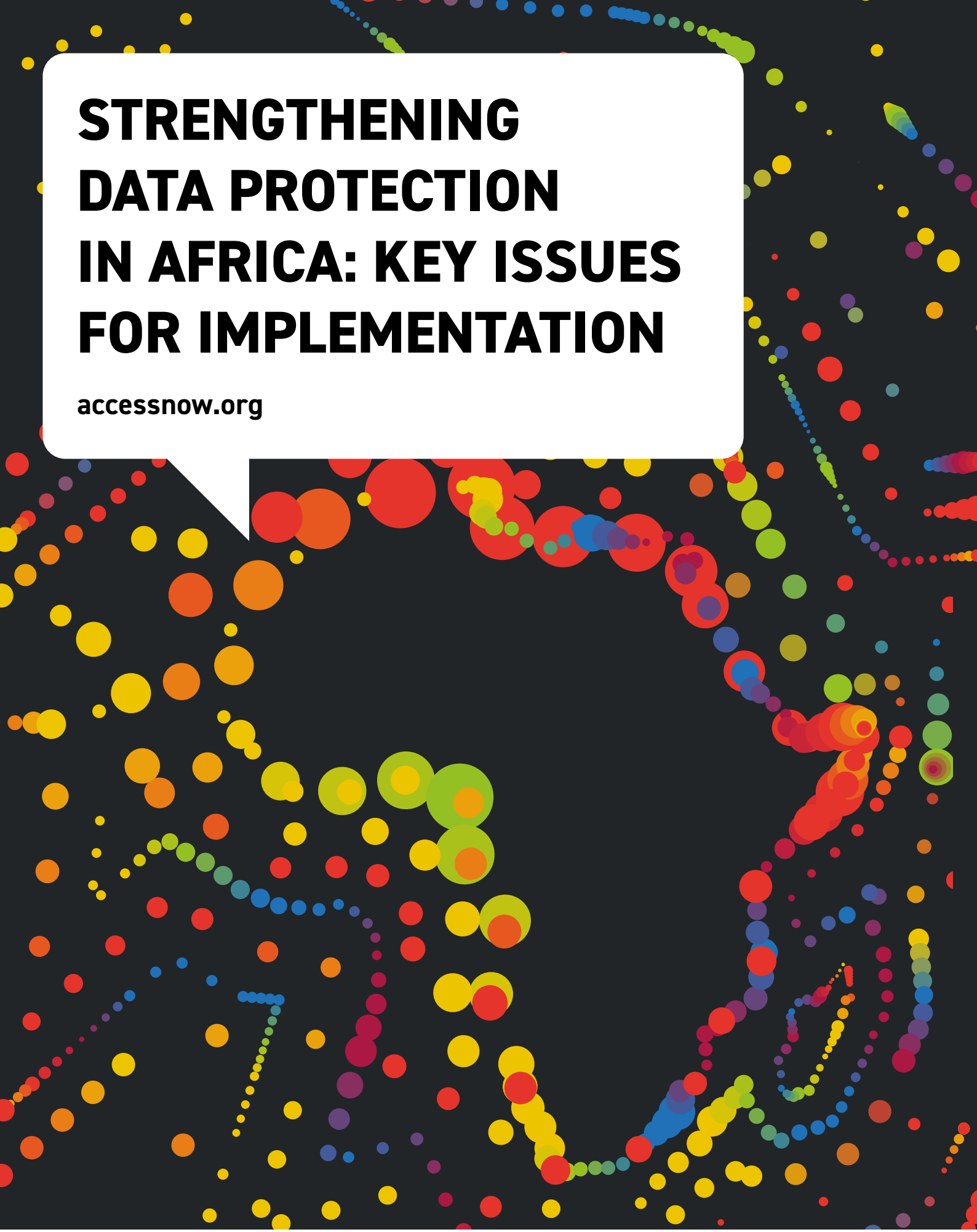
STRENGTHENING DATA PROTECTION IN AFRICA: KEY ISSUES FOR IMPLEMENTATION

accessnow.org



accessnow

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organisation, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

STRENGTHENING DATA PROTECTION IN AFRICA: KEY ISSUES FOR IMPLEMENTATION

This report is an Access Now publication. It is written by Bridget Andere and Megan Kathure. We would like to thank the Access Now team members who provided support, in particular Donna Wentworth, Chérif El Kadhi, Chiara Manfredini, Daniel Leufer, Franco Giandana, Jaimee Kokonya, Milica Pandžić, Peter Micek, and Sage Cheng.

