ISSN 0012-8678

EASTERN AFRICA LAW REVIEW

ISSUE NO. 1	VOLUME 51	JUNE	2024

A JOURNAL OF LAW AND DEVELOPMENT

Published by University of Dar es Salaam School of Law
This issue was published in March 2026

EASTERN AFRICA LAW REVIEW
A Journal of Law and Development

Editor in-Chief:
Prof. H.I. Majamba, *Professor*, *School of Law, University of Dar es Salaam*

Associate Editor:
Dr. I. R. Mandi, *Lecturer, School of Law, University of Dar es Salaam*

Technical Editor:
Dr. A. Kaitu, *Lecturer, School of Law, University of Dar es Salaam*

Editorial Assistants:
Dr. G. Kiwory, *Lecturer, School of Law, University of Dar es Salaam*
Dr. V.G. Buchumi, *Lecturer, School of Law, University of Dar es Salaam*

Editorial Board:
Prof. S.J. Mramba, *Associate Professor, Law School of Tanzania*
Prof. B.S.I. Rutinwa, *Associate Professor, University of Dar es Salaam*
Prof. L.P. Shaidi, Associate Professor, *School of Law, University of Dar es Salaam*
Dr. S.F. Materu, *Senior Lecturer, School of Law, University of Dar es Salaam*
Dr. L.L. Mussa, *Senior Lecturer, School of Law, University of Dar es Salaam*

International Editorial Advisory Board:
Prof. G.M. Fimbo, *Professor Emeritus, School of Law University of Dar es Salaam*
Prof. E. Kalula, *Professor Emeritus, University of Cape Town, South Africa*
Prof. C.M. Peter, *Professor Emeritus, School of Law, University of Dar es Salaam*
Prof. I.G. Shivji, *Professor Emeritus, School of Law, University of Dar es Salaam*
Prof. U. Wanitzek, *Professor Emerita, University of Bayreuth, Germany*
Prof. Y. Fessha, *Professor, University of Western Cape, South Africa*
Prof. T. P. Milej, *Professor, Kenyatta University School of Law, Kenya*
Prof. J. Mujuzi, *Professor, University of Western Cape, South Africa*
Prof. R. Oppong, *Professor, Thomson Rivers University, Canada,*
Prof E. Situma, *Professor, University of Nairobi, Kenya*
Prof. B. Twinomugisha, *Professor, Makerere University, Uganda*
Prof. D.V. Williams, *Professor, New Zealand*
Prof. E. Kasimbazi, *Professor, Makerere University, Uganda*
Prof. J.E. Ruhangisa, *Associate Professor, Tumaini University Makumira*
Dr. R. O. Onyango, *Senior Lecturer, Kenyatta University of Agriculture, Kenya*

Review Process of the Eastern Africa Law Review, Journal of Law and Development

1. After submission of an article to the Editor in Chief, the Editor reads it and forms the first opinion whether the article is worth going through the process for publication purposes. The Editor may advise on corrections to be made as he deems fit and sends the article back to the author for necessary action. After making the corrections the author resubmits the article.

2. The Editor in Chief then sends the article to a reviewer for evaluation of the article and advises the Editorial Board on the following:
   (a) Originality and contribution to knowledge;
   (b) Relevance of the article in terms of substance;
   (c) Propriety of the format;
   (d) Whether the article should-
      - be published as it is;
      - be published after corrections indicated by the reviewer;
      - not be published at all.

3. After effecting corrections or improvements suggested by the reviewer the author resubmits the article to the Chief Editor for further processing.

4. The review team comprises all senior staff of the University of Dar es Salaam School of Law, i.e., those with PhD degrees and Professors and other qualified staff from outside the UDSM School of Law. An article is sent to a reviewer depending on the expertise of the said reviewer in the particular area of the law. The School has 13 professors who are PhD degree holders and 15 PhD degree holders who are not yet professors.

Instructions to Authors

The Editorial Board of the Eastern Africa Law Review, a Journal of Law and Development, welcomes submission of articles to be considered for publication in the journal.

Articles to be submitted should comply with the format and Guideline for Authors available at
http://www.sol.udsm.ac.tz/images/Mypdf/UDSoLJournals.pdf

All hard and soft copies of materials to be considered for publication including all correspondence, letters to the editor, notes, comments, articles and book reviews should be addressed to:

The Editor-in-Chief,
Eastern Africa Law Review,
P.O. Box 35093,
Dar es Salaam,
Tanzania.
Email: udsmlawjournals@gmail.com

Price

Price per issue exclusive of postage is TShs. 20,000 (within Tanzania)
USD 20 (outside Tanzania)

Frequency of publication

The publication is biannual: It is published in June and December.

Table of Contents

ANALYSIS OF THE FACILITATIVE RATIONALE IN DATA SUBJECT RIGHTS IN KENYA

*Josphat Idambira Ayamunda**

Abstract

Data protection law (DPL) has dual objectives: the protection of individuals and the free flow of personal data. These objectives can be conceptualised into the dualistic 'protective/facilitative' rationales. Relevant legal discourse is dominated by the protective rationale. This article employs doctrinal and comparative legal analysis to examine data subject rights in Kenya with a view to determining the extent to which they are permissive in nature and hence more facilitative of data flows than protective of individuals compared to the DPL of the European Union (EU). The analysis reveals that while the data subject rights in Kenya are generally consistent with the ones obtaining in the EU, some differences exist highlighting the permissive nature of Kenya's DPL. The study recommends an interpretation based on the often-overlooked permissive theory and, therefore, the facilitative objective of DPL in order to enable and nurture innovation within the digital economy while safeguarding data subjects.

Keywords: data protection; data subject rights; facilitative rationale; protective rationale; control; fairness

* PhD Candidate, University of Dar es Salaam, School of Law; Lecturer, Moi University School of Law. The author may be contacted through ayamunda@mu.ac.ke or ayamunda@yahoo.co.uk.

1.0 INTRODUCTION

The Data Protection Act (DPA) of Kenya is largely modelled on the General Data Protection Regulation (GDPR)[1] of the European Union (EU).[2] Moreover, the GDPR often guides Kenyan authorities' interpretations of the DPA.[3] While the EU has not yet granted an adequacy decision to Kenya, there are claims that the Kenyan DPL is essentially equivalent to the EU one and/or that it should be interpreted in the same (broad/expansive) way as in the EU focusing on the protective rationale of data protection.[4] Indeed, most literature analysing Kenyan DPL focuses on its alignment with the GDPR and human rights through the protective theoretical lens.[5] There is a lack of readily available academic literature that explicitly interrogates Kenya's DPL from a specific facilitative theoretical lens — focusing on its role in enabling personal data processing for data-driven innovation. Although some works that somewhat indirectly

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) OJEC L 119/1, 4.5.2016 (GDPR).

2 African Declaration on Internet Rights and Freedoms Coalition, "Privacy and Personal Data Protection in Africa: A Rights-based Survey of Legislation in Eight Countries", May 2021, available at <https://africaninternetrights.org> (accessed 10 June 2023).

3 See e.g., Nubian Rights Forum &2 others v. Attorney General & 6 others, Child Welfare Society & 9 others (Interested Parties) [2020] eKLR, para. 758-60.

4 See, e.g., Alunge, R., "Analyses of Selected Legal Issues Related to Personal Data Security and the Inter-Relationship between Personal Data Protection Law in Africa and Europe", PhD Thesis, University of Bologna, 2020, pp. 86-87; Wanekeya, E., "Effectiveness of Domestic Data Protection Laws in African Countries: A Case Study of the Data Protection Law in Kenya", MA Research Project Report, University of Nairobi, 2023, pp. 35-38; Nubian Rights Forum Case, Ibid.

5 See, eg, Laibuta, A.M., "Adequacy of Data Protection Regulation in Kenya", Ph.D Thesis, University of the Witwatersrand, 2023; Wanekeya, Effectiveness of Domestic Data Protection Laws in African Countries, Ibid.

examine Kenya's DPL from a permissive perspective are emerging, they do not specifically analyse the *DPA itself* as a *facilitative* regulatory framework for the data economy.[6] Instead, they tend to view the DPL more as a necessary regulatory mechanism to protect individual data subject rights, rather than as an active enabler of data-driven growth. To address this gap, this article provides a new analysis of data subject rights using under-examined tools (i.e., individual control and substantive fairness) that stem principally from the underlying theoretical assumptions about the role of data protection in society. It argues that Kenya's DPL tends to be permissive and facilitative. It proposes a different approach to the interpretation of data subject rights based on the often-overlooked permissive theory and, therefore, the facilitative objective of data protection.

