisions are required in almost all existing statutes.

iv Data subject rights

Section 26 of the Data Protection Act sets out the data subject rights that form an intrinsic part of the constitutional right to privacy. Data subject rights expand the latter right to privacy and must be taken into consideration when making incursions into an individual's right to privacy.

In *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*,[45] the Court of Justice of the European Union observed that one of the key objectives of data protection law is the effective and complete protection of the fundamental rights and freedoms of natural persons with respect to

41 *Idem* s 7.

42 Independent Electoral and Boundaries Commission Act, cap 7C.

43 Employment Act, cap 226.

44 Capital Markets Act, cap 485A; Kenya National Examinations Council Act, cap 214A; Kenya Citizenship and Immigration Act 12 of 2011; Basic Education Act, cap 211; Universities Act, cap 210; Central Depositories Act, cap 485C; Proceeds of Crime and Anti-Money Laundering and Proceeds of Crime Act, cap 59A; Kenya Information and Communications Act, cap 411A; and Insolvency Act, cap 53.

45 Case nr C-131/12 (13 May 2014) at 53.

https://doi.org/10.47348/FUND/v30/i1a4

the processing of personal data. To ensure effective protection, data protection laws should therefore empower data subjects to have a measure of control over how their personal data is processed; this is achieved through the use of data subject rights.

The Council of Europe, when commenting on the Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 1981,[46] posited that the main purpose of the Convention was to enable individuals to know, understand and manage how others process their personal data. The Convention explicitly refers to the autonomy of an individual and the right to manage personal data, which derives from the dignity of the individual. Human dignity is to be secured when processing personal data so that the individual is not treated as a mere object.[47]

Despite the empowerment of an individual to manage their personal data, a privacy paradox exists: Although individuals "say that they value privacy highly, … they readily give away sensitive personal information for small discounts or tiny benefits – or sometimes for nothing at all".[48] Individuals easily supply personal data when they perceive some measure of control, even if the control is illusory.[49] Nevertheless, "privacy's value involves the right to have choices and protections".[50] As a result, the protection of privacy should not only rely on individuals undertaking privacy self-management, but should also "focus on regulating the architecture that structures the way information is used, maintained, and transferred".[51] This means that the focus on the right to privacy should be on the persons seeking to make incursions into the right. As one scholar posits, "privacy cannot be solved at the individual level. Rights should certainly be part of privacy laws, but they can only play a small supportive role. Meaningful protection must be large-scale and structural in nature".[52] Or put simply, there should be a balance between individual rights and constitutional obligations of those who wish to make incursions into the right to privacy.

46 Council of Europe 2018: 108.
47 *Idem* at 10.
48 Solove 2021: 2.
49 *Idem* at 17.
50 *Idem* at 24.
51 *Idem* at 6.
52 *Idem* at 50.

https://doi.org/10.47348/FUND/v30/i1a4

There is therefore a need for data subject rights that limit the power of government and companies;[53] ensure respect for individuals;[54] maintain appropriate social boundaries;[55] create trust;[56] allow the individual control over their own life;[57] and offer protection of intimacy, bodies and sexuality.[58] Data subject rights provide people with "notices, rights and choices".[59] For data subject rights to be meaningful, the data subject has to be informed of their rights; its effects; how to exercise the rights; and of the circumstances under which the rights may be limited. This is critical in empowering the individual.

The personal data ecosystem must first create a culture where data subject rights are respected, protected and promoted. This will be achieved when data controllers and data processors comply with article 31 of the Constitution and with the Data Protection Act.

In those cases where it is argued that the rights of data subjects are not comprehensive enough, the Office of the Data Protection Commissioner and the courts should be guided by article 20(3) of the Constitution, which provides that it should "(a) develop the law to the extent that it does not give effect to a right or fundamental freedom; and (b) adopt the interpretation that most favours the enforcement of a right or fundamental freedom".

v Data protection principles and lawful processing of personal data

The law should clearly set out any legitimate reasons for making incursions into an individual's right to privacy. Ideally, the legislative framework should provide that the processing of personal data is permissible only if it meets the legal requirements. Data protection principles set the benchmark that ought to be complied with where the right to privacy and data protection is at risk.[60] Data protection principles provide the common understanding from which to comply with data protection regulations.[61] It also ensure uniformity in the interpretation of data protection rules.[62]

53 *Idem* at 38.
54 *Ibid*.
55 *Idem* at 39.
56 *Ibid.*
57 *Ibid.*
58 *Ibid.*
59 *Idem* at 49.
60 De Hert 2017: 167, 168.
61 *Idem* at 169.
62 *Idem* at 175.

https://doi.org/10.47348/FUND/v30/i1a4

Data protection principles are the guiding light where the processing of personal data is concerned; they offer the ideal vision of the right to privacy, as well as the bare minimum that must be met by anyone processing personal data. On data protection principles, one scholar cites "control and consent; transparency, portability and interoperability; and strong enforcement and real accountability" as matters that should be provided for in a data protection statute.[63] This view creates a link between privacy and other rights and freedoms, and argues that the individual right to privacy "must be supported by legislation that renders the right effective and realizable".[64] The "legitimate interest" as the basis for the processing of personal data "must be weighed against the human rights of affected individuals and will only be justified where the impact on those human rights is not disproportionate to the goals sought to be obtained".[65]

The rights of a data subject, the principles of data protection, and lawful data processing are all meant to accord individuals privacy and self-management. The latter is achieved when individuals are granted express rights regarding their personal data. These rights include a right to opt out of data sharing; a right to notification; and a right to deletion.[66] Self-management should not be illusory. Individuals must have statutory powers to take action against natural and legal persons wishing to collect their personal data.[67] As already pointed out above, self-management should operate within a data processing ecosystem that respects, protects and promotes data subject rights.

One scholar has identified several data protection principles that must feature in a data protection statute.[68] These are fair and lawful processing;[69] purpose specification;[70] minimality;[71] quality;[72] openness and transparency;[73] data subject participation;[74]

63 Scassa 2020: 174.
64 *Idem* at 178.
65 *Idem* at 179.
66 *Idem* at 179.
67 *Ibid.*
68 Roos 2006: 103–130.
69 *Idem* at 108. See, also, Roos 2009: *passim*.
70 Roos 2006: 111.
71 *Idem* at 113.
72 *Idem* at 114.
73 *Idem* at 116.
74 *Idem* at 119.

https://doi.org/10.47348/FUND/v30/i1a4

sensitivity;[75] security and confidentiality;[76] accountability;[77] as well as exceptions and exemptions.[78] These basic universal principles should be encapsulated in data protection legislation even where there are differences in language, legal traditions and cultural and social values.[79] In other words, there is need for uniformity in the text of data protection laws, especially regarding data protection principles. These are set out in section 25 of the Act.

The Data Protection Act does not provide for security as an explicitly stated principle. It is submitted that the lack of security as a data protection principle in the Data Protection Act is a regrettable omission as it does not conform to the universal principles listed above. In practice, the lack of the security principle may be interpreted by data controllers, data processors, the Office of the Data Protection Commissioner and the courts as being of diminished importance, even though it is a crucial principle.

In addition to data subject rights and data protection principles, the right to privacy is further enhanced by section 30 of the Data Protection Act, providing for situations where lawful processing of personal data may take place. Section 30(1)(b)(v) of the Act is a peculiar provision and states that "a data controller or data processor shall not process personal data, unless the processing is necessary for the performance of any task carried out by a public authority". This phrasing is problematic, because the Act does not define what "any task" would entail, what a "public authority" refers to or when processing would be "necessary". Broad and/or vague statutory provisions have the potential to limit fundamental rights and freedoms unnecessarily. Section 30(1)(b)(v) appears to grant the state a tremendous amount of latitude in processing personal data of individuals. The ambiguity, vagueness and broadness of the phrasing in the statute unjustly limits the rights of data subjects.

vi Oversight and remedies

In line with section 8 of the Data Protection Act, the Office of the Data Protection Commissioner oversees all processes applicable in terms of the Act. Ideally, the Office must be independent.