Published in January 2024

For more information, please visit:
https://www.accessnow.org

Contact:
Bridget Andere | Senior Policy Analyst
bridget@accessnow.org

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Africa saw its first data protection law enacted in Cabo Verde in 2001[1]. Since then, 35 countries have enacted data protection laws, and as of December 2023, three others are close behind, engaging in the process of finalising their own data protection regimes. Notably, 13 of these laws were enacted in the last five years, and 24 in the last 10 years. This means that in most of these countries, data protection laws are still in the teething stage, and people are currently experiencing the impact of challenges stemming from early implementation efforts.

Despite these challenges, it is encouraging to see data protection laws gain traction in Africa, particularly considering society's race toward digitisation — especially the digitisation of government services. Given the context, it's clear that some data protection laws have been conceived and enacted to serve as enablers of digitisation programmes, including digital identification and social welfare programmes. This has at times resulted in lawmakers rushing to create legislative frameworks without adequate planning, which in turn has led to problems and delays in implementation.

Nevertheless, there has been no significant pause in the development of data protection legislation in Africa. Region-wide conventions such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo convention), and the Economic Community Of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, are a testament to the fast-gaining recognition of the importance and urgency of enacting data protection laws. We must note, however, that not all countries have ratified the conventions that apply to them.

As African governments continue to demonstrate leadership on developing data protection laws for the digital age, we look at four key issues that will be critical for ensuring these laws are implemented in a way that safeguards people's rights. Specifically, we cover the danger of broad or inappropriate exemptions; the importance of implementing both privacy and data protection regimes; the requirement for data protection authorities (DPAs) to be structurally and substantially independent; and the extent to which data protection regimes can be helpful for ensuring transparency and accountability for government and private sector use of artificial intelligence via Automated Decision Making systems (ADMs). For each issue, we offer case studies from African countries that are implementing data protection regimes, flagging where and how they can be strengthened.

[1] ALT Advisory: Cabo Verde Data Protection Factsheet https://dataprotection.africa/cabo-verde/

I. EXEMPTIONS AND WHY THEY HARM US

Over time, even as we have seen countries across Africa develop and adopt badly needed data protection laws, we have also seen lawmakers include harmful exemptions to the protections these laws offer. It is important to note that in most countries, data protection laws stem from constitutionally founded privacy laws that are not absolute and can therefore be limited by statute. Most exemptions are justified on the basis of national security or legitimate interest arguments, often to the benefit of state agencies. In many instances, these laws then serve to give people important protections with one hand, and take them away with the other.

Following are two examples of data protection laws that have a number of exemptions. As our case studies below will demonstrate, exemptions like these can open the door to rights violations and abuse. This jeopardises people's right to privacy, which is vital for safeguarding other basic rights, such as the right to free expression, a freedom that is critically important for any functioning democracy.

Kenya: The Data Protection Act, 2019

Part VII of Kenya's Data Protection Act 2019[2] contains several exemptions to data protection, including national security exemptions, court-sanctioned exemptions, journalism and art exemptions, research and history exemptions, exemptions for the data commissioner, and exemptions for data-sharing codes (which are issued by the data commissioner). It is also important to note that Section 8(2) of the act provides for a function of the data commissioner to 'collaborate with national security organs'.

Uganda: Data Protection and Privacy Act, 2019

Similar to the law in Kenya, Section 13 (3) of Uganda's Data Protection and Privacy Act,2019[3] contains dangerous exemptions, such as an exemption from the requirement to get informed consent when you collect data from a third party, if you are collecting it for national security reasons or to avoid compromising law enforcement powers.

Of course, data protection laws have their own conceptual limitations, including those to ensure the functionality of other rights and freedoms. For example, there are often limits associated with guaranteeing the right to access information, which itself has limitations. However, in this brief, we are focusing on data protection limitations, or exemptions, with potentially harmful impacts.

On the face of it, the exemptions that lawmakers have introduced in various data protection regimes across the region appear to be reasonable, not unique to Africa, and similar to what we see in laws that are widely considered as positive models, such as the European Union's General Data

[2] Kenya: The Data Protection Act, 2019. https://www.odpc.go.ke/dpa-act/
[3] The Republic of Uganda: Data Protection and Privacy Act, 2019
https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf

Protection Regulation (GDPR); see, for example, Articles 23 and 89 of the GDPR.[4] However, it is important to consider that in the GDPR, these provisions exist within the codification of limited, rights-enabling legislation. Whenever a lawmaker introduces limits to protections, they must take into account the environment within which the limitations exist, and the impact they could have on the enjoyment of one's personal rights. In the GDPR, for instance, there is a specific threshold that data processors must meet, to ensure the provisions are not applied in an overbroad or punitive manner.