This study was conducted by field research as well as a review of library-based resources. It used doctrinal, comparative and empirical legal research approaches. These methodologies were combined because they are complementary and not mutually exclusive. The doctrinal research entailed two steps. First, there was review of applicable statutory provisions. Second, there was a review of judicial precedent and administrative actions by data protection supervisory authorities. The qualitative research

---

6 Wanditi, G., "Safeguarding Personal Data: Meta Consent as a Remedy to Section 28(2)(c) of Kenya's Data Protection Act", 7(1) Strathmore Law Review, 2022, p.127; King'ori, M., "The Data Protection Act as a tool for permitting innovation and consumer safety in Kenya's digital finance market", available at <https://cipit.strathmore.edu/the-data-protection-act-as-a-tool-for-permitting-innovation-and-consumer-safety-in-kenyas-digital-finance-market/> (accessed 10 January 2026).

subcomponent entailed review of secondary materials such as scholarly books and journal articles, policy documents, government reports, guidelines, commentaries, etc. This step was intended to bridge the legal and practical aspects of data protection. The sources of data under this approach included the relevant rules regarding interpretation of data protection, cases generated under those rules, legislative history, and commentaries and literature on those rules. Under the comparative approach, the study undertook critical analysis of the relevant bodies of law in Kenya and the EU to examine how the outcome of interpretation of data subject rights could be different under each set of laws. The comparison was done on a small scale. It explored the specific question of the nature and scope of data subject rights in the two jurisdictions. It also examined why the two systems interpret the rights at issue in the way they do as well as considering their common and divergent elements. Particular attention was paid to the comparative law notion of legal transplantation. The EU is a good comparator because Kenyan DPLs are largely modelled on the GDPR and the conventional EU-influenced definition of personal data is adopted verbatim by the DPA.[7] Moreover, in their day-to-day practice, data protection stakeholders in Kenya make reference to the EU sources (despite the fact that the EU legal framework is not binding on them). The article also builds on interviews with various data protection stakeholders such as data

---

7 See, e.g., s. 2 DPA; Boshe, P., Hennemann, M. and Meding, R., "African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward", Global Privacy Law Review 2022, available at <https://ssrn.com/abstract=3947664> (accessed 9 April 2022).

controllers, data processors, data subjects, High Court judges, academics and data protection practitioners.

Doctrinal methodology is appropriate for this study because interpretation of law is largely a black letter law endeavour. However, its main limitation is the belief that doctrinal legal research "is devoid of social facts or is far away from social reality."[8] It is particularly limited when studying the practical realities of a new and evolving law like Kenya's DPL. To address this concern, this study involved considerations of the technological, political and social context in which the analysis takes place. These considerations of social value as evidenced in statutory provisions, cases, government reports, etc., provided the setting for the analysis of data subject rights. The comparative approach was chosen because it provided a critical analytical tool to distinguish particular features of the data subject rights in Kenya and the EU. Field research was chosen because it could directly address the limitations of the doctrinal approach by enriching understanding of context and accounting for socio-political or economic factors that influence data protection practices and outcomes in Kenya.

Throughout this article, the term protective objective refers to the aim of DPL to safeguard individuals against the risk of harm (to the rights and interests of the individual) that may result from the collection, use, disclosure or any other processing of their personal data. Harm in this context is broadly interpreted to include a wide

8 Vibhute, K., & Aynalem, F., "Legal Research Methods", 2009, p. 84, available at <https://chilot.files.wordpress.com> (accessed 8 December 2021).

range of loss /injury such as discrimination, anxiety, financial ruin, etc. Accordingly, 'protective rationale' is used to mean the idea of safeguarding natural persons' individual rights and interests in a strong, complete and effective manner. The protective objective is mostly a derivative of the prohibitive theory of data protection as explained below under the section on theoretical framework. Conversely, the term facilitative objective means enabling of personal data flows. That is, making it easy/possible or smoothing the way for free flow of personal data. Thus, the term 'facilitative rationale' is used to mean the substantial balancing of interests among data controllers and data subjects with a view to mitigating unfair imbalances (i.e., power and informational asymmetries) that create situations of vulnerability or impediments to data processing. The facilitative objective is mostly a derivative of the permissive theory of data protection as explained below under the section on theoretical framework. Key conceptual terms emerging from that theoretical framework are 'control' and 'fairness'. Control means both individual and architectural capacity/power to influence or determine whether and how personal data may be processed by data controllers. Fairness means the formal respect of procedures (e.g., in terms of transparency, lawfulness or accountability), as well as the substantial mitigation of power imbalances (between data controllers and data subjects) that create situations of vulnerability. This is usually attained by such measures as providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with DPL; ensuring the processing of personal data of a data subject is guided by the principles set out in the law; and providing for obligations of data controllers and processors.

This article comprises three substantive sections. The first section provides the contextual insight to reveal the underlying motivation behind the DPA and help align its interpretation with the complete DPL environment and circumstances of Kenya. It shows that the motivation for data protection in Kenya as expressed in the national data protection policy is primarily for economic reasons and less focused on individual rights. The next section introduces and lays out the basic theory behind the research. It also explains how the chosen theory manifests itself in and guides the analysis in the article. It does so by identifying control and fairness as the key distinctive features of the two theoretical lenses and using them as the analytical framework of the research. The third section makes the main contribution to the existing academic literature by applying the chosen theories to select data subject rights and related exceptions, demonstrating the extent to which the Kenyan data protection regime might actually be permissive in nature and hence more reflective of the facilitative rationale of data protection than the protective one.

2.0 POLICY BACKGROUND AND CONTEXT

As set out in this section, Kenya's data protection policy indicates that economic considerations drove the enactment of the DPA more than concerns about individual harms. As such, the DPA takes on a permissive orientation rather than a prohibitive one. The Ministry of Information, Communications and Technology (ICT) constituted the Task Force on the Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya.[9]

[9] Ministry of ICT Kenya, The Kenya Gazette 2018, Gazette Notice No. 4367, Vol. CXX - No. 56, Nairobi: Government Printer, 2018, available at

The task force produced the Data Protection Policy (2018) and the Data Protection Bill (2018) which were released for public commentary in August 2018. Under that Policy, the Kenyan government took the position that personal data is a resource to drive economic activity and create efficiencies rather than a fundamentally political object that relates to the rights and obligations of both individuals and data controllers.[10] It is also noteworthy that the task force referenced only one other policy in its Data Protection Policy namely, the National ICT Policy.[11] The ICT Policy was "designed to realise the potential of the digital economy by creating an enabling environment for all citizens and stakeholders."[12] Several pieces of evidence point in this direction.

First, the stated policy objectives included facilitating the creation and "growth of data centres, pervasive instrumentation (Internet of Things), machine learning and local manufacturing while fostering a secure, innovation ecosystem"; increasing the overall size of the digital and traditional economy to 10% of GDP by 2030, by using ICT as a foundation for the creation of a more robust economy; taking advantage of emerging trends such as the shared and gig economy by fostering an innovation and start-up ecosystem; and, gaining global recognition for innovation.[13] In light of those objectives, the policy focused on four key areas:

<http://kenyalaw.org/kenya_gazette/gazette/volume/ MTcwNg--/Vol.CXX-No.56> (accessed 5 May 2023).

10 Ministry of ICT Kenya, Data Protection Policy 2018, Nairobi: Government Printer, 2018, at p. 3.

11 Ibid.

12 Ministry of ICT Kenya, National Information, Communications and Technology (ICT) Policy, Nairobi: Government Printer, 2018, at p. 6.