75 *Idem* at 122.
76 *Idem* at 124.
77 *Idem* at 126.
78 *Idem* at 127.
79 *Idem* at 130.

https://doi.org/10.47348/FUND/v30/i1a4

One scholar has pointed out that the independence of an authority is tied to its "distance from constitutionally recognized branches of power"[80] and speaks to the integrity of the service it renders.[81] However, such independence is not absolute as the authority is subject to oversight itself from institutions, such as Parliament and the courts,[82] which may only act within their constitutional mandates and powers.[83]

Also, there must be effective remedies in instances where personal data protection are violated. Article 8 of the Universal Declaration of Human Rights, 1948 provides for a right to an effective remedy and so does article 2(3) of the International Covenant on Civil and Political Rights, 1966. According to both these international instruments, an effective remedy has four components. First, there must have been a violation of a recognised fundamental right. Secondly, there must be a remedy for such violation. Thirdly, a competent authority must determine the remedy. Fourthly, the remedy should be enforced by a competent authority once it is granted.

One view posits that "remedies make rights real in practice for plaintiffs. They can provide redress and solace, punish, and condemn outrageous violations, potentially deter future harmful conduct, and vindicate interests that are of importance to individuals and society as a whole".[84] This view argues that remedies must be linked to the norms they relate to, or, simply put, remedies cannot be divorced from the rights they are tied to.[85] The next paragraph draws attention to some of the remedies that have been made available by the Office of the Data Protection Commissioner.

vii Decisions by the Office of the Data Protection Commissioner

The Data Commissioner has issued administrative and penal notices to data handlers. These are an indication of the administrative remedies available for the violation of provisions of the Data Protection Act. In *Koros Kiprotich v Higher Education Loans*

80 Sajó 2007: 14.
81 *Ibid*.
82 *Idem* at 13, 24.
83 *Idem* at 24.
84 Varuhas & Moreham 2018: ch 1.
85 *Ibid.*

https://doi.org/10.47348/FUND/v30/i1a4

Board,[86] a matter that involved a claim for the rectification of data, the Commissioner ordered the respondent to rectify the personal data they had on the complainant. In *Abubakar Hussein v Ceres Tech Limited t/a Chapaa Loan*,[87] the Commissioner found the respondent liable for not respecting the data subject rights of the complainant as required by section 26 of the Data Protection Act. In addition, the Commissioner awarded extensive damages to the complainants in *Emily Sila v Zerox Technology Company Limited*,[88] where the respondent had violated the former's data subject rights. In *Pauline Muhanda v Safaricom PLC*,[89] the Commissioner found that an employee of the respondent was liable for criminal prosecution for sharing personal data of the complainant, contrary to the respondent's internal policies and the provisions of the Data Protection Act.

The Commissioner recently indicated that penalty notices have been issued against several data handlers.[90] For example, Mulla Pride, a digital credit lender, was fined Ksh (Kenyan shillings) 2 975 000 for not complying with data protection principles and data subject rights. Casa Vera Lounge was fined Ksh 1 850 000 for posting images of clients on social media without obtaining consent, and Roma School was fined Ksh 4 450 000 for posting photos of minors on public forums without parental/guardian consent. It is clear from the amounts of these fines that the Commissioner takes such violations seriously.

3 1 2 The HIV and AIDS Prevention and Control Act 14 of 2006

The HIV and AIDS Prevention and Control Act was enacted even before the promulgation of the current Constitution. The Act protects personal information relating to the HIV status of an individual. Section 20 of the Act provides as follows with regard to privacy guidelines:

86 *Koros Kiprotich v Higher Education Loans Board* ODPC Complaint no 0781 of 2023.

87 *Abubakar Hussein v Ceres Tech Limited t/a Chapaa Loan* ODPC Complaint no 2194 of 2023.

88 *Emily Sila v Zerox Technology Company Limited* ODPC Complaint no 2109 of 2023.

89 *Pauline Muhanda v Safaricom PLC* ODPC Complaint no 1212 of 2023.

90 See Office of the Data Protection Commissioner 2023.

https://doi.org/10.47348/FUND/v30/i1a4

> (1) The Minister for the time being responsible for matters relating to health may, in regulations, prescribe privacy guidelines, including the use of an identifying code, relating to the recording, collecting, storing and security of information, records or forms used in respect of HIV tests and related medical assessments.
>
> (2) No person shall record, collect, transmit or store records, information or forms in respect of HIV tests or related medical assessments of another person otherwise than in accordance with the privacy guidelines prescribed under this section.

These envisioned privacy guidelines are yet to be developed.[91] This is one of the first Kenyan statutes to regulate the processing of specified personal information. Section 21 provides for the confidentiality of records, while section 22 defines those circumstances under which information may be disclosed. Section 22(1)(a) indicates that "no person shall disclose any information concerning the result of an HIV test or any related assessments to any other person except … with the written consent of that person". Section 22 further provides for other reasons for disclosure of information, including "for the purpose of an epidemiological study or research authorized by the Minister" and "to a court where the information contained in medical records is directly relevant to the proceedings before the court or tribunal". On breaching confidentiality, section 23 states that "a person who contravenes any of the provisions of this Part or of any guidelines prescribed hereunder commits an offence".

The Act further makes provision for a tribunal to handle complaints regarding breach of confidentiality. The HIV & AIDS tribunal has considered the question of disclosure of information of an individual's HIV and AIDS status without consent. In *SKM v CBM*,[92] the tribunal stated it must be shown how the disclosure of information was carried out.[93] The tribunal found that *in casu* there had been disclosure without consent, and it granted the claimant monetary damages.[94] The tribunal also inquired into the reasons why such protection is necessary. It held that since the "claimant suffered emotionally or psychologically as a result of the unauthorized disclosure, we find that there is sufficient evidence on record to prove that the Claimant has, directly and indirectly

91 See, in general, Akinyi 2019; Sircar & Maleche 2020: 167–176.
92 [2021] eKLR.
93 *Idem* at 56.
94 *Idem* at 77.

https://doi.org/10.47348/FUND/v30/i1a4

through her family, suffered emotionally and psychologically".[95] Similarly, in *JK v AAR Healthcare Kenya Ltd*,[96] the tribunal considered the question of disclosure of an individual's HIV status to third parties and made it clear that a claimant has to prove that there has been unauthorised disclosure to third parties.[97]

The HIV and AIDS Prevention and Control Act complements the provisions of the Data Protection Act regarding the privacy and data protection of an individual's HIV and AIDS status. The term "health status" is defined as "sensitive personal data" under section 2 of the Data Protection Act. Sensitive personal data requires a high level of protection as defined under part V of the Act. What this means is that complaints related to the HIV status of an individual may be adjudicated under both the HIV and AIDS Prevention and Control Act and the Data Protection Act.

3 1 3 The Computer Misuse and Cybercrimes Act 5 of 2018

The Computer Misuse and Cybercrimes Act provides for offences relating to computer systems. The aims of the Act are to protect computer systems, programs and data; to prevent unauthorised use of computer systems; to deal with cybercrimes; and to protect the right to privacy, freedom of expression and access to information.[98] Some of the offences created by the Act include unauthorised access; unauthorised interference; unauthorised interception; unauthorised disclosure; cyber espionage; child pornography; computer fraud; cyber harassment; identity theft; impersonation; and wrongful distribution of obscene or intimate images. These offences have an impact on the right to privacy and data protection.[99]

The Computer Misuse and Cybercrimes Act plays an important role in the protection of data in instances of cybersecurity. Cybersecurity lapses may cause data breaches, which in turn may lead to the loss or unauthorised disclosure or exposure of personal data, in effect contravening provisions of the Data Protection Act.