Specifically, Article 23 of the GDPR, in outlining grounds for exemptions, stresses that any legislation to restrict data protection rights must have a degree of specificity with regard to the purpose and categories of data to be processed, among other factors. In Article 89, the law further specifies that any exemptions for 'public interest, scientific or historical research purposes or statistical purposes' must have appropriate safeguards. The law also outlines suggested safeguards such as pseudonymisation, and underscores the importance of ensuring data processing takes place for a specific purpose, that the data processor/controller gets consent for any new or additional processing, and that any such processing protects the identity of data subjects.

Case studies from Kenya and Uganda

// *Kenya*

In 2020, former President Uhuru Kenyatta signed into law The Statute Law (Miscellaneous Amendments) Act 2020,[5] which gave extraordinary powers to the Cabinet Secretary of Interior and Coordination of National Security to access data from any phone or computer, and introduced hefty penalties for anyone who would not comply.

In a country where there are constant attacks[6] on the right to privacy, especially for human rights defenders, journalists, and the general population, data protection laws need to be robust and difficult to bypass. Unfortunately, this amendment granted powers to the cabinet secretary that remain largely unchecked, as there is no 'check-and-balance' mechanism, such as the requirement for a court order before accessing data. This is just one instance of government disregard for Kenyans' privacy and data protection that has been codified and rationalised as necessary for national security. When government leaders approve laws like this amendment, or advance infrastructural developments such as the Digital Management System,[7] — a system intended to be

[4] European Union: General Data Protection Regulation https://gdpr-info.eu/art-89-gdpr/
[5] Kenya: The Statute Law (Miscellaneous Amendments) Act 2020 https://www.accessnow.org/wp-content/uploads/2021/01/The-Statute-Law-Miscellaneous-Amendments-Act-No.20off2020.pdf
[6] *See*: Privacy International. In Kenya, communications surveillance is a matter of life and death https://www.privacyinternational.org/news-analysis/979/kenya-communications-surveillance-matter-life-and-death; Access Now. Kenya's sneak attack on privacy: changes to the law allow government access to phone and computer data https://www.accessnow.org/kenya-right-to-privacy/
[7] Dosunmu, Damilare. Kenya's plan for tracking down counterfeit phones has digital rights activists concerned https://restofworld.org/2023/kenya-device-management-system-digital-rights-activists/

installed on all mobile networks to detect fraud and counterfeiting — they can create harmful loopholes that circumvent and undermine Kenyans' constitutional rights.

Additionally, Kenya's draft Medium-term Debt Strategy for the period 2024/25 – 2026/27[8] proposes making the revenue collecting agency, Kenya Revenue Authority, exempt from the Data Protection Act's provisions. Since this was not specifically envisioned when the law was conceptualised one can only guess what the effect would be, particularly given that most people are subject to the tax authority.

// Uganda

In August 2023, the government of Uganda announced the introduction of an 'Intelligent Transport Monitoring System'[9] to track the real-time location of all vehicles in the country, citing as a justification national security and the public interest. This system adds to the large-scale, real-time mass surveillance infrastructure that already exists in Uganda. For example, the government reportedly procured 5,552 Huawei CCTV cameras for use in public spaces,[10] claiming it is necessary for national security.

The context for these actions matters. In 2019, the Ugandan government was accused of colluding with Huawei to spy on members of the opposition party, including by intercepting their communications, according to a report from The Wall Street Journal.*[11] While the government strongly refuted[12] these allegations, this incident highlights the risks to human rights when a government can easily access people's data, especially sensitive and personally identifiable data. This kind of power in the hands of an authoritarian regime can even put people's lives at risk.*

II. WHY WE SHOULD NOT CONCEPTUALISE DATA PROTECTION LAWS AS PRIVACY LAWS

The right to privacy — which in most cases is constitutionally founded — plays an instrumental role in how lawmakers conceptualise data protection, and it can be said that data protection rights are an extension of the right to privacy. Data protection is, however, not the 'end all, be all' to the right

[8] Kenya's draft Medium-term Debt Strategy for the period 2024/25 – 2026/27
https://www.treasury.go.ke/wp-content/uploads/2023/09/Draft-MTRS-Final.pdf
[9] Uganda Infrastructure, Intelligent Transport Monitoring System (ITMS)
https://infrastructure.go.ug/intelligent-transport-monitoring-system-itms/
[10] Biryabarema,Elias. Uganda's cash-strapped cops spend $126 million on CCTV from Huawei
https://www.reuters.com/article/us-uganda-crime/ugandas-cash-strapped-cops-spend-126-million-on-cctv-from-huawei-idUSKCN1V50RF/
[11] Parkinson, Bariyo. Chin Huawei technicians helped African governments spy on political opponents
https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017
[12] Kamusiime, Wilfred. Police refutes claim of spying on opposition
https://www.upf.go.ug/police-refutes-claim-of-spying-on-opposition/

to privacy. Interpreting the right to privacy solely through the lens of data protection reduces this internationally recognised and often constitutionally founded right to a footnote in the development of our laws. To keep people safe in the digital age, it is important to continue to make the distinction between privacy and data protection, as they protect different facets of our everyday lives.