13 Ibid.

mobile telephony; market; skills and innovation; and public service delivery.[14]

Second, the ICT Policy was clear that "subsequent subsidiary policy [i.e., the Data Protection Policy] will seek to create a uniform approach to the *new data centric landscape*, establishing basic principles and rules (emphasis added)."[15] This further shows that the legislator was keen on the protection of personal data for its facilitative rationale rather than protection of the individual. Broader political concerns about rights of the individual did not feature much. For instance, throughout the policy, privacy is only referred to four times in passing. In this regard, the policy says that while citizens of Kenya may request and receive a copy of their personal data and may so dispose, use and store that data as they see fit, the "Government of Kenya will retain a copy of such data, and note the demand and establish rules and regulations for the use of such deactivated data."[16] Thus, the focus on the market rather than on protective concerns was evident in how the broader data protection framework was conceived. It further implies that Kenya favoured a permissive understanding of the right to personal data protection, and therefore, narrow data subject rights.

Third, both the Data Protection Policy and the Data Protection Bill emerged out of a policy debate focused on economics and market-driven business discourses. This policy debate took place at the same time as the EU was moving away from a market-

14 Ibid.
15 Id, at p. 33.
16 Id, at p. 32.

oriented structure, in the lead up to the introduction of the GDPR. The near-identical language seen in the DPA and the GDPR suggests that the drafters might have intended to satisfy the EU requirements for adequacy. However, the local legislative process (including public participation and parliamentary input) was able to substantially alter the Bill's initial content.[17] In other words, while Kenya has a population that is largely familiar with the EU DP framework, it still adapted the DPA to local conditions through the said lawmaking processes. It was not just a blind transplantation process. This view is also supported by legal research that shows that "while the DPA has been influenced by the Brussels effect, other country specific contextual factors the including the '*Huduma* Effect' have helped to shape the DPA."[18] 'Huduma Effect' denotes Kenya's drive for digital services via Huduma Centres, leading to specific local context considerations, balancing data protection with service delivery goals and potentially different national priorities than the EU. That adaptation to local dynamics is also visible in the interpretation and application of the DPA as is discussed in section 3 of this article.

Fourth, the ICT Policy further established that "[r]egulations and laws will be enacted that specifically *ensure that data is processed fairly* and lawfully … and that clearly *establish that all data on a person is*

---

17 See, eg, Article 19 Memo annexed to the Report of the Departmental Committee on Communication, Information and Innovation on the Consideration of the Data Protection Bill, 2019, pp. 7 & 20.

18 Mukiri-Smith, H. and Leenes, R., "Beyond the 'Brussels Effect'? Kenya's Data Protection Act (DPA) 2019 and the European Union's General Data Protection Regulation (GDPR) 2018", 4 EDPL 2021, p. 502.

owned by the person."[19] Two issues emerge from this particular policy statement. First, it emphasises the essence of fairness as the overarching interpretative value built into the DPA, showing a direct permissive and facilitative orientation. In reference to the marketplace rules, the goal of the policy was to mitigate information asymmetry. In terms of what kind of rules were envisaged in that regard, the Policy states that "[t]his policy requires *carefully crafted rules that ensure that there is fairness in the market place*, that transactions are honoured, contracts and agreements are enforced, and that that scarce national resources … are fairly allocated (emphasis added)."[20] It further states that it is the goal of the Policy to "review the competitive environment for *fair* trade practices" and to "[m]aintain market integrity and competitive honesty by preventing and promptly punishing *unfair* and/or misleading market conduct (emphasis added)."[21] This is reflective of the permissive theory of data protection and is partly why this article positions the Kenyan right to data protection as a claim for fairness rather than a claim for individual control. Second, by the Policy saying that the relevant law to be established under it shall ensure that *data on a person is owned by the person* it reveals further the focus on the market-oriented structure of the DPA and reinforces its permissive nature. Though ownership rights in reference to the concept of personal data might be regarded as fundamental rights, they basically reflect the informational capitalism and pro-innovation values in the digital economy.

---

19 Ministry of ICT Kenya, National Information, Communications and Technology (ICT) Policy, above note 12, at p. 14.

20 Id, at p. 18.

21 Id, at p. 26

Fifth, still following the permissive approach, the Policy states in reference to consumer protection that the Government will protect all Kenyan citizens from unfair, deceptive or fraudulent business practices and "[d]evelop rules and regulations that maintain and ensure a free and fair marketplace."[22] This policy statement does not only reflect the right to personal data protection as an ordinary consumer protection right (rather than a fundamental right), it advances the right's permissive theory-based economic orientation and its essence as a claim for fairness in personal data processing (rather than individual control over one's personal data).

Lastly, the Policy says that the Government will, *inter alia*, "[p]romote *confidence and trust in the use of ICTs by requiring confidentiality of personal information*, integrity and availability of ICT services in Kenya"; and enact "specific and effective legislative instruments on *privacy*, security, cybercrimes, ethical and moral conduct, encryption, digital signatures, copyrights and *fair trade practices* (emphasis added)."[23] Two issues arise this policy statement. First, it is clear from the Policy that the requirement for confidentiality of personal data was not motivated by the need to protect individuals but to promote confidence and trust in the use of ICTs. Second, although the politicians and policy makers have presented this as an attempt to protect such issues as privacy, they have increasingly focused on the consumer and the market rather than the data subject. This view is reinforced by the Data Protection Policy stating that data "protection is an essential

22 Ibid.
23 Id, at p. 36.

element in maintaining public trust in entities managing Personal Data and essential for the social-economic development of Kenya in the fourth revolution."[24]

3.0 THEORIES OF DATA PROTECTION

3.1 Overview

In the academic literature on data protection, two particularly influential legal theories of data protection have emerged within the broad theoretical framework of personal data protection as a separate right from the right to privacy. They are generally known as the prohibitive theory and the permissive theory. These theories are linked to the understanding of the right to personal data protection as either a permissive or a prohibitive right. Although these two forms of understanding differ, "both start from the premise that the overarching purpose of the right is to counter the power and knowledge asymmetries that emerge, in an increasingly digitalised society, between the controllers and data subjects."[25] It should also be pointed out right from the outset that viewing the right to data protection as a prohibitive or permissive right is disputed by some academics.[26] Nevertheless, it is advocated by many other scholars.[27]

---

24 Ministry of ICT Kenya, Data Protection Policy 2018, above note 10, at p. 3.

25 Christofi, A. and Verdoodt, V., "Exploring the Essence of the Right to Data Protection in a Smart City Context: A Report in the Framework of the SPECTRE Research Project", 2019, p. 54, available at <https://spectreproject.be/> (accessed July 25 2022).

26 Vogiatzoglou, P. and Valcke, P., "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law" in Kosta, E., Leenes, R. and Kamara, I. (eds.), Research Handbook on EU Data Protection, Cheltenham: Edward Elgar, 2022, pp. 11-49, at p. 12.

27 Id, p. 28. Scholars who emphasis this approach include Clifford, 2019; Rouvroy, A. and Poullet, Y., "The Right to Informational Self-Determination and the Value of

3.2 The prohibitive theory

Under the prohibitive theory, data protection is closely linked to opacity and shielding individuals against the use of or interference with personal information relating to them. While the prohibitive theory says that data protection protects the opacity of the individual, the permissive theory says data protection channels power through transparency tools. That is to say, the prohibitive theory frames data protection law (DPL) as a prohibitive tool of opacity meant to curtail personal data processing (with a view to protecting the rights and interests of the individual data subject). Consequently, the rationale of the right to data protection is conceived as giving an individual control over their personal information. Put another way, on account of the prohibitive theory, data protection is basically a right intended to reduce information and power asymmetries between data controllers and data subjects by giving the latter control over their personal data and its processing. That way, it is hoped that the individual will be effectively protected from the harms that might arise from the processing of their personal data.