95 *Idem* at 78.

96 *JK v AAR Healthcare Kenya Ltd* [2020] eKLR.

97 *Idem* at 49.

98 Section 3 of the Computer Misuse and Cybercrimes Act 5 of 2018.

99 For example, s 14 of the Act makes it an offence to access a computer system without authorisation; s 16 makes it an offence to interfere with a computer system without authorisation; s 29 criminalises the act of engaging in electronic identity theft and impersonation; and s 38 makes it an offence to fraudulently use electronic data.

https://doi.org/10.47348/FUND/v30/i1a4

Section 43 of the Data Protection Act provides for notification and communication of a breach of personal data. Also, the Act contains provisions regarding the crimes set out under the Computer Misuse and Cybercrimes Act. It is submitted that the latter Act be read together with the Data Protection Act to ensure greater protection of personal data.

3 1 4 The Children Act 29 of 2022

The Children Act is the most recent statute to provide for the protection of the right to privacy. It replaces section 19 of the repealed Children Act 8 of 2001, which stated that "every child shall have the right to privacy subject to parental guidance". The Children Act 29 of 2022 gives "effect to Article 53 of the Constitution"[100] and makes provision for children's rights and for parental responsibility. This Act was drafted within the context of the Data Protection Act. On the protection of children's personal data, section 33 provides as follows:

(1) Every data controller or data processor shall not process personal data relating to a child unless–
   (a) consent is given by the child's parent or guardian; and
   (b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.

(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of–
   (a) available technology;
   (b) volume of personal data processed;
   (c) proportion of such personal data likely to be that of a child;
   (d) possibility of harm to a child arising out of processing of personal data; and
   (e) such other factors as may be specified by the Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).

100 Children Act 29 of 2022

https://doi.org/10.47348/FUND/v30/i1a4

On the right to privacy of a child, section 27 of the Children Act further provides as follows:

> (1) No person shall subject a child to arbitrary or unlawful interference with his or her privacy, family or private affairs, or correspondence, or to attacks upon his or her honour or reputation.
>
> (2) Without prejudice to the generality of subsection (1), parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children.
>
> (3) The personal data concerning a child shall be processed only in accordance with the provisions of the Data Protection Act.

The Children Act also contains other provisions on the privacy of a child. With regard to the right to healthcare, section 16(3) states that "in pursuance of the right to healthcare services under this section, every child has the right to privacy and a child-friendly environment". On detention of children in conflict with the law, section 26(6) provides that "the competent authorities shall take appropriate measures to facilitate humane treatment and respect for the privacy, legal capacity and inherent human dignity of children deprived of liberty, including children with disabilities". Section 94 indicates that proceedings relating to children should ensure privacy. Section 220(1) provides that a "child offender has the right to privacy during arrest, the investigation of the offence and at any other stage of the cause of the matter". Section 235(g) provides that "every child accused of having violated any rule of law shall … have his or her privacy respected at all stages of the proceedings".

When comparing the provisions of the Children Act to those of the Data Protection Act, it is clear that the former focuses on the general right to privacy of a child, while the latter provides more specific guidelines regarding a child's right to data protection. This is confirmed by section 27(3) of the Children Act, which states that personal data relating to children shall be processed in accordance with the Data Protection Act. There is a synergetic relationship between these two statutes. However, both address the role of parents and legal guardians. This is because a child's right to privacy is exercised subject to parental guidance as stated in section 33 of the Data Protection Act.

In this regard, one scholar argues that "a child's human right to privacy should not be rendered conditional upon another's wishes

https://doi.org/10.47348/FUND/v30/i1a4

and behaviour, or control and consent".[101] According to this view, while a parent may have control over a child's privacy, the courts ought to consider the best interests of the child.[102] Secondly, the courts should specifically inquire into the potential harm to the child if their right to privacy is violated, irrespective of parental control and consent.[103] This is in line with article 53(1)(e) of the Kenyan Constitution, which, when read together with the Children Act, recognises parental care and protection unless such care and protection is harmful to the child. I agree with these proposals. Where a parent exercises parental control and consent, there is an assumption that the parent understands the parameters within which the right to privacy may operate. In this regard, the courts should inquire whether the parent was empowered to make the right call. Moreover, when considering a child's data protection rights, the Children Act should be read together with the Data Protection Act.

The next part looks at the legislation that limits the right to privacy.

3 2 Legislation limiting the right to privacy

Article 24 of the Kenyan Constitution contains the general limitations clause.[104] Kenya has a few statutes that limit the right to privacy.

101 Gligorijević 2019: 203.

102 *Idem* at 210.

103 *Idem* at 212.

104 Article 24(1) provides "A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including– (a) the nature of the right or fundamental freedom; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and (e) the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose."
Article 24(2) states that legislation limiting a fundamental right or freedom "is not valid unless the legislation specifically expresses the intention to limit that right or fundamental freedom, and the nature and extent of the limitation"; is not valid "unless the provision is clear and specific about the right or freedom to be limited and the nature and extent of the limitation"; and "shall not limit the right or fundamental freedom so far as to derogate

https://doi.org/10.47348/FUND/v30/i1a4

These include the Registration of Persons Act, the National Intelligence Service Act, the National Police Service Act and the Private Security Regulation Act. These should be interrogated through the proportionality test, which has been described as an assessment indicating that "the harms of a particular act not outweigh the benefits of that act".[105] Where the harm caused by any act outweighs the benefits of that act, the act is considered disproportionate.[106] One scholar argues that when deciding whether an act is proportionate or disproportionate, the difference between the harm and benefits should be significant.[107] While it may not be possible to have a uniform harm-versus-benefits scale, legislation should be evaluated on a case-to-case basis.[108] The following questions have been proposed when applying the proportionality test:[109]

1. Does the legislation (or other government action) establishing the right's limitation pursue a legitimate objective of sufficient importance to warrant limiting a right?
2. Are the means in service of the objective rationally connected (suitable) to the objective?
3. Are the means in service of the objective necessary, that is, minimally impairing of the limited right, taking into account alternative means of achieving the same objective?
4. Do the beneficial effects of the limitation on the right outweigh the deleterious effects of the limitation; in short, is there a fair balance between the public interest and the private right?

The Kenyan High Court applied the proportionality test in *Jacqueline Okuta v Attorney General*.[110] The court held that the test is a fluid one that necessitates analysis and application of the law while having "regard to the surrounding circumstances, including recent developments in the law, current political and policy challenges and contemporary public interest considerations".[111] In its judgment,

from its core or essential content". Article 24(3) declares that "the State or a person seeking to justify a particular limitation shall demonstrate to the court, tribunal or other authority that the requirements of this Article have been satisfied".

105 Macnish 2015: 532.
106 *Ibid.*
107 *Ibid.*
108 *Idem* at 539.
109 Huscroft, Miller & Webber 2014: 21.
110 [2017] eKLR.
111 *Ibid.*

https://doi.org/10.47348/FUND/v30/i1a4

the court reasoned that a proportionality test "preserves rights, provides a framework for balancing competing rights and enables other important public concerns, such as national security and public order, to be duly taken into account".[112]

The specific statutes discussed below should be read with the proportionality test in mind.