While the regulation of data processing operations is a significant and positive development in the region, lawmakers' focus on data protection as an absolute interpretation of the right to privacy has shown not only to limit the scope and efficacy of the data protection laws themselves, but also to limit state authorities' commitment to protect privacy as a universally recognised human right. Lawmakers have repeatedly turned to data protection laws when civil society raises privacy concerns related to the roll out of new policy and legislative frameworks. However, the purpose of data protection laws is not to provide political cover or theoretical areas of retreat for individuals whose fundamental privacy rights are at risk. Instead, it is intended to protect individuals and groups from the specific risks of data collection and processing, addressing the structural power asymmetry between data controllers — which can include governments — and data subjects.

To be clear, no one should discount the relevance of data protection laws in discussions on the right to privacy. However, it is imperative to understand and address the risks inherent to data collection and processing, which transcend privacy violations, as well as to separately protect the right to privacy. Following are two examples of data protection laws that have been conceptualised to subsist as privacy laws. As our case study below from Uganda demonstrates, this singular reliance on data protection as a conveyor of the right to privacy is putting people at risk, since regulations that blur the line between privacy and data protection are not likely to be adequate for protecting either one.

Uganda: Data Protection and Privacy Act, 2019 and the Data Protection and Privacy Regulations, 2020

Uganda's data protection regime is constituted of the aforementioned Data Protection and Privacy Act, 2019[13] and the Data Protection and Privacy Regulations, 2020.[14] The preamble to the Data Protection and Privacy Act specifies that the legislation is intended to '...protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors, and data controllers; to regulate the use or disclosure of personal information; and for related matters'. Section 10 of the Data Protection and Privacy Act mandates that data processors and controllers do not hold or process personal data in a manner which infringes on the privacy of a data subject.

[13] The Republic of Uganda: Data Protection and Privacy Act of 2019
https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf
[14] The Republic of Uganda: Data Protection and Privacy Regulations 2020
https://ict.go.ug/wp-content/uploads/2020/08/Data-Protection-and-Privacy-Regulation.pdf

Ghana: Data Protection Act 2012

Ghana's data protection regime was created through the Data Protection Act 2012.[15] The preamble is captured as an 'Act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information'. The Data Protection Act contains a set of data protection principles, which provide that an entity that processes data shall take into account the privacy of the individual by applying the data protection principles of accountability, lawfulness of processing, specification of purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards, and data subject participation.

Case study from Uganda

// Uganda

As we write this report, the government of Uganda is attempting to roll out a new digital ID programme, Ndaga Muntu, that relies on a data protection law as the basis for its legality. However, civil society, including Initiative for Social and Economic Rights (ISER)[16] and Unwanted Witness,[17] have brought a case to the high court that challenges the programme due to privacy concerns. As Access Now noted in our amicus brief[18] supporting the plaintiffs, '...the right to privacy also protects physical privacy — preventing bodies, homes, or private property from intrusion….' According to the UN Human Rights Council (UNHRC), this right includes bodily integrity and autonomy.

Court authorities have found that collecting biometric data without consent can amount to search of a person,[19] which implicates the right to privacy. In the context of the Ndaga Muntu programme, one could argue that a person is granting their consent when they allow authorities to capture their biometric data in order to participate in the programme. However, failure to enrol would lock a

[15] Ghana: Ghana Data Protection Act 2012 https://www.dataprotection.org.gh/media/attachments/2021/11/05/data-protection-act-2012-act-843.pdf
[16] Initiative for Social and Economic Rights (ISER). https://iser-uganda.org/
[17] Unwanted Witness. https://www.unwantedwitness.org/
[18] Access Now. In The Matter Of An Application For Leave To Intervene As Amici Curiae By The Applicants Herein Arising From Miscellaneous Cause No. 86 Of 2022 between CIPESA and 2 others & ISER and 2 others and the Attorney General Republic of Uganda and Anor https://www.accessnow.org/wp-content/uploads/2023/03/CIPESA_ACCESS-NOW_-ARTICLE-19-AMICUS-APPLICATION.pdf
[19] Madhewoo v. The State of Mauritius and Anor, 2015 SCJ 177, p. 23. Under the programme at issue, enrollment was mandatory for citizens, and any failure by a citizen to comply with the provisions of the law triggered criminal sanctions. The court found that, 'The coercive taking of fingerprints from the fingers of a person and the extracting of its minutiae would thus clearly fall within the scope of the protection afforded to the integrity and privacy of the person'. However, the court concluded that 'such interference is proportionate to the legitimate aim, i.e., prevention of identity fraud'.