3.3 The permissive theory

The permissive theory of the right to the protection of personal data conceives the right as constituting rules regulating and limiting the processing of personal data, but not forbidding it. This permissive conception "assumes that personal data in principle may and will be processed, but asserts that such processing should

Self-Development: Reassessing the Importance of Privacy for Democracy" in Gutwirth, S., et al (eds.), Reinventing Data Protection? The Hague: Springer, 2009.

be fair".[28] In the words of Dalla Corte: "Data protection is meant to allow information sharing: there would be no need for it if there were a general prohibition of personal data disclosure, and the law very seldom prohibits the processing of personal data, rather mandating the requirements to be respected to make it lawful."[29] Thus, DPLs are *not* barriers to the processing of personal data but *permissive* laws to *enable* the use of personal data within a set of standards and safeguards designed to protect data subjects. It has also been argued that this permissive conception of the right as a tool of transparency is coherent with the generally procedural nature of personal data protection in the sense that "data protection channels a particular activity – personal data processing – by setting certain procedures and by granting a number of rights to data subjects and obligations to controllers and processors."[30]

In brief, under the permissive theory, the right to data protection enshrines a claim based on fairness, aimed at providing safeguards to personal data processing. This theory is based on the premise that "data protection is pragmatic and that allowing data processing by public and private entities is desirable – or even necessary in modern society."[31] The essence of the prohibitive approach is control, whereas the permissive approach places a premium on

---

28 Fuster, G.G. and Gurtwirth, S. "Opening up Personal Data: A Conceptual Controversy", 29 Computer Law & Security Review, 2013, p. 532.

29 Dalla Corte, L., "Safeguarding Data Protection in an Open Data World: On the Idea of Balancing Open Data and Data Protection in the Development of the Smart City Environment", Ph.D Thesis, Tilburg University, 2020, p. 148.

30 Ibid.

31 Christofi and Verdoodt, Exploring the Essence of the Right to Data Protection in a Smart City Context, above note 25, p. 54.

fairness and checks-and-balances as the essence of rights. As a permissive right, personal data protection is designed to provide safeguards to individuals whenever their personal data is processed and not to prevent data processing per se.

As a permissive regime, data protection is designed to facilitate the flow of personal data (rather than curtail it) by providing safeguards to individuals whenever their personal data is processed. That is to say, as an inherently permissive regime, data protection is meant to channel personal data processing through a set of rules rather than prohibit it *tout court*.[32] It regulates the processing (not by prohibiting it) but by setting the rules for doing it. Therefore, by framing data protection as a permissive right – a tool of transparency that defines how personal data is processed – this article emphasises the facilitative objective of data protection rather than the protective one. In light of the permissive nature of data protection, the essence of the right to data protection is framed as substantive fairness rather than individual control in reference to personal data processing.

While this theory has been hailed for pointing out that data protection is largely a procedural body of law which serves other rights and freedoms, it has been criticised for failing to focus on data protection itself.[33] According to Dalla Corte, the "theory is persuasive, and yet its main utility is to clarify the teleological

---

32 Dalla Corte, Safeguarding Data Protection in an Open Data World, above note 29, p. 156.

33 Tzanou, M., "Data Protection as a fundamental Right next to Privacy? 'Reconstructing' a not so new Right" 3(2) International Data Privacy Law, 2013, pp. 88-99, p. 93.

dichotomy between privacy and data protection, rather than the latter's substance."[34] That is to say, this theory is somewhat weak because it tries to demonstrate the added value of data protection through its distinction from privacy. Similarly, there is some concern that since the permissive approach puts forward a right to data protection by allowing and regulating processing activities through data protection principles and rights, "the permissive approach might result in a mere procedural compliance test, due to the prominent role of the principles and rights."[35] However, this concern is partly allayed by emerging studies that show that data protection law is not purely a procedural body of law.[36] For instance, while it was initially thought that the data protection principle of fairness was all about procedural fairness, it is now increasingly viewed as seeking substantive fairness.[37] In that regard, therefore, the understanding of the right to the protection of personal data from the permissive perspective is that "what is relevant is not the formal respect of procedures (in terms of transparency, lawfulness or accountability), but the substantial mitigation of unfair imbalances that create situations of vulnerability."[38]

Further criticism of the permissive theory of data protection is that the theory is essentially state-centric. The concern here appears to

---

34 Dalla Corte, Safeguarding Data Protection in an Open Data World, above note 29, p. 144.

35 Vogiatzoglou and Valcke, Two decades of Article 8 CFR, above note 26, p. 28.

36 Malgieri, G., "The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation", in Proceedings of the 2020 Conference on Fairness, Accountability and Transparency, New York: ACM, 2020, pp. 154-66.

37 Id, p. 163.

38 Ibid.

be that the theory might unduly favour the state or give the state the upper hand in balancing the dual objectives of DPL. While that concern is real, it is somewhat moderated by inherent safeguards in the theory at hand as follows. The permissive theory, by its very nature, channels processing of personal data through a set of rules. Put another way, the permissive theory is a tool of transparency and therefore safeguards against abuse of power by the state. Moreover, this theory puts emphasis on substantive fairness and as such, is better placed (than individual control) to mitigate unfair imbalances that create situations of vulnerability. The fact that the permissive theory of data protection has these in-built mechanisms which put a premium on transparency and substantive fairness (rather than opacity and individual control as does the prohibitive theory) has implications as regards its state-centric nature. Thus, any state action that might otherwise deprive individuals of protection would be moderated by these two elements.

3.4 Engaging with the theories in the analysis of data subject rights

The two theories manifest themselves in and guide the analysis in the article by providing the 'why' and 'how' explanations for observed patterns in the data subject rights at hand, allowing one to move beyond mere description to a deeper interpretation of their nature and scope. The article identifies the key distinctive features of the two theoretical lens (i.e., control and fairness) and uses them as the analytical framework. These features offer standards to judge whether the data subject right at issue leans towards a more permissive or facilitative approach in practice. Ordinarily, the prohibitive theory approaches the right to data protection as a claim for control whereas the permissive one views

the right from the perspective of a claim for substantive fairness (in the sense of balancing of interests among data controllers and data subjects with a view to mitigating power and informational asymmetries). Therefore, a data subject right that puts emphasis on giving greater control to the individual implies a protective function while one that prioritises substantive fairness suggests it is fundamentally facilitative and permissive. It should be noted that the illustrated features are not clear-cut lines but rather a matter of emphasis. These features are used variously throughout the article to represent two individualised points along an interpretative spectrum with which EU and Kenyan DPLs tend to align. For instance, a narrow right is suggestive of a bent toward the facilitative objective while a broad right orients it to the protective objective. Similarly, the greater the scope of exceptions or limitations to a given right the more the right aligns well with the facilitative objective and vice versa.

4.0 ANALYSIS OF SELECT DATA SUBJECT RIGHTS IN KENYA

4.1 The right to object to the processing of one's data for commercial purposes

The right to object is generally said to apply as an absolute right where the processing is for direct marketing, including profiling that relates to direct marketing.[39] But this right is subject to so many qualifications that are designed to facilitate data processing that in essence it turns out to be more facilitative than protective.

---

39 Kashindi, G. et al, Kenya Data Protection Law and Practice, Nairobi: Chambers and Partners, 2023, p. 13.

For instance, the data subject's right to object may be overridden if the data controller demonstrates compelling legitimate interests for processing that override the data subject's interests or for the establishment, exercise or defence of a legal claim.[40] So, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Moreover, the Cabinet Secretary, in consultation with the Data Protection Commissioner, may prescribe practice guidelines for such use.[41] While this provision has not been used by the Cabinet Secretary, it provides an extremely expansive room in reference to limitations to the protective rationale.

The better view is that the right to object to the processing of one's data for commercial purposes under s. 36 is not absolute. That right might have been absolute under s. 37 in reference to commercial use were it not for the qualification under s. 37(1)(b) regarding 'authorisation under any written law' exception. The right would also have been absolute under regulation 15(1) save for the use of the conjunction 'or' rather than 'and' in 15(1)(d). The use of 'or' suggests that a data controller or data processor may use personal data, other than sensitive personal data, concerning a data subject for the purpose of direct marketing where any of the listed conditions applies rather than only where all the conditions apply cumulatively. For instance, a controller or processor may use personal data concerning a data subject for the purpose of direct marketing where the controller or processor provides a simplified

40 DPA, s. 36.
41 DPA s. 37(3).

opt out mechanism for the data subject to request not to receive direct marketing communications or the data subject has not made an opt out request.[42] In that regard, it is noteworthy that even the proponents of the prohibitive nature of the right to personal data protection agree that regulation 15(1) waters down the right to object by granting a data controller or data processor several options.[43] In contrast, under EU DPL the right to object is absolute in reference to profiling for direct marketing purposes.[44] The watering down of that right in Kenyan DPLs is further testimony to this article's argument that the Kenyan right to personal data protection diverges from the GDPR one by taking a permissive rather than protective orientation.