3 2 1 The Registration of Persons Act, cap 107

Section 9A of the Registration of Persons Act provides for the National Integrated Identity Management System (hereafter "NIIMS"). The section introduces sweeping changes to citizen registration by migrating it to a digital platform. The purpose of this provision is to create a national digital identity card. This digital identity programme has been challenged in court in several cases.

In *Nubian Rights Forum v Attorney General; Child Welfare Society*,[113] the High Court ruled that the state is at liberty to proceed with the implementation of NIIMS and to process and utilise the data collected for such purposes on condition that an appropriate and comprehensive regulatory framework on the implementation of NIIMS be enacted that is compliant with article 31 of the Constitution. The court identified the need for data protection laws in Kenya. It held that "the collection of DNA and GPS co-ordinates for purposes of identification is intrusive and unnecessary, and to the extent that it is not authorised and specifically anchored in empowering legislation, it is unconstitutional and a violation of Article 31 of the Constitution".[114] This case indicates that, while provision of digital identity cards may be necessary in incorporating technology with the right to an identity, the infringement of the right to privacy in order to do so must be exercised cautiously and subject to data subject rights and data protection principles.

The digital identity cards roll-out was also challenged in *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology Ex Parte Katiba Institute; Immaculate Kasait, Data Commissioner (Interested Party)*.[115] The petitioners argued that before the roll-out, the government should

112 *Ibid*.
113 [2020] eKLR.
114 *Idem* para 1047.
115 [2021] eKLR.

https://doi.org/10.47348/FUND/v30/i1a4

have carried out an assessment on data protection impact. In its judgment, the court made two key pronouncements that have an impact on the promotion, protection and respect of the right to privacy and personal data protection. The court agreed with the petitioners and ruled that the state should have done a data protection impact assessment before implementing the roll-out. The court ordered the state to halt the roll-out of the digital identity cards until the assessment has been completed. This decision demonstrates that the courts may be persuaded to uphold the right to privacy. The decision points to the requirement that, in the case of personal data, any incursions into the right to privacy should be subject to the provisions of the Data Protection Act.

3 2 2 National security organs legislation

This part deals with the three statutes that regulate Kenya's national security organs, namely the National Intelligence Service Act 28 of 2012, the National Police Service Act 11A of 2011 and the Defence Forces Act 25 of 2012. Article 239 of the Constitution lists the national security organs as the National Police Service, the National Intelligence Service and the Defence Forces.

The functions of the National Intelligence Service and the National Police Service necessitate the processing of personal data. Nevertheless, these institutions have to respect the constitutional right to privacy and process personal data in compliance with the Data Protection Act. The latter Act creates a link between the National Intelligence Service Act and the National Police Service Act. Section 8(2) of the Data Protection Act provides that the "Office of the Data Commissioner may, in performance of its functions collaborate with national security organs". However, the Data Protection Act does not define the nature of the collaboration that is to take place between the Office of the Data Commissioner and the national security organs. It is submitted that without clarity, the provision is vague, overly broad and therefore void.

Section 51(2)(b) of the Data Protection Act further states that processing of personal data is exempt from the provisions of the Act "if it is necessary for national security". However, the term "national security" is not defined. Again, there is no room for ambiguous, vague or broad legal provisions that allow for arbitrary incursions into the right to privacy and data protection.

https://doi.org/10.47348/FUND/v30/i1a4

In this context, the long title of the National Intelligence Service Act provides that the National Intelligence Service is responsible for security intelligence and counterintelligence to enhance national security in accordance with the Constitution. The National Intelligence Service is to "gather, collect, analyse, and transmit or share with the relevant State agencies, security intelligence and counterintelligence". Under the Act, the Service has the power to investigate, gather, collate, correlate, evaluate, interpret, disseminate and store information that is relevant to the performance of its functions, whether within or outside Kenya.

The National Intelligence Service Act is one of the statutes that provides the state with powers to process personal data and carry out surveillance, in effect limiting the right to privacy and data protection. Specifically, section 36(1) of the National Intelligence Service Act states:

> [T]he right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person who is subject to investigation by the Service or suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with.

With regard to state surveillance, the National Police Service Act establishes the Police Service, with one of its functions being collection of criminal intelligence.[116] In line with the limitations clause in the Constitution,[117] section 47(3) of the National Police Service Act provides that the right to privacy may be limited in certain circumstances. Any such limitation must be justified by–[118]

(a) the protection of classified information;
(b) the maintenance and preservation of national security;
(c) the security and safety of officers of the Service;
(d) the independence and integrity of the Service; and
(e) the enjoyment of the rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others.

116 Act 11A of 2011.
117 Article 24(5) of the Constitution provides that "provision in legislation may limit the application of the rights or fundamental freedoms in the following provisions to persons serving in the Kenya Defence Forces or the National Police Service" and then specifically refers to the right to privacy in art 31.
118 Section 47(2) of the National Police Service Act 11A of 2011.

https://doi.org/10.47348/FUND/v30/i1a4

Section 48 of the Kenya Defence Forces Act 25 of 2012 also limits the right to privacy. The justification set out under section 43(2) is to ensure–

(a) the defence and protection of the sovereignty and territorial integrity of the Republic of Kenya;
(b) the protection of classified information;
(c) the maintenance and preservation of national security;
(d) the security and safety of members of the Defence Forces;
(e) that the enjoyment of the rights and fundamental freedoms by any individual member of the Defence Forces does not prejudice the rights and fundamental freedoms of any other individual member of the Defence Forces;
(f) good order and service discipline; and
(g) public health and safety.

The National Police Service Act and the Defence Forces Act are the only statutes within Kenya's legal system that expressly provide for limitation of the right to privacy. Both Acts are instrumental in illustrating statutory provisions justifying incursions into fundamental rights and freedoms.

3 2 3 The Private Security Regulation Act 13 of 2016

The purpose of this Act is to regulate the private security industry and to provide for a framework for cooperation with the Kenya Defence Forces, the National Security Intelligence Service and the National Police Service. Section 47 of the Act grants private security providers the authority to conduct searches.[119] Section 48 of

119 "(1) A private security service provider, a security guard or security officer manning a building or responsible for any property may search a person on entry or exit of that building or property without a warrant. (2) In the exercise of the power to search under subsection (1), a private security service provider, a security guard or a security officer shall not infringe on any right or fundamental freedom of an individual under the Constitution. (3) The power to search under subsection (1) shall be exercised responsibly and shall be subject to any other written law. (4) A private security service provider, a security guard or security guard who violates an individual right or fundamental freedom in exercise of the right to search under this section commits an offence and shall in addition to cancellation of licence, be liable on conviction to the penalty prescribed under this Act or any other written law whichever is higher. (5) The Cabinet Secretary shall, within three months

https://doi.org/10.47348/FUND/v30/i1a4

the Act grants powers to record and temporarily withhold identification documents.

This Act is problematic in that it gives broad powers to private security providers to make incursions into an individual's right to privacy. Private security providers are allowed to use such personal data for commercial purposes, which amounts to an abuse of data protection principles and data subject rights. Private security providers may rely on section 30(1)(b)(ii) of the Data Protection Act, which states that personal data may only be processed where it is "necessary for compliance with any legal obligations to which the controller is subject". If so, they are bound by the principles of data protection under section 25 of the Act; must ensure that the rights of data subjects are respected and protected as per section 26; and, if using such personal data for commercial purposes, must comply with section 37 of the Act that requires express consent from data subjects.