person out of government benefits and services, such as social welfare and health benefits. Such 'consent' is hardly free or informed, and the existence of a data protection law does not address this fundamental privacy issue.

III. WHY DPAS SHOULD BE INDEPENDENT, ROBUST, AND COMMAND RESPECT INTERNATIONALLY

Most Data Protection Authorities (DPAs) in the African region are not substantively independent. This stems from the structuring of the offices within the laws as well as other policy factors, such as budgeting provisions. Certain laws, for instance, explicitly state or provide that DPAs must work in collaboration with specific ministries or departments. We note that some region-wide laws do state that authorities should act independently; however, at times, structural issues have appeared to undermine that purported independence.

Despite these less-than-ideal conditions, some DPAs are nevertheless issuing decisions that have a positive impact on people's data protection rights. For example, the Kenyan Office of the Data Protection Commissioner (ODPC) has issued penalties to Whitepath company and Regus for unlawful processing of data,[20] as well as penalising Oppo Kenya for using a person's photograph without consent.[21]

To understand how these authorities function, we must look at how they are resourced. The budgets for most DPAs fall under the respective dockets of the ministries they are required to work under. In Kenya, for instance, this is the Ministry of Information, Communications, and the Digital Economy, and in Uganda, the National Information Technology Authority. One must wonder how much independence there can be when your budget is not substantively under your control.

When DPAs are not independent, sufficiently resourced, or structured in a robust way, it can make them prey for bad actors seeking to exploit people's data for profit. In some cases, it is clear that foreign companies view the data protection regimes in some Global Majority countries as mere suggestions for their conduct. A notable illustration is the Worldcoin cryptocurrency fiasco[22] that put Kenyans' data security at risk. Tech for Humanity (TFH) piloted their Worldcoin programme in Kenya, attracting thousands of people willing to have their biometric data collected in return for the equivalent of Ksh. 7000. On 2 August 2023, authorities suspended Worldcoin operations in

[20] ODPC. Office of the Data Protection Commissioner issues penalty notice against Whitepath Company Limited and Regus Kenya and an enforcement notice against Ecological Industries Limited. https://www.odpc.go.ke/download/odpc-issues-penalty-notice-against-whitepath-company-limited-regus-kenya-and-an-enforcement-notice-against-ecological-industries-limited/

[21] ODPC. Office of the Data Protection Commissioner issues a penalty notice against Oppo Kenya https://www.odpc.go.ke/download/office-of-the-data-protection-commissioner-issues-a-penalty-notice-against-oppo-kenya/

[22] Njenga, Schmitz. Worldcoin: Thousands flock KICC to have eyeballs scanned for Ksh.7k https://www.citizen.digital/news/worlcoin-thousands-flock-kicc-to-have-eyeballs-scanned-for-ksh7k-n324643

Kenya, citing public safety concerns.[23] According to the ODPC, the regulator had previously ordered TFH to stop all collection of data, but the company flagrantly ignored the order.[24] The company admitted to ignoring the order, but attempted to justify this behaviour by pointing out that they had sent a letter to the ODPC asking the regulator to lift restrictions, and stated that unless the ODPC responded, TFH would consider all outstanding issues resolved and continue processing[25] people's biometric data. Since TFH did not get a response, the company said, they resumed processing.[26]

Companies like TFH are not likely to engage in this kind of behaviour if they have the perception that data protection laws in a country are robust and that infractions will carry substantial consequences. Strengthening data protection laws in Global Majority countries, including by ensuring that DPAs are independent and sufficiently resourced, can not only better protect people's rights, it can prevent foreign companies from operating in an unacceptable colonialist manner, where they benefit from the lack of accountability or recourse for those harmed by their actions.

Case studies from Kenya and Ghana

// Kenya

When ODPC's guidance has fallen short or was not provided at all, it has often been in cases with ties to other government agencies.