In comparison to the GDPR, the DPA has a narrow approach towards commercial use of personal data in that it only regulates use of personal data for direct marketing. This Regulation is said to be too permissive of data processing and too pro-innovation in reference to the digital economy.[45] For instance, it does not directly regulate data processing related to commercial interests advanced through other means apart from direct marketing such as the use of personal data to train algorithms. In other words, the regulations provide a highly pro-growth regime for data controllers engaged in commercial and economic interests that may be articulated through means other than direct marketing.

---

42 Regulation 15(1) (d) and (e) of the Data Protection (General) Regulations, 2021, Legal Notice No. 263.

43 Laibuta, Adequacy of Data Protection Regulation in Kenya, above note 5, p. 249.

44 Art. 21 para. 2 GDPR.

45 Laibuta, Adequacy of Data Protection Regulation in Kenya, above note 5, p. 240.

4.2 The right to erasure

Generally, the GDPR provides a broad 'right to be forgotten', while the DPA's equivalent right of deletion is more narrowly applied, primarily when data is false or misleading. Under the DPA, the right to erasure does not apply where processing is done to establish, exercise or defend a legal claim; exercise the right of freedom of expression and information; comply with a legal obligation; perform a task in the public interest or in the exercise of official authority; create an archive in the public interest; or pursue scientific research, historical research or statistical purposes if the erasure is likely to seriously impair the achievement of that processing.[46] The scheme of the exceptions to this right shows that the Kenyan legislator did not intent them to be simply protective of the individual but also to primarily facilitate data processing. Indeed, in that regard, proponents of the protective rationale of the right to data protection concede that the DPA "provides for vague statutory exemptions to cater for public purpose and public interest in data processing."[47] Such provisions are couched in such terms as for "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" and "the performance of any task carried out by a public authority".[48] While these provisions may not necessarily deprive data subjects of their right to data protection, they definitely sway the emphasis on the right away from the protective rationale toward the facilitative one.

---

46 DPA, s. 40 as read together with ss. 51-55.

47 Laibuta, Adequacy of Data Protection Regulation in Kenya, above note 5, p. 28.

48 S. 30(1) (b), DPA.

Although both DPA and EU GDPR aim to give individuals control over their data, the main difference is that the EU GDPR offers a broader, more explicit right to erasure (right to be forgotten) for almost any reason, while Kenya's DPL focuses the right to erasure more narrowly on specific conditions, primarily when data is **false, outdated, incomplete, or unlawfully obtained**, requiring clear conditions for deletion rather than a general 'just because' right.[49] In essence, GDPR sets a high bar for controllers to justify *not* erasing, whereas the Kenyan DPA provides clearer grounds for deletion, often linked to consent withdrawal or data inaccuracy, but lacks GDPR's comprehensive 'forgotten' scope.[50] By offering a broader right and setting a higher bar for controllers to justify not erasing, the GDPR is clearly manifesting its strong bent toward individual control and the protective objective. Conversely, by focusing the right to erasure more narrowly on specific conditions often tied to data being inaccurate or unnecessary, Kenya's DPL is demonstrating greater focus on fairness (due process and power reversal objectives), manifesting a permissive and facilitative approach.

4.3 The right to access data

Some rights such as the right to access data[51] which were literally carried over from the EU Data Protection Directive, have been demonstrated to be more about facilitating data processing than

---

49 Reeve, R. et.al, Data Privacy and Protection in Kenya: A Regulatory Review, Nairobi: FSD Kenya, 2022, at pp. 41-44.

50 OneTrust DataGuidance, "Comparing Privacy Laws: GDPR v. Kenya Data Protection Act", p. 59, available at <https://www.dataguidance.com> (accessed 15 January 2024).

51 GDPR art. 15; DPA s. 26(b).

protecting the individual.[52] These provisions boil down to due process and power reversal objectives of DPLs. As Boshe and others demonstrate, "up until 2001, the protection of personal data in African states was only guaranteed by the constitutional right to privacy",[53] but "over a period of time, states revised or amended these provisions by adding specific protections to personal data, especially a right to access.[54] This particular development of adding specific protections to personal data, especially a right to access, is significant in one major sense. Studies that have been undertaken to analyse traditions of data protection with a view to uncovering the theoretical justification for the right to access to personal data indicate that the main and direct justifications for the right to access to personal data are twofold: due process and power reversal.[55] In sum, the essence of the right of access to personal data is the fairness of the processing of the data in question. Put another way, the right to access one's personal data gives the data subject a claim that their data is processed appropriately in line with an established system of checks and balances (including the principles of transparency and fairness), but not a claim that their data may not be processed.

4.4 The right to data portability

It is necessary to question the scope of the Kenyan right to data portability. The DPA frames the right to portability in very broad

---

52 Mahieu, R.L.P., "The Right of Access to Personal Data: A Genealogy", Technology and Regulation 2021, at p. 62.

53 Boshe, P., Hennemann, M. and Meding, R., "African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward" Global Privacy Law Review, available at <ssrn.com/abstract=3947664> (accessed 9 April 2022).

54 Ibid.

55 Mahieu, The Right of Access to Personal Data, above note 52, at p. 62.

terms compared to the GDPR. Under the GDPR, the right to data portability "should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract."[56] The fact that this right applies only when the processing is based on the data subject's consent is an intrinsic limit aimed at ensuring fair competition between service providers.[57]

In Kenya, however, this qualification – restricting the right to situations where the processing is based on the data subject's consent – is not expressly provided for in the DPA. Did the Kenyan legislator pick and choose some aspects of this right and leave out the qualification or can it be argued that the qualification is implicitly envisaged? On the face of it, the adoption of a broader right to data portability in the DPA might suggest that the Kenyan legislator intended to emphasise the protective objective. However, on bringing some critical thought to bear on it, it becomes clear that actually the intention was to de-emphasise the protective objective in the sense that individual control (in the form of consent and the data subject's freedom of contract) is disregarded in favour of free flow of personal data including in situations where the processing is not based on consent or contract. Indeed, some commentators have argued in this regard that the GDPR and the DPA bear a high degree of difference with

---

56 Recital 68 GDPR; compare art. 20 GDPR.

57 Mariavittoria, C., Handbook on the Techniques of Judicial Interactions in the Application of the EU Charter: Data Protection, Florence: European University Institute, 2021, at p. 29.

regard to the rationale, core, scope, and application of the right to data portability.[58]

In other words, by allowing the data subject to port[59] data that was collected indirectly by the data controller, the DPA is effectively turning away from individual control (in the form of consent which, prioritises individual interest at the expense of the greater social good) and instead expanding data processing beyond the narrow protective scope of the GDPR. Put another way, the Kenyan legislator is signaling that data controllers who use artificial intelligence (AI) and big data analytics to profile people in actionable ways should not have a monopoly of that information and that such information as derived from aggregated data should flow freely to spur more and further innovation.

This signal is particularly important given the current important technological and societal developments whereby Big Data, AI, quantum computing and other techniques make it even easier to infer personal data from aggregated data.[60] While aggregated data can also be personal data, the Kenyan legislator is presenting the view that the collection and use of aggregated data should not be unduly restricted by the right to portability. This suggests that the protective rationale should not be seen as an equally important

---

58 One Trust Data Guidance, "Comparing Privacy Laws: GDPR v. Kenya Data Protection Act", above note 50, at p. 59.

59 The term 'to port' is loosely used in this study to mean to move data from the system of one data controller to another system without it being changed.

60 Sloot, B., van Schendel, S. and López, C.A.F., The Influence of (Technical) Developments on the Concept of Personal Data in Relation to the GDPR, Tilburg: Tilburg Institute for Law, Technology and Society of Tilburg University, 2022, at p. 8.

rationale as the facilitative one and, as such, the former rationale can only be furthered within the boundaries set by the facilitative rationale.