3 2 4 Other legislation

The Health Act 21 of 2017 mandates the national government to formulate policy promoting disease surveillance in connection with the prevention of diseases related to food, water, the environment and sanitation.[120] The Kenya Citizenship and Immigration Act 12 of 2011,[121] the Refugees Act 13 of 2006[122] and the Statistics Act 6 of 1999[123] all contain provisions that require information from an individual, in effect allowing for blanket intrusions into the privacy of persons and for mass collection of personal data. It is submitted that any statutory justifications should comply with constitutional guidelines on the limitation of fundamental rights and freedoms, with data protection principles and with data subject rights set out in the Data Protection Act.

of the commencement of this Act, make regulations generally to provide for the responsible exercise of the power of search granted under this section."

120 Section 69 of the Health Act.

121 See parts III, IV, V, VI, VII and VIII of the Citizenship and Immigration Act.

122 Section 26 of the Refugees Act.

123 See part II of the Statistics Act.

https://doi.org/10.47348/FUND/v30/i1a4

3 3 Concluding thoughts on statutes

The statutes mentioned in this part illustrate the regulation of data protection in Kenya. As shown in this contribution, the courts have confirmed the Data Protection Act to be the foundational statute with regard to the processing of personal data by public and private sector actors. The discussion has shown that the HIV and AIDS Prevention and Control Act 14 of 2006, the Computer Misuse and Cybercrimes Act 5 of 2018 and the Children Act 29 of 2022 all contain provisions complementing the application of the Data Protection Act.

In contrast, the Registration of Persons Act cap 107, the National Intelligence Service Act 28 of 2012, the National Police Service Act 11A of 2011 and the Private Security Regulation Act 13 of 2016 all contain provisions that may limit the right to privacy and the application of the Data Protection Act. The vague and overly broad provisions in the Data Protection Act on national security and collaboration between the Office of the Data Protection Commissioner and national security organs are problematic. As indicated, the provisions of these statutes should be interpreted or applied in line with the principles set out in the proportionality test.

4 Judicial interpretation of the constitutional right to privacy in Kenya

Where there is a right, there should be a remedy. Article 8 of the Universal Declaration of Human Rights states that "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law".[124] One of the avenues to access an effective remedy is through the national court system. Article 22(1) of the 2010 Kenyan Constitution provides that "every person has the right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened". There have been numerous cases in that country claiming that the right to privacy has been denied, violated, infringed or threatened.

124 Universal Declaration of Human Rights, 1948.

https://doi.org/10.47348/FUND/v30/i1a4

In *Samura Engineering Limited v Kenya Revenue Authority*,[125] the High Court ruled that warrantless searches and seizures violate the right to privacy protected under article 31 of the Constitution.[126] The court stated that the right to privacy is entrenched in the Constitution and includes the right not to have one's person, home or property searched or one's possessions seized. Since warrantless searches infringe on the right to privacy, it must be conducted in compliance with legislation, which, in turn, must comply with the provisions of article 24 of the Constitution. The court held that such constitutional safeguards "regulate the way in which state officials enter the private domains of ordinary citizens [and] is one of the features that distinguish a democracy from a police state".[127] The onus is on the state to prove that the conduct of their agents is not in conflict with the constitutional standard when making incursions into the privacy of individuals.[128] The court recognised that the state's authority to collect taxes should be "balanced with that of the individual right to privacy and dignity and in balancing these rights, the State must justify its actions".[129] The court further held that when society places the values of rule of law, good governance, transparency and accountability at the centre of the Constitution, the culture should be one that provides justification for any infringement of fundamental rights and freedoms. Searches and seizures without reasonable cause are therefore in breach of the right to privacy.[130]

In *Kenya Plantation and Agricultural Workers Union James Finlay (K) Limited*,[131] the issue in contention was the safety of patients' records once a medical facility ceased to exist. The petitioners argued that even where a medical facility was closed down, the patients' records were still regulated by the doctor-patient confidentiality. In its judgment, the court emphasised that under article 31(c) of the Constitution, every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed. This right extends to "having information such as official

125 [2012] eKLR.
126 *Idem* para 104.
127 *Idem* para 66.
128 *Idem* para 76.
129 *Idem* para 77.
130 *Idem* para 83.
131 [2013] eKLR.

https://doi.org/10.47348/FUND/v30/i1a4

records, photographs, correspondence, diaries and medical records kept private and confidential".[132] Thus, there is a need for medical professionals to "take positive steps to prevent intrusions into the privacy of its hospital's patients".[133] This decision was instrumental in highlighting the kind of information that requires protection.

In *COM v Standard Group Limited*,[134] the petitioner's claim related to the publication without his consent of his photos in the respondent's newspaper. He claimed that this was a violation of his right to privacy under article 31 of the 2010 Constitution. The High Court asserted that "the Petitioner's written consent was not sought for his photograph and names to appear in the publication, I am also persuaded to find that the Respondent also violated the Petitioner's right to privacy as pleaded".[135] The court awarded the petitioners general damages for pain and suffering.[136] This decision dealt with the matter of the infringement of privacy as it relates to the requirement of consent. Despite this judgment being delivered before the enactment of the Data Protection Act, it indicates the court's willingness to provide effective remedies for the infringement of the right to privacy. However, the courts didn't follow the same approach in another case regarding a claim for similar damages.

In *David Lawrence Kigera Gichuki v Aga Khan University Hospital*,[137] the respondent had released the petitioner's medical information to a third party without his consent, thereby in effect violating the petitioner's right to privacy under article 31. The court noted that "the right to privacy is not absolute and must, in certain circumstances, give way to the greater public interest in disclosure".[138] The court emphasised that the right to privacy is not an absolute right, but that it is subject to limitations outlined under article 24 of the Constitution.[139] The Court conceded that there had been a breach of privacy,[140] but held that it was "not satisfied that there was any loss occasioned to the petitioner, or that damages,

132 *Ibid.*
133 *Ibid.*
134 [2013] eKLR.
135 *Idem* para 25.
136 *Idem* para 32.
137 [2014] eKLR.
138 *Idem* para 22.
139 *Idem* para 18.
140 *Idem* para 37.

https://doi.org/10.47348/FUND/v30/i1a4

are as a result of such disclosure, merited"; it therefore refused to award any damages.[141]

Similarly, in *JLN v Director of Children Services*,[142] the petitioners claimed that their right to privacy had been violated unnecessarily and without just cause when a hospital disclosed confidential medical information to a third party. The petitioners argued that the hospital had breached the doctor-patient confidentiality agreement in disclosing the details of a surrogacy arrangement. The court found that the hospital had been correct to inform the Director of Children Services about the surrogacy arrangement *in casu* since, at the time, Kenya did not have any laws regulating surrogacy. As in the *Gichuki* case, the court indicated that the right to privacy is not absolute.[143]

In *Aids Law Project v Attorney General*,[144] the petitioner challenged certain statutory provisions[145] that compelled persons living with HIV/AIDS to disclose their medical status to their "sexual contacts". The petitioner argued that disclosure of such information undermines the right to privacy. The court agreed that such disclosure was inconsistent with article 31, as well as with the confidentiality principle of medical information.[146] In its judgment, the court ruled that the provision on disclosure of health status was vague, too broad and lacked certainty, especially with regard to the meaning of the term "sexual contact". Such vagueness creates the undesired situation of maintaining a law that vaguely prescribes criminal offenses that leave it to a court's subjective opinion as to whether the defendant may be convicted or acquitted.[147] This judgment therefore upheld the individual's right to privacy against any vague, broad or uncertain legislative provisions that infringe on such right.