For example, in 2022, the Communications Authority (CA) in Kenya ordered telcos[27] to require that people re-register their SIM cards. In implementing this order, telcos collected facial biometric data, which the CA later clarified was unnecessary and ultra vires*. Some telcos have nevertheless continued to collect this data, and to date, have not been transparent regarding how much data they collected or whether they will retain it. The ODPC has stayed silent on this issue. It is worth noting that, like the ODPC, the CA works under Kenya's Ministry of Information, Communications, and The Digital Economy.*

In a second example, in 2021, many Kenyans discovered that they had been registered to political parties they had no affiliation with, without their knowledge or consent.[28] The Office of the Registrar of Political Parties (ORPP) distanced themselves from the incident, stating that they do not maintain

[23] Kenya Ministry of Interior. Statement on Worldcoin https://twitter.com/InteriorKE/status/1686709534075629568
[24] Gent, Edd. Worldcoin launched. Then came the backlash https://spectrum.ieee.org/worldcoin-2664361259
[25] *Ibid*
[26] Worldcoin. Kenya Communications Timeline https://worldcoin.org/kenya-communications-timeline
[27] Robi, Amoz. Everything you need to know on April 15 deadline for SIM cards https://www.pulselive.co.ke/news/unregistered-sim-cards-to-be-switched-off-on-april-15-communications-authority-warns/mycrbf5
[28] Mireri, Junior. Kenyans furious after being registered to 'foreign' political parties https://www.standardmedia.co.ke/counties/article/2001416132/kenyans-furious-after-being-registered-to-foreign-political-parties

political parties' registers. The ODPC responded by committing — together with the ORPP — to developing a digital platform through which people could 'resign' from the parties they were registered to, or register with their preferred parties.[29] They followed up by providing information to show people exactly how to 'resign'. Finally, in 2022, the ORPP stated that people would be notified by SMS text message before they could be registered to a political party.[30]

While these steps are positive, they are not sufficient for protecting people's data and safeguarding the democratic process. Ideally, the ODPC would have carried out an investigation, identified the parties at fault, and exercised their mandate under the law, as they have the power to take action against entities that unlawfully process people's personal data.[31] The ODPC's mandate is to ensure that potentially sensitive data does not end up in the wrong hands, and is not exploited to benefit others — especially without people's knowledge or consent.

// *Ghana*

While Ghana's data protection law[32] does not have a specific provision as to independence, the office of the Data Protection Commissioner (DPC) is conceptualised as such. Yet the reality is that it is not substantively independent. Similar to most countries in Africa, governance laws in Ghana place governing powers in other government agencies. Therefore, we see the same issues that have plagued Kenya plaguing Ghana.

For example, the DPC has never spoken out strongly or publicly to address the glaring data protection problems with the GhanaCard,[33] a digital identification programme the National Identification Authority (NIA) has fully rolled out despite major gaps that put people at risk. When administrators of the GhanaCard demanded that people re-register their SIM cards and provide biometric data, the DPC's silence was deafening, particularly considering that the Ghana Data Protection Act addresses necessity requirements and minimisation in data collection and processing. There have been multiple allegations of data breaches and forms of fraud connected to the GhanaCard,[34] with no word from the DPC. Yet moments like these are precisely when authorities should deliver on implementing the law in a way that demonstrates the legislation can in fact protect people's rights.

---

[29] Gachuhi, Kennedy. Political parties move to resolve errors in registration https://www.standardmedia.co.ke/politics/article/2001419535/parties-move-to-resolve-errors-in-registration

[30] Awich, Luke. Kenyans to receive SMS alert before being enrolled to political party https://www.the-star.co.ke/news/2022-03-03-kenyans-to-receive-alert-before-being-enrolled-to-political-party/

[31] *See*: Section 30 Kenya Data Protection Act, 2019 https://www.odpc.go.ke/dpa-act/

[32] Ghana: Ghana Data Protection Act 2012 https://www.dataprotection.org.gh/media/attachments/2021/11/05/data-protection-act-2012-act-843.pdf

[33] Introduction to the GhanaCard https://nia.gov.gh/the-ghanacard-introduction/

[34] Emmanuel Bonney. Stolen identity! Many at risk from SIM card re-registration https://www.graphic.com.gh/news/general-news/stolen-identity-many-at-risk-from-sim-card-re-registration.html

IV. HOW DATA PROTECTION LAWS CAN ENABLE GREATER ACCOUNTABILITY FOR ADM SYSTEMS

With an increase in computing power and the promise of improved efficiency, the public and private sectors are steadily accelerating the development and use of automated decision-making systems (ADMs).[35] These systems are fundamentally data-driven, relying on the mass collection and processing of data. They are used to automate human-centred procedures, practices, or policies. For instance, governments and companies use ADM systems to predict, identify, surveil, detect, and target individuals or communities,[36] for a variety of reasons. Examples are systems for 'predictive' policing, pre-trial risk assessments, school-assignment matching, fraud-detection systems, traffic-management systems, job screening tools, and face recognition.[37]