4.5 The right to withdraw consent

Public conversations during the making of the DPA highlighted the need for permissive data protection in refence to the right to withdraw consent. Section 32 of the Bill provided for the right of the data subject to withdraw consent at any time. The provision was found to threaten the facilitative objective of data protection as it allowed for unrestricted withdrawal of consent whenever. To mitigate this threat, industry actors such as Digital Lenders Association of Kenya (DLAK) suggested the section be amended to include that the withdrawal of consent should not be arbitrary and should be subject to the overriding legitimate purpose of the data controller and processor.[61] DLAK reasoned that such unfettered right of withdrawal of consent by the data subject would unfairly bear on data controllers that rely on consent for provision of service.[62] Further, DLAK averred that data subjects must be informed of the process and grounds for withdrawal at the time they are giving consent.[63] The Parliamentary Committee, in upholding the right of data subjects to withdraw consent at any time, was keen to observe that caution should be taken to ensure that the procedure given by data controllers for withdrawal was not so stringent that it prevents the data subject from easily

---

61 The Report on Data Protection Bill, p. 216: "Annexed Comments by Digital Lenders Association of Kenya (DLAK): Clause 32(2) – Withdrawal of Consent of the Data Subject," (July 2019), p. 6.

62 Ibid.

63 Ibid.

withdrawing consent.[64] By data controllers providing the procedure for withdrawal, it is intimated a degree of checks and balances to ensure that lawful data processing is not hurt in the process of data subjects exercising their right to withdraw consent. This serves to promote the facilitative objective of data protection and highlights substantive fairness (rather than individual control) as its essence.

Indeed, some authors argue "that four of the conditions for lawful processing are all more or less independent of the data subject's 'will' or control (i.e., excluding the conditions of consent and contract)."[65] They question how control can be positioned as the essence of the right to data protection when "four of the conditions for lawful processing are all more or less independent of the data subject's 'will' or control (i.e. excluding the conditions of consent and contract)."[66] While some legal scholars say the RDP is about individual control over personal data and informational self-determination, others take the view that if that is the case, the law has manifestly failed because they do not think anyone could honestly say they have control over their personal data.[67]

In Kenya, one study examines a specific provision (Section 28(2)(c)) of the DPA that allows for indirect collection of personal data (from sources other than the data subject) in certain situations

---

64 The Report on Data Protection Bill, above note 61, at p. 25: "The Committee's Decision: Clause 32 – Conditions of Consent," (October 2019), para. 96.

65 Clifford, D. and Ausloos, J., "Data Protection and the Role of Fairness", (CiTiP Working Paper 29/2017, KU Leuven Centre for IT & IP Law), Leuven, 2017, p. 17.

66 Ibid.

67 Lynskey, O., "Complete and Effective Data Protection", 76 Current Legal Problems, 2023, p. 297

where a data subject previously consented.[68] It analyzes the 'permission' granted by this section arguing that it poses a significant danger to the protective objective of data protection through secondary use, highlighting a specific permissive provision in the DPA. Instructively, the DPA expands the conditions for lawful processing from the six in the GDPR to nine. The additional three bases of lawful processing in Kenya are not dependent on individual control or consent of the data subject. They include any task carried out by a public authority;[69] performance by any person of any function of a public nature;[70] and purposes of historical, statistical, journalistic, literature and art or scientific research.[71] This further expansion of the bases for lawful processing under the DPA greatly reduces the role of the will or individual control of the data subject. Consequently, it somewhat diminishes the protective rationale of the DPA and enhances its facilitative objective and therefore accords exactly with the permissive theory of data protection.

In the context of commercial use, how should the distinct rights and interests of the individual to control the processing of his personal data, the interests of businesses to continue processing the personal data collected, and the public interest in creating an optimal environment for the development of digital innovations by facilitating rather than impeding data processing be reconciled? For instance, take a business that creates promotional videos.

---

68 Wanditi, Safeguarding Personal Data, above note 6.
69 S. 30(1)(b)(v) DPA.
70 S. 30(1)(b)(vi) DPA.
71 S. 30(1)(b)(viii) DPA.

Think of the practical burden of commercial inconvenience suffered by such a business to create new promotional videos every time a data subject withdraws consent to recently created videos. Conversely, if the business in question were allowed to rely on alternative basis (e.g. legitimate interest or compliance with legal obligation) to continue processing the video made before withdrawal of consent it might deprive the concerned data subject the right to protection. One possible solution might be to consider whether continued/further processing of the data at issue (after the withdrawal of consent) amounts to a new purpose that is separate and incompatible with the initial purpose for which the personal data had been collected.[72]

4.6 The right not to be subject to automated individual decision making

Another data subject right worth interrogating in this regard is the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.[73] In both Kenya and the EU, this right does not apply, inter alia, where the decision is authorised by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.[74] In the GDPR this exception would apply, for instance, in reference to fraud and tax-evasion monitoring and prevention purposes.[75] But in such

---

72 See, eg, Cyrus Mwaniki Ndung'u v. Moja Expressway Company, ODPC Complaint Number 0264 of 2024, Final Determination, paras. 42-55.

73 DPA, s. 35 and art. 22 GDPR.

74 DPA, ss. 35(2b) and 35(5) and art. 22, paras. 2-4 GDPR.

75 Recital 71 GDPR.

concrete data processing instances in Kenya, it is highly questionable whether the applicable laws lay down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests equivalent to the EU.[76]

For instance, the CJEU declared that legislation granting public authorities access '*on a generalised basis*' to the content of electronic communications compromises the essence of the right to data protection under the Charter.[77] However, Kenyan jurisprudence on this issue suggests that the Kenyan DPL might fall short of its EU comparator in this regard. Two Kenyan cases suffice to prove this point. First there is the difficulty regarding cases under Kenyan legislation where public authorities such as the Kenya Revenue Authority (KRA) are granted access *on a generalised basis* to the content of electronic communications of Safaricom M-Pesa customers.[78] Although in 2018 the High Court ordered KRA to suspend enforcement of the relevant legal provision, the order was reversed by the Court of Appeal. Second there is the problem regarding some Kenyan banks sharing or unlawfully disclosing customer data. An instance of this is the case in Environment and Land Court in Nairobi where an Equity Bank customer is sued the Bank through Thabiti Capital claiming that his personal data was unfairly processed by the Bank by way of unlawful sharing with the Mombasa County Commissioner.[79]

---

76 High Court Judge J1, Interview by author (12 May 2023, Sawela Lodge, Naivasha).

77 Maximillian Schrems v. Data Protection Commissioner [2015] Court of Justice of the EU C-362/14, Curia, para 94.

78 Tax Procedures Act 2015, s. 60.

79 See, e.g., Kiplagat, S., "Customer Sues Equity Bank for Data Breach Dispute", Business Daily, Nairobi, 15 May 2023, available at <https://www.businessdailyafrica.com> (accessed 30 September 2023).

In the area of the criminal justice system, compliance with this obligation would likely jeopardise or prejudice the purpose of processing. If the processing of data is being conducted for the prevention and detection of crime, the capture or prosecution of offenders or the assessment or collection of tax, then there may be an exemption of many of the DPA's provisions. These include all the individual (data subject) rights; notification of data breaches; the principle of transparency; and the purpose limitation principle. For instance, take compliance with the right to inform regarding the Safaricom M-Pesa and KRA cases as well as those involving Kenyan banks alleged breaches. Should the data controllers suspect a customer or client of money laundering, the data controllers could share information, including personal data relating to the individual, with the Department of Criminal Investigations (DCI) for the purpose of further investigation. In doing so, should they be obliged to inform the data subject? Informing the individual is likely to lead to interference with investigations by the individual, e.g., through obscuring or destroying data, or even absconding. It is questionable whether noncompliance with the right to inform in such a case would be deemed to meet GDPR's requirement of appropriate measures to safeguard the data subject's rights, freedoms and legitimate interests (in particular given Kenya's somewhat uncertain rule of law record[80]).

[80] High Court Judge J1, Interview by author (12 May 2023, Sawela Lodge, Naivasha); Legal practitioner LP1, Interview by author (19 May 2023, Lake Naivasha Resort, Naivasha).