In *Kenya Legal and Ethical Network on HIV & AIDS v Cabinet Secretary Ministry of Health*,[148] the High Court was asked to rule on the constitutionality of a presidential directive instructing

141 *Idem* paras 39, 40.
142 [2014] eKLR.
143 *Idem* para 22.
144 [2015] eKLR.
145 The obligation was set out under s 24 of the HIV and AIDS Prevention and Control Act, 2006.
146 *Aids Law Project v Attorney General* [2015] eKLR para 87.
147 *Idem* para 88.
148 [2016] eKLR.

https://doi.org/10.47348/FUND/v30/i1a4

county commissioners to cooperate with all County Directors of Education and County Directors of Medical Services in collecting up-to-date data on all school-going children living with HIV and on all expectant and breastfeeding mothers. Such information was to be gathered by way of a prescribed data matrix linking individuals' names to their HIV status. The court ruled that article 31(c) of the Constitution protects an individual against the unnecessary disclosure of information relating to their family or private affairs.[149] The court held that "the right to privacy protects the very core of the personal sphere of an individual and basically envisages the right to live one's own life with minimum interference. The right also restricts the collection, use of and disclosure of private information".[150] The court further stated that the respondents had not yet indicated how they would collect the information; neither had they indicated when the information would be collected and if it would only be done once consent had been obtained. The court held that the directive in question "amounted to compulsory testing which would be a violation of the right to privacy".[151] It is submitted that this decision indicates the court's willingness to seek clarity with regard to the way in which information is to be collected and provides more details on the justification for such collection.

In *Roshanara Ebrahim v Ashleys Kenya Limited*,[152] intimate images of the petitioner had been shared without their consent. The court posited that "the protection of privacy must serve a lawful purpose, [that is] the preservation of the petitioner's dignity in conduct that accords with the law".[153] The court stated that an expectation of privacy was reasonable where one shared intimate photos in "a boy-girl relationship" and that "although the photographs were not obtained in an intrusive manner, the purpose of the access by the friend did not include the publication thereof to third parties".[154] In its finding, the court proclaimed as follows:[155]

> Article 31(c) of the Constitution provides for the right to informational privacy which includes privacy of private photographs of a person. In taking selfie nude pictures using a mobile phone or

149 *Idem* para 112.
150 *Idem* para 69.
151 *Idem* para 78.
152 [2016] eKLR.
153 *Idem* para 27.
154 *Idem* para 29.
155 *Idem* para 38.

https://doi.org/10.47348/FUND/v30/i1a4

> other communication gadget, a person does not thereby waive her right to privacy, she only exposes herself to the risk and danger of the photographs being transmitted to and viewed by other persons through the communication networks by unauthorised access and publication, or by authorised access but unauthorised publication.

This decision indicates that consent is key if the petitioner's privacy is to be infringed; any such infringement should be justified. In this case, there was no justification for accessing and publishing the petitioner's photographs. The photographs represented personal information. It is clear that not only the state, but also private actors will be taken to task for incursions upon the right to privacy of other individuals. Furthermore, such incursions remain questionable whatever its reason, and need not be limited to having a commercial purpose only. Also, the decision highlights the fact that consent granted for a specific aspect does not equal blanket consent.

In *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre*,[156] the petition involved personality rights that were defined as "the right of an individual to control the commercial use of his or her name, image, likeness, or other unequivocal aspects of one's identity".[157] The court held personality rights to include "the right to privacy, or the right to be left alone and not have one's personality represented publicly without permission".[158] It asserted that photography and written articles may possibly encroach upon the personal life of another, which in turn may constitute a breach of privacy.[159] In its judgment, the court reasoned that a breach of privacy includes the scenario–[160]

> when there is a disclosure of true facts to outsiders contrary to the determination and will of the person concerned. A right to privacy encompasses the competence to determine the destiny of private facts, and the individual concerned is entitled to dictate the ambit and method of disclosure of such facts.

The court ruled that privacy included an individual's right "to decide for themselves who should have access to their image and

156 [2017] eKLR.
157 *Idem* para 1.
158 *Idem* para 2.
159 *Idem* para 16.
160 *Idem* para 20.

https://doi.org/10.47348/FUND/v30/i1a4

likeness – something that goes to the root of individual autonomy or privacy".[161] This decision indicates the courts' recognition of the nuanced approaches to the right to privacy. Control over personal information must be respected, especially when the information is sought for commercial purposes and is obtained without the individual's consent.

In *NWR v Green Sports Africa Ltd*,[162] the issue in contention concerned the use of minors' images to promote gambling on billboards. The court analysed personality rights, stating that it consists of "the right to privacy and the right of publicity". It further defined the right to privacy as "the right to keep one's image and likeness from exploitation without permission or compensation and generally applies to members of the general public".[163] The court considered whether there was a general reasonable expectation of privacy and held that there was a "heightened protection afforded to the privacy rights of children".[164] *In casu*, the respondents did not obtain the consent of the parents before taking the photos of the children, and were therefore in violation of the fundamental rights and freedoms of the children as protected under articles 31 and 53 of the Constitution. Essentially, the courts are keen to protect special interest groups, such as children. Legal justification remains fundamental in the commercialisation of personal data.

In *EG v Attorney General; DKM (Interested Parties); Katiba Institute (*amicus curiae*)*,[165] a case that sought the decriminalisation of gay sex, the High Court held an extremely narrow view of privacy, arguing that gay sex does not fall within the purview of the right to privacy.[166] This case dealt with the privacy concepts of personhood and intimacy. The petitioners had challenged the constitutionality of sections 162(a) and (c) and 165 of the Penal Code,[167] which make it an offence to engage in same-sex conduct. The petitioner argued that these provisions violate, among others, the right to privacy. The court disagreed and ruled that the latter provisions do not violate the Constitution or the petitioners' rights to dignity and privacy, because article 45 of the Constitution only

161 *Idem* para 21.
162 [2017] eKLR.
163 *Ibid*.
164 *Ibid*.
165 [2019] eKLR.
166 *Idem* para 395.
167 Penal Code, cap 63.

https://doi.org/10.47348/FUND/v30/i1a4

allows for the marriage between a man and a woman and, therefore, the Constitution does not contemplate same-sex relations.[168] Three points of criticism may be raised here. First, the court did not consider any other constitutional rights that would be affected by the criminalisation of gay sex, such as the right to equality and freedom from discrimination (art 27); the right to human dignity (art 28); and the right to freedom and security of the person (art 29). Secondly, the court did not uphold the need to respect personal autonomy. Thirdly, the court did not consider the potential and/or actual harm of such criminalisation, such as the discrimination and emotional distress suffered by the offenders.

This case raises the question as to whether the Data Protection Act will elicit a broad interpretation of the right to privacy by the courts or not. It is submitted that the decision wrongly interprets the Constitution and should not inform future jurisprudence on the right to privacy. Instead, the courts should rather be persuaded by the jurisprudence reflected by the case below that recognised interdependence of fundamental rights and freedoms and that broadly interpreted the right to privacy.

In *Communications Authority of Kenya v Okiya Omtatah Okoiti*,[169] the Court of Appeal overturned the decision of the High Court.[170] In the court *a quo*, the petitioner had challenged the introduction of a Device Management System (hereafter "DMS") into the networks of various telecommunication companies. The petitioner argued that the DMS had the capacity to access customers' information, which should only be accessed in a manner prescribed by law. Because there was no lawful prescription regarding it, the DMS violated Kenyans' right to privacy. The High Court agreed that the DMS violated certain constitutional provisions. The Court of Appeal rejected this argument, asserting that the High Court did not identify the actual probable evidence that led to the conclusion that the DMS would intrude on privacy, and held that even if there were issues of concern, they were still being addressed.[171]

It is submitted that the Court of Appeal failed to identify those principles pertaining to the right to privacy that ought to

168 [2019] eKLR para 405.

169 [2020] eKLR.