A government will not move to govern ADMs and protect people's rights if the public isn't even aware they exist. Unfortunately, not only are companies often secretive about how these systems work, public authorities are likewise opaque about how they test or use algorithmic systems in the provision of social services, or even whether they are using such systems in the first place. People affected by these systems often only find out that an ADM system was involved due to the work of investigative journalists, freedom of information requests or purely by chance.[38] When the public demands transparency and accountability, the makers of proprietary software and systems often cite intellectual property rights or trade secret protection. Yet the use of ADMs has implications on the public's rights and freedoms, such as the right to administrative review[39] among other constitutional rights. Kenya's Constitution, Article 47, affords every person the right to administrative action that is expeditious, efficient, lawful, reasonable, and procedurally fair. This right is also listed under the Bill of Rights section of the constitution.

Below, we look at how data protection laws can be used to increase transparency and accountability for ADM systems, protecting people's rights to non-discrimination and freedom of

[35] In many cases, ADM systems are also referred to as 'artificial intelligence' (AI) systems. For example, the definition of 'AI system' in the European Union's Artificial Intelligence Act is not limited to advanced machine learning systems, but also captures 'less complex' rule-based systems and many ADM systems. While we use the term ADM here, in many cases the systems we refer to could be marketed as AI systems, particularly if they involve the use of machine learning. See here for a discussion of the definition of 'AI systems' in the EU AI Act: https://www.accessnow.org/wp-content/uploads/2021/11/AI_Act_Statement_November_2021.pdf

[36] AI Now Institute, Richardson, Rashida. Confronting black boxes: a shadow report of the New York City Automated Decision System task force. https://ainowinstitute.org/publication/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated; AI Now Institute. Algorithmic Accountability Policy Toolkit https://ainowinstitute.org/wp-content/uploads/2023/04/aap-toolkit.pdf

[37] *Ibid*

[38] Lighthouse Reports, France's Digital Inquisition https://www.lighthousereports.com/investigation/frances-digital-inquisition/

[39] Beyleveld, Alexander. Questions at the interface between automated decision making, administrative law and socio-economic rights: the example of access to affordable housing in Kenya https://africlaw.com/2022/03/18/questions-at-the-interface-between-automated-decision-making-administrative-law-and-socio%E2%80%91economic-rights-the-example-of-access-to-affordable-housing-in-kenya/

information, including through requiring transparency and human rights impact assessments for the ADMs that private actors and public institutions develop and use.

Following is an example of a regime that demonstrates the relationship between data protection law and ADM accountability.

Kenya: The Data Protection Act, 2019, Data Protection (General) Regulations, 2021, Guidance Note on Data Protection Impact Assessment

Kenya's data protection law regime, specifically through the Data Protection Act, 2019, the Data Protection (General) Regulations, 2021,[40] and the Guidance Note on Data Protection Impact Assessment,[41] reins in on the use of ADMs, imposing measures such as requiring data protection impact assessments, and setting out rights for data subjects and obligations for data controllers and processors. Under the Data Protection Act, Kenyans have the general right not to be subject to a decision that is based solely on automated processing when it has a legal effect or otherwise significantly affects the individual, including the right not to be made subject to automated profiling. This general right is limited, however, where the ADM is (a) necessary for parties to enter into, or perform, a contract between the data subject and a data controller; where it is (b) 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; or is (c) based on the data subject's consent.

Kenyans enjoy further protections under the Data Protection (General) Regulations, which require data controllers and processors employing ADM systems to: inform data subjects when they engage in data processing that entails fully automated decision-making for the individual; provide meaningful information about the logic involved; ensure they meet specific transparency and fairness requirements; ensure that the data subject has the rights to oppose profiling and specifically profiling for marketing; carry out a data protection impact assessment when a processing operation is likely to result in high risk to the rights and freedoms of a data subject; process personal data in a way that eliminates discriminatory effects and bias; and ensure that a data subject can obtain human intervention and express their point of view.