Relatedly, there is a relatively high risk of organizational dysfunctions and technical failures, including data breaches in reference to personal data shared with the DCI for the purpose of further investigation. For instance, in the *Kisorio* case,[81] the petitioner's subscriber information was provided (by the data controller) to a police officer for purposes of criminal investigations on the strength of a court order (pursuant to the Kenya Information and Communications Act, Section 27A(3)(b)). However, there was leakage of that information to third parties and, as a result, the Petitioner lost out on a business venture worth several million US dollars. Most unfortunately, it was not clear the information was leaked by the data controller or the police officer. It will be observed that this is a fairly regular occurrence in the Kenyan data protection ecosystem. So, the problem of the high risk of organizational dysfunctions and technical failures, including data breaches in Kenya is exacerbated by the evidential difficulty that effectively further weakens measures to safeguard the data subject's rights, freedoms and legitimate interests. However, the possibility of organisational dysfunction (including data /security breaches resulting from illegal acts) appears to rank lowly amongst the relevant factors to be considered when evaluating the means of identification.

Paradoxically, the Kenyan gate keepers themselves (i.e., judiciary) might also be complacent with subjecting individuals to decisions based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting data

---

81 Joshua Kiprop Kisorio v. Safaricom Plc & 4 others; Abdinajib Adan Muhumed (Interested Party) [2021] eKLR.

subjects. A case in point is the instance where some judges solely use AI to render decisions.[82] Fundamentally, the right not to be subject to automated individual decisions seems to constitute a watered down right to object because it does not obviously enable data subjects to prevent the respective processing operation totally but instead only allows them to request decision-making that affects them not to be wholly automated.[83] Moreover, this right is dependent on the data subject being aware of the particular instance of the automated processing in question. In practice, data processors hardly inform the data subjects of such activities. Even if failure to inform the individual is an offence, it is extremely difficult to enforce that controller responsibility. For example, if data controllers who subject individuals to decisions based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting data subjects, do not disclose that activity on their own volition, the affected individuals may never know that they have been subjected to such decisions.

4.7 The right to data processing in the course of a purely household activity

Lastly, one thought-provoking exception regards 'household use'. It might be useful to understand the meaning of 'household' in the African context. It could mean family circle, clan or tribe. For example, in Tanzania, a household appears to have a relatively broader scope than in Kenya, when viewed as home, family or domestic unit. This is because in Tanzania, 'household' ordinarily means 'Kaya' which is a very broad concept. One interviewee said

82 High Court Judge J1, Interview by author (12 May 2023, Sawela Lodge, Naivasha).
83 Clifford and Ausloos, Data Protection and the Role of Fairness, above note 65.

that "*watoto* means *wana wenza pia, napendekeza wazazi wa upande wa pili wawepo pia*."[84] That loosely translates to: "by the term 'one's children' is meant not only the children birthed by the person in question but also any other children that might call him or her their parent." Nonetheless, it is rather odd that the Tanzanian DPL does not provide for the household exemption. In this regard, it only exempts data processing for personal use.[85] It says that the exception applies "*ikiwa uchakataji huo unafanywa na mhusika wa taarifa katika shughuli zake binafsi*" (roughly translated as 'if it relates to the processing of personal data by the *data subject* in the course of a purely personal activity.'). The official English language version reads: "if the processing is held by the data subject for his personal use."[86] This has major implications on the scope of personal data protection. As such, the Tanzanian scope of this exemption is narrower than the Kenyan one in at least two ways. First, the Tanzanian version restricts the exception to personal use only rather than also household use. Second, the Tanzanian version appears to further narrow personal use to only use by a data subject of their own data and not that of others.

In the EU, DPL does not apply to the processing of personal data by a natural person in the course of a purely household activity.[87] In this regard 'household' simply means a house and its occupants regarded as a unit. So, household activity is partly interpreted to mean that the processing is with no connection to a professional

84 Data Processor DP1, Interview by author (1 April 2023, Nairobi).
85 The Personal Data Protection Act, s. 58(2) (a).
86 Ibid.
87 Art. 2(c) GDPR.

or commercial activity but could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.[88] It is highly questionable whether the same concept of 'household' obtains in Kenya and Africa generally. One of the idiosyncrasies of the EU law in this regard is the following. While household activity is partly interpreted to mean that the processing is with no connection to a professional or commercial activity, the notion of personal data itself is interpreted to include activities of a professional or business nature.[89] In Kenya 'household' is a broad concept including such local variants as polygamous marriages that might not be acceptable within the frame of the EU notion of household. Furthermore, there are many African customary law woman-to-woman marriages which effectively mean a broad concept of a household partly because it does not entail lesbian relationships due to the fact that the parties are not oriented towards persons of the same sex, but ropes in a wide array of partners and children. Additionally, there are households, where not only extended family members but also clans and other related kinsmen are roped in. What complicates matters even further is the fact that the term 'household' is not defined in the DPA. For that reason, a household in Kenya might mean a relatively 'small domestic entity' which in actual fact could mean a very large extended family unit. For instance, Kenyans are notorious for the peculiar model of owning and operating family businesses. In this model, family is

---

88 Recital 18 GDPR.

89 Council of Europe, "Privacy and Data Protection", available at <httpps://www.coe.int/freedom-of-expression> (accessed 13 June 2023).

business and business is family.[90] So, how do you distinguish between household activity and family business activity?

In Kenya, the Data Commissioner had opportunity to adjudicate this issue in the *Mark Ross v. Graeme Thompson Complaint.*[91] In that matter, the Data Protection Commissioner interpreted the term 'household' to mean 'domestic'. That is, a data processing activity is regarded as falling within the household exemption if it relates to the running of a home or to family relations. In reaching this interpretation, the Data Protection Commissioner referred to and followed the CJEU decision in Jehovan todistajat v *Tietosuojavaltuutettu (Jehovan).*[92] However, in light of the permissive theory of data protection, the Commissioner's application of the rule in *Jehovan* to the complaint at hand might not be particularly correct. In this particular complaint, the Commissioner considered the question of "whether the CCTV cameras in question were collecting personal data from outside the private setting of the Respondent's premises."[93] The Commissioner took the view that where the CCTV camera processes personal data outside the individual's property boundary, the processing should be regarded as extending to a public place outside the Respondent's premises or directed outwards from the Respondent's private setting.[94] As such, the Commissioner's interpretation of the household

90 Data Processor DP2, Interview by author (21 April 2023, Nairobi).
91 Mark Ross v. Graeme Thompson Complaint ODPC Complaint No. 2431 of 2023, Determination.
92 Jehovan todistajat v. Tietosuojavaltuutettu, CJEU Case C-25/17 / (10 July 2018) (Jehovan).
93 Mark Ross Case, above note 91, para. 31.
94 Id, paras. 31 & 32.

exemption in the *Mark Ross v Graeme Thompson Complaint* is too narrow and might unduly overprotect data subjects and deprive individuals the right to process personal data in reference to purely personal or domestic activities as intended by the legislator. Such a narrow interpretation of exemptions also adversely impacts the second purpose of data protection: the free flow of personal data (as is manifest in permissive theory of data protection).

Ordinarily, the household exemption is interpreted as relating only to activities which are carried out in the course of private or family life of individuals. However, the use of CCTV cameras or video surveillance is a tricky scenario. The special logic in *Ryne*[95] and related case law is that video recording cannot be regarded as an activity which is purely personal or household for the purpose of exemption under data protection law if that recording covers, even partially, a public space. While existing case law does not make it clear to what extent this logic extends beyond CCTV, certain characteristics of CCTV operations limit the reasoning in *Ryne* to CCTV surveillance. For instance, unlike other forms of video recording (e.g., items of wearable technology such as body worn cameras and video recording devices built into cyclist's helmets), fixed CCTV video surveillance systems involve the constant recording and storage of personal data. This raises the risk of harm to individuals in that it is not only an intrusive means of collecting potentially sensitive information about data subjects but does so at an extensive scale.