170 *Okiya Omtatah Okoiti V Communication Authority of Kenya* [2018] eKLR.

171 *Communications Authority of Kenya v Okiya Omtatah Okoiti* [2020] eKLR para 47.

https://doi.org/10.47348/FUND/v30/i1a4

be considered when implementing technology, such as the DMS. Nonetheless, the Court of Appeal was correct in finding that no evidence had been offered to indicate a breach of the right to privacy.

In its judgment, the High Court defined privacy as follows:[172]

> Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.

The court *a quo* held that the individual's right to privacy means that such an individual has to be able to manage their personal information and perform their personal work free from unwanted interference.[173] The right to privacy grants individuals the power to be alone; however, individual autonomy is qualified by relationships with others in a society. The High Court recognised that new challenges may impact on the right to privacy. In this case, the discussion on data protection was analysed within the context of the global information society.[174] When information technology determines almost every aspect of individuals' lives, the court confirmed that it had a duty to give constitutional importance to the freedom of individuals in a networked world. Although the Constitution protects privacy as a basic principle, the courts need to be sensitive to the needs, opportunities and dangers of freedom in the digital world.[175] The High Court emphasised that data protection is but one aspect of an individual's right to privacy. When an individual's personal data is processed by another, there should be legal protection. The court identified the processing

172 *Okiya Omtatah Okoiti v Communication Authority of Kenya* [2018] eKLR para 63.
173 *Idem* para 77.
174 *Idem* para 64.
175 *Ibid.*

https://doi.org/10.47348/FUND/v30/i1a4

of personal data as involving the collection, storage, use and distribution of information. Data processing is a potential threat to an individual's privacy. The acquisition and disclosure of false or misleading information may lead to identity infringement.[176] The court further recognised emerging threats to the right to privacy and identified technology as driving these threats.[177] As a result, the right to privacy requires that an individual have control over their personal information.[178]

Although the High Court decision was overturned, it provides a much more robust analysis and consideration of the right to privacy. In contrast, the Court of Appeal was simplistic in its consideration and analysis of the right to privacy and data protection. It is hoped that, in future cases involving state surveillance, the Kenyan courts will choose to adopt the analysis and conclusions of the High Court instead. It is not necessary for potential harm to be proven through concrete evidence as required by the Court of Appeal. It is submitted that it is more important that any potential harm not materialise at all. This is due to the fact that, once the right to privacy has been infringed, it cannot be undone.

In *PAK v Attorney General*,[179] the High Court also embraced a wide view of the right to privacy. The court was asked to determine whether the lack of access to safe abortion services is a violation of the right to privacy. The court confirmed that it was and held that "forcing someone to carry an unwanted pregnancy to term, or forcing them to seek out an unsafe abortion, is a violation of their human rights, including the rights to privacy and bodily autonomy".[180] This is a progressive and purposeful interpretation of the right to privacy with regard to bodily autonomy.

From the above discussion it is clear that the Kenyan courts generally hold progressive views on the protection of the right to privacy. The courts have aptly defined the boundaries of the right to privacy and embraced the principles of autonomy, consent, legitimate expectation, legitimate use of personal information and potential harm to the violation of the right to privacy. The exceptions to these views are demonstrated by decisions such

176 *Idem* para 65.
177 *Idem* para 73.
178 *Idem* para 74.
179 [2022] KEHC 262 (KLR).
180 *Idem* para 57.

https://doi.org/10.47348/FUND/v30/i1a4

as *EG v The Attorney General*[181] and the Court of Appeal's judgment in *Communications Authority of Kenya v Okiya Omtatah Okoiti*.[182]

Moreover, the Kenyan courts include several principles when defining the right to privacy. First, the right to privacy is an individual right. Secondly, the right to privacy is linked to other rights, such as the right to human dignity and the right to freedom from discrimination. Thirdly, the right to privacy may at times be balanced by other rights and interests, such as public policy. Fourthly, limitations to the right to privacy must be justified through constitutional principles or statutory provisions. Fifthly, such justifications for limiting the right to privacy do not apply in a blanket manner. Lastly, where an individual suffers harm due to incursions into their privacy, they are eligible to claim for damages.

5 Conclusion

This contribution describes the right to privacy within the Kenyan legal system. The independence and post-independence constitutional texts provided for an individual's right to privacy of their home and property. Both these indicated the need for consent and for justification for violating the right, and identified those circumstances where the right may be limited. However, the texts did not provide for an express individual right to privacy. It was not until the promulgation of the 2010 Constitution that the individual's right to privacy was entrenched in the constitutional text.

This study also highlights the legislation that provides for privacy rights or elements of those rights. The most important of these is the Data Protection Act 24 of 2019, which has been confirmed by the courts to have retrospective application from the date the Constitution was promulgated. The Data Protection Act unpacks the right to privacy by providing for data subject rights, data protection principles, the legitimate processing of personal data and for oversight by the Office of the Data Protection Commissioner. The Act contains certain vague provisions that may undermine the right to privacy. Such vague and overly broad provisions are to be lamented and should not apply. These include the provisions on the tasks by a public authority constituting legitimate personal data

181 *EG v Attorney General; DKM (Interested Parties); Katiba Institute (*amicus curiae*)* [2019] eKLR.

182 [2020] eKLR.

https://doi.org/10.47348/FUND/v30/i1a4

processing and on the collaboration between the Office of the Data Protection Commissioner and national security organs.

The contribution also looks at the relevant provisions of the Children Act 29 of 2002 and the HIV and AIDS Prevention and Control Act 14 of 2006 that directly address the right to privacy and confidentiality elements. These provisions of the HIV and AIDS Prevention and Control Act have been subject to disputes considered by the HIV & AIDS Tribunal, which often rules in favour of the confidentiality of HIV and AIDS status information and requires complainants to prove not only that their right to privacy has been infringed, but also that they have suffered actual harm in the process. These Acts, read together with the Data Protection Act, ensure comprehensive protection of the rights to privacy and data protection.

The Registration of Persons Act, the National Intelligence Service Act 28 of 2012, the National Police Service Act 11A of 2011 and the Private Security Regulation Act 13 of 2006 are identified as statutes limiting the right to privacy. In addition, the National Police Service Act and the Kenya Defence Forces Act 25 of 2012 expressly limit the right to privacy of certain individuals.

The case law discussed here demonstrate how the courts have repeatedly ruled in favour of the protection of the right to privacy and have demanded that the right be respected and promoted. Furthermore, the courts are not averse to interrogating action by state and non-state actors if it appears that such action potentially infringes on the right to privacy. However, with regard to the available remedies in cases where the right has been infringed, the courts have shown a disjointed approach in contemplating damages for breach of the right to privacy and data protection.