These duties not only lay the foundation for accountability when data controllers or processors employ automated decision making for individuals, they also bolster requirements to protect people when controllers undertake general data processing, such as through ensuring data controllers comply with data protection principles and facilitate the enjoyment of data subjects rights. Moreover, the requirement that data controllers conduct a data protection impact assessment when they undertake processing operations in ADMs that are likely to put the data subjects' rights and freedoms at high risk represents a bulwark against ADM operations that would otherwise jeopardise citizens' socio-economic rights. Lastly, it is highly beneficial that in

[40] ODPC. The Data Protection (General) Regulations, 2021
https://www.odpc.go.ke/download/the-data-protection-general-regulations-2021-2/
[41] ODPC. Guidance Note on Data Protection Impact Assessment
https://www.odpc.go.ke/wp-content/uploads/2022/01/ODPC-guidance-note-on-Data-Protection-Impact-assessment.pdf

order to implement the data protection principle of fairness, data controllers and processors are required to incorporate human intervention. This can help to minimise the impact of biases that automated decision-making processes can deepen and exacerbate.

However, even with these measures in place – including requirements for human intervention, DPIAs or any other form of risk assessment – there is no foolproof way to operate such systems without relying on extensive goodwill or legal intervention to address the risks involved. It is pertinent to ask whether mitigation measures lawmakers are putting in place in response to identified risks are simply superficial and therefore ineffective. In cases where a DPIA is conducted, how can we ensure that it focuses objectively on people's rights, and that it is adequately, transparently, and openly conducted? Where big risks are identified, especially ones that cannot be mitigated, how can we ensure that systems will not be deployed, or will be withdrawn from use until those risks are properly addressed? We must recognise, in the end, that human intervention is not the ultimate answer for addressing the risks associated with ADMs; particularly given the well-researched issues of automation bias,[42] practicability, and the ethics of the sector.[43] It is not beyond reason, as recent history has shown, for human intervention to fall short at the most critical moments.

Case studies from Kenya and South Africa

// *Kenya*

To help make housing more affordable in Kenya, Kenya's national government is running an Affordable Housing Programme that relies on ADMs. Per framework guidelines,, the government intends to use automated profiling and credit scores to make decisions about housing applications.[44] *The system would use data about applicants to determine the credit scores, including data gathered from an applicant's device metadata, social and email data, psychometric profile data, Small and Medium Enterprise-specific data, data from telco and utilities companies, and data from credit bureaus. Per the Housing Development Framework Guidelines, the assessment of applicants' credit-worthiness would be driven by data analytics, making the credit and risk decision-making fully automated.*

While these factors implicate the application of the provision in Kenya's Data Protection Act that relates to automated decision making for individuals, they also implicate other portions of the act. The act requires data controllers to inform data subjects[45] *of the fact that their personal data is being*

[42] Antonio Coco. Exploring the Impact of Automation Bias and Complacency on Individual Criminal Responsibility for War Crimes, Journal of International Criminal Justice, 2023 https://doi.org/10.1093/jicj/mqad034
[43] Harvard Business Review. Content Moderation Is Terrible by Design https://hbr.org/2022/11/content-moderation-is-terrible-by-design
[44] Kenyan Affordable Housing Programme Development Framework https://web.archive.org/web/20220614095026/https://bomayangu.go.ke/downloads/Development_Framework_Guidelines_Release_Version.pdf
[45] Section 26

collected and for what purpose,[46] *which means that administrators implementing the Affordable Housing Programme are required to inform applicants beforehand about the collection and specific uses of their personal data.*

Lamentably, this duty to inform data subjects is limited. Under the law, data controllers or processors do not have to notify data subjects when it is not practicable for them to do so. No one should underestimate the likelihood that most data controllers will assume informing people is not practicable, as it is in their interest to do so. The fact that data controllers/processors can use the law to deflect accountability speaks to the reality that corporations have to some degree co-opted a procedure that is meant to rein in negative effects of the ADMs they sell.[47] *Data regulators should therefore pay attention to how corporate and state actors can render accountability mechanisms in regulatory instruments ineffectual.*

Other ways to ensure people's rights are protected when ADMs are used include requiring a human rights impact assessment, building in safeguards for non-discrimination, and creating transparency and accountability mechanisms.

Kenya's Data Protection (General) Regulation addresses non-discrimination through Regulation 22(2)h, which requires data controllers and processors to ensure that personal data is processed in a way that eliminates discriminatory effects and bias.

To ensure transparency for public entities implementing ADMs, it would help to create a public register of where and how ADMs are being put to use.[48] *Access Now recommends setting up such public registries as a basic first step necessary to enable more public deliberation, more accountability, and better oversight processes.*[49] *However, regardless of whether Kenyan lawmakers ultimately require public registries as part of the data protection regime, it is positive that Kenya's Data Protection Act already includes the obligation for data controllers and data processors in the public and private sectors to provide meaningful information about the logic involved, and to explain the significance and envisaged consequences of data processing.*[50]

Kenya also has measures in place for accountability. Kenyan law requires data processors and controllers to ensure that a data subject can obtain