95 Rynes v. Urad (C-212/13) EU:C:2014:2428.

In that regard, it is important to consider the application of the reasoning in *Mark Ross v Graeme Thompson* to the operation of smart doorbell cameras. Generally, smart doorbells count as domestic CCTV as regards data protection law. Usually, the doorbell notifies an absent homeowner via a smartphone when a visitor arrives at their door. The owner can watch and talk to the visitor by using the doorbell's built-in camera and microphone. By its very nature, smart doorbell audiovisual surveillance might enable one to collect data outside their property's boundaries. In light of the permissive theory, such processing should not necessarily fall outside the scope of the household exemption as any video personal data is likely to only be *incidentally* processed if the data subject passed by on the street. Because any video personal data of an individual is likely to be collected only *incidentally* as they passed by, the property owner's legitimate interest in protecting his home whether he is there or not is not overridden by the data subject's right to avoid such incidental collection on a public street as held in the *Fairhurst* case.[96] In short, the permissive theory-based logic of the *Fairhurst* case is that a data subject's right to avoid incidental collection of their personal data is overridden by the data controller's/processor's right to protect their home. Put another way, incidental collection of (a third party's) personal data outside one's property's boundaries does not necessarily mean that processing is 'directed outwards from the private setting of the person processing the data'.

---

96 Fairhurst v. Woodard [2021] 10 WLUK 151 (CC (Oxford)) (unreported), para. 134.

Therefore, the correct interpretation of the household exception in light of the permissive theory of data protection is that the exception covers only activities which are carried out in the course of purely private or family life of individuals. It does not focus on the nature of the setting (i.e., the place from which the information is processed or the source of the processed data). What matters is the nature of the processing activity. Of course, the location or spatial element, context and *telos* of the processing might be relevant factors to consider in determining the nature of the activity. Just because an activity happens in one's household (e.g., domestic workers entering the house and carrying out their duties there on a regular basis) does not make it a data protection law exempt activity. Conversely, just because an activity happens out of one's household (e.g., a family recording videos to document their holidays or a downhill mountain biker recording her descent with an action camera) does not make it fall within the scope of data protection law. What matters is whether the 'activity' is personal or household in nature.

4.8 The public interest exception

The claim that the scheme of the exceptions to data subject rights in Kenya shows that the Kenyan legislator did not intent them to be simply protective of the individual but also to primarily facilitate data processing is exemplified by exemptions to cater for public purpose and public interest in data processing.[97] One of the permitted public interest parameters regards situations where data is processed for lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health or safety;

[97] DPA ss. 30(1) (b); 51(2)(b); 52(1)(b).

taking appropriate action in relation to suspected unlawful activity or serious misconduct; locating a person reported as missing; asserting a legal or equitable claim; conducting an alternative dispute resolution process; or performing diplomatic or consular duties.[98] In practice, the term is interpreted so broadly that it narrows down the data rights, which is a key aspect of a facilitative framework. Two cases will suffice to illustrate this point.

In *Chabari & another v Longhorn Publishers*, the Complainants were professional hikers at Mount Kenya.[99] They assisted persons taking the Kenyan flag and a copy of the 2010 Constitution to the top of the mountain and in the process, photographs were taken. They filed a complaint with the Data Commissioner alleging data subject rights violations by the Respondent whom they claimed used their photographs in an Atlas without their knowledge and for commercial purposes. The Respondent submitted that the publication of the Complainants' image was exempted from application of the Act because the Respondent reasonably believed that publication would be in the public interest. It was the Respondent's case that public interest was tied to the historic significance of the hike which marked the rebirth of the Kenya's new Constitution. The Data Commissioner was satisfied with that the publication was in the public interest and discontinued the complaint. Although the High Court found that the Data Commissioner's decision was procedurally flawed and sent the

---

98 Regulation 56 of the Data Protection (General) Regulations, 2021, Legal Notice No. 263.

99 Chabari & another v Longhorn Publishers (Civil Appeal E1338 of 2024) [2025] KEHC 13387 (KLR).

matter back to the Data Commissioner for proper consideration, the case highlights the Data Commissioner's rush to apply the public interest exception without balancing individual rights with societal benefits.[100]

Similarly, in *Faith Wavinya v Nation Media Group*[101] the Complainant filed a complaint with the Data Protection Commissioner alleging violation of data protection principles under the DPA, specifically regarding consent and use of personal data for commercial purposes. The Respondent's position was that it published an article featuring the Complainant's name, photos and likeness with a caption linking her to cigar enthusiasm in view of public interest to protect public health by informing the public that cigars might not be a safe alternative to either cigarettes or sisha.[102] The Data Commissioner agreed with the Respondent on this issue without giving any reasons except that the article in question raised issues to protect public health and safety.[103] It should be observed here that the DPA clearly states that nothing therein exempts a data controller or data processor from complying with the data protection principle relating to minimisation of collection.[104] In fact, the Complainant's position was that it was not necessary in the public interest for the Respondent to publish the Complainant's name, images and likeness in the offending article.[105] The article could have easily been published for the

---

100 Id, paras. 42-45.

101 Faith Wavinya v Nation Media Group, ODPC Complaint No. 2648 of 2023, Determination.

102 Id, para. 80.

103 Id, para. 81.

104 S. 51(1) DPA.

105 Faith Wavinya complaint, above note 101, para. 52.

alleged goal of informing the public of the adverse effects of cigar smoking without publishing the Complainant's name, images and likeness. However, the Data Commissioner did not consider this issue in arriving at the decision that the article in question fell within the exemption of public interest provided for under s. 52(1)(b) of the DPA.

The foregoing two cases accord well with the national Data Protection Policy which puts emphasis on a facilitative framework for economic interests. For instance, in the Wavinya case, by finding that the use of the personal data in question fell within the exemption of public interest without considering the overriding data minimisation principle the Data Commissioner is de-emphasising individual control and prioritising societal benefits of data processing and thus demonstrating a facilitative view. Likewise, in the Chabari case, by rushing to hold that the processing of the personal data at issue fell within the public interest exemption and failing to consider all the evidence on record adduced by the Complainant before delivering its decision, the Data Commissioner is reducing the importance or prominence of the data subject's capacity/power to influence or determine whether and how their personal data may be processed by data controllers. This reflects a tilting of the balancing of individual rights with societal benefits in favour of the facilitative rather than protective objective.

5.0 CONCLUSION

Most literature regarding the DPLs of Kenya unduly focuses on their alignment with the GDPR and human rights through the protective theoretical lens. Such an approach largely overlooks the equally important but contrasting permissive and facilitative approach. This article properly addresses this gap by providing a pioneering analysis of data subject rights in Kenya from a facilitative theoretical lens, which remains an under-explored area. Even though the DPA introduced such rights as the right to erasure, the right to object and the right to portability, they feature largely as an isolated selection of rights amongst a broader data protection framework oriented towards the market in reference to fostering innovation in personal data processing. Moreover, it is questionable whether some of these rights are truly equivalent to the GDPR ones (in terms of the extent to which they protect the individual rather than facilitate data flows). This article argues that while there are alignments of the Kenyan data subject rights with the EU ones, there are also striking divergences, which suggest that the overarching regulatory objective of the DPLs of Kenya might be more permissive in nature relative to the one obtaining in the EU.

Overall, the permissive theory and, therefore, the facilitative objective of the right to personal data protection informed every aspect of Kenya's Data Protection Policy. Kenya's approach to the data protection framework was therefore designed with a view to protecting individuals while ensuring that it does not stifle innovation, investment and economic growth. In other words, the Kenyan society decided that it is not the sole purpose of DPL to

protect individuals as general societal interests related to the use of personal data also play an important role. Accordingly, it ensured that the DPA should make it possible to use personal data in a manner acceptable to the Kenyan society. While the DPA respects the individual's right to data protection, it recognises that the individual is part of society and it is not desirable that the individual fully withdraws from society. Therefore, it puts more emphasis on fairness (rather than individual control) in order to give level protection to the inherent asymmetric data subject-controller relationships.

Therefore, data protection law in Kenya should be interpreted permissively. The permissive character of the DPLs of Kenya requires the competent interpreter to read and interpret those laws as allowing (rather than prohibiting) personal data processing and safeguarding the right through a framework of checks and balances adopted and enforced by the state with a view to reducing power and information asymmetries between ordinary citizens and those who control the processing of their personal data. By doing so, the interpreter will be promoting the attainment of the aim of the DPLs of Kenya to balance the dual objectives by counteracting power asymmetries between controllers and data subjects by offering the latter tools to strengthen their position while ensuring the free movement of personal data within an innovation-friendly digital economy.