This contribution paints a picture of the past and present status of the right to privacy and of data protection in Kenya. It is evident that past regulation of the rights to privacy and data protection informs the status of the law today.[183]

183 Boorstin 1941: 424–436.

https://doi.org/10.47348/FUND/v30/i1a4

Bibliography

Books and journals

Akinyi, BA (2019) *Laws, Policies and the Right to Privacy for People Living with HIV in Kenya* (MA, University of Nairobi)

Bhat, PI (2019) *Idea and Methods of Legal Research* (Oxford)

Boorstin, DJ (1941) "Tradition and method in legal history" *Harvard LR* 54: 424–436

Boshe, P, M Hennemann & R von Meding (2022) "African data protection laws – Current regulatory approaches, policy initiatives, and the way forward" *Global Privacy LR* 3(2): 56–88

Committee of Experts on Constitutional Review (2010) *Final Report* (Nairobi) available at *https://katibaculturalrights.wordpress.com/wp-content/uploads/2016/04/coe_final_report-2.pdf* (accessed 4 Jul 2024)

Constitution of Kenya Review Commission (2005) *Final Report* (Nairobi) available at *https://kenyalaw.org/kl/fileadmin/CommissionReports/The-Final-Report-of-the-Constitution-of-Kenya-Review-Commission-2005.pdf* (accessed 4 Jul 2024)

Council of Europe (2018) *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* available at *https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a* (accessed 17 Jul 2024)

Dale, W (1993) "The making and remaking of Commonwealth constitutions" *International and Comparative L Quarterly* 42: 67–83

De Hert, P (2017) "Data protection as bundles of principles, general rights, concrete subjective rights and rules: Piercing the veil of stability surrounding the principles of data protection" *European Data Protection LR* 3: 160–179

Du Plessis, L (2011) "The status and role of legislation in South Africa as a constitutional democracy: Some exploratory observations" *PELJ* 14(4): 92–102

Dubber, MD (1998) "Historical analysis of law" *Law and History Review* 16: 159–162

Gligorijević, J (2019) "Children's privacy: The role of parental control and consent" *Human Rights LR* 19(2): 201–229

Huscroft, G, BR Miller & G Webber (eds) (2014) *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (Cambridge)

Macnish, K (2015) "An eye for an eye: Proportionality and surveillance" *Ethical Theory and Moral Practice* 18: 529–548

https://doi.org/10.47348/FUND/v30/i1a4

Muigai, G (2001) *Constitutional Amendments and the Constitutional Amendment Process in Kenya (1964–1997): A Study in the Politics of the Constitution* (PhD, University of Nairobi)

Muigai, G & D Juma (2022) *Power, Politics & Law: Dynamics of Constitutional Change in Kenya, 1887–2002* (Nairobi)

Neethling, J (2005) "The concept of privacy in South African law" *SALJ* 122: 18–28

Office of the Data Protection Commissioner (2023) "Press release" 26 Sep 2023 available at *ODPC-ISSUES-THREE-PENALTY-NOTICES-TOTALLING-TO-KSHS-9375000.pdf* (accessed 25 Jul 2024)

Roos, A (2006) "Core principles of data protection law" *CILSA* 39: 103–130

Roos, A (2009) *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD, UNISA)

Sajó, A (2007) "Independent regulatory authorities as constitutional actors: A comparative perspective" *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae* 48: 5–52

Scassa, T (2020) "A human rights-based approach to data protection in Canada" in E Dubois & F Martin-Bariteau (eds) *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa): 173–188

Silungwe, CM (2014) "On 'African' legal theory: A possibility, an impossibility or mere conundrum?" in O Onazi (ed) *African Legal Theory and Contemporary Problems: Critical Essays* (Dordrecht): 17–30

Sircar, NR & AA Maleche (2020) "Assessing a human rights-based approach to HIV testing and partner notification in Kenya: A qualitative study to examine how Kenya's policies and practices implement a rights-based approach to health" *Health and Human Rights J* 22(2): 167–176

Solove, DJ (2021) "The myth of the privacy paradox" *George Washington LR* 89: 1–51

Varuhas, JNE & NA Moreham (2018) "Remedies for breach of privacy" in JNE Varuhas & NA Moreham (eds) *Remedies for Breach of Privacy* Kindle ed (Sydney): ch 1

Woolman, S (2016a) "South Africa's aspirational Constitution and our problems of collective action" *SAJHR* 32: 156–183

Woolman, S (2016b) "Understanding South Africa's aspirational Constitution as scaffolding" *New York Law School LR* 60(2): 283–295

https://doi.org/10.47348/FUND/v30/i1a4

Legislation

Kenya

Basic Education Act, cap 211
Births and Deaths Registration Act, cap 149
Capital Markets Act, cap 485A
Central Depositories Act, cap 485C
Children Act 8 of 2001
Children Act 29 of 2022
Computer Misuse and Cybercrimes Act 5 of 2018
Constitution of Kenya, 1963
Constitution of Kenya, 2010
Data Protection Act 24 of 2019
Employment Act, cap 226
Health Act 21 of 2017
HIV and AIDS Prevention and Control Act 14 of 2006
Independent Electoral and Boundaries Commission Act, cap 7C
Insolvency Act, cap 53
Kenya Citizenship and Immigration Act 12 of 2011
Kenya Defence Forces Act 25 of 2012
Kenya Information and Communications Act, cap 411A
Kenya National Examinations Council Act, cap 214A
National Intelligence Service Act 28 of 2012
National Police Service Act 11A of 2011
Penal Code, cap 63
Private Security Regulation Act 13 of 2016
Proceeds of Crime and Anti-Money Laundering Act, cap 59A
Refugees Act 13 of 2006
Registration of Persons Act, cap 107
Statistics Act, cap 112
Universities Act, cap 210

South Africa

Constitution of the Republic of South Africa, 1996

https://doi.org/10.47348/FUND/v30/i1a4

Case law

Kenya

Aids Law Project v Attorney General [2015] eKLR

*Attorney General v Ndii; Prof Rosalind Dixon (*amicus curiae*)* [2022] KESC 8 (KLR)

COM v Standard Group Limited [2013] eKLR

Communications Authority of Kenya v Okiya Omtatah Okoiti [2020] eKLR

David Lawrence Kigera Gichuki v Aga Khan University Hospital [2014] eKLR

David Ndii v Attorney General [2021] eKLR

*EG v Attorney General; DKM; Katiba Institute (*amicus curiae*)* [2019] eKLR

Heiwua Auto Kenya Limited v The Office Commanding Police Division Central Police Station [2010] eKLR

Independent Electoral and Boundaries Commission v David Ndii; Kenya Human Rights Commission [2021] eKLR

Jacqueline Okuta v Attorney General [2017] eKLR

Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre [2017] eKLR

JK v AAR Healthcare Kenya Ltd [2020] eKLR

JLN v Director of Children Services [2014] eKLR

Kenya Legal and Ethical Network on HIV & AIDS v Cabinet Secretary Ministry of Health [2016] eKLR

Kenya Plantation and Agricultural Workers Union v James Finlay (K) Limited [2013] eKLR

NWR v Green Sports Africa Ltd [2017] eKLR

Nubian Rights Forum v Attorney General; Child Welfare Society [2020] eKLR

Okiya Omtatah Okoiti v Communication Authority of Kenya [2018] EKLR

PAK v Attorney General [2022] KEHC 262 (KLR)

Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology Ex Parte Katiba Institute; Immaculate Kasait, Data Commissioner (Interested Party) [2021] eKLR

Roshanara Ebrahim v Ashleys Kenya Limited [2016] eKLR

Samura Engineering Limited v Kenya Revenue Authority [2012] eKLR

S*KM v CBM* [2021] eKLR

Standard Newspapers Limited v Attorney General [2013] eKLR

https://doi.org/10.47348/FUND/v30/i1a4

Decisions by the (Kenyan) Office of the Data Protection Commissioner

Abubakar Hussein v Ceres Tech Limited T/A Chapaa Loan ODPC Complaint no 2194 of 2023

Emily Sila v Zerox Technology Company Limited ODPC Complaint no 2109 of 2023

Koros Kiprotich v Higher Education Loans Board ODPC Complaint no 781 of 2023

Pauline Muhanda v Safaricom PLC ODPC Complaint 1212 of 2023

International courts

Court of Justice of the European Union

Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González Case nr C-131/12 (13 May 2014)

International instruments

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 1981

International Covenant on Civil and Political Rights, 1966

Universal Declaration of Human Rights, 1948

https://doi.org/10.47348/FUND/v30/i1a4



www.juta.co.za

FUNDA0009

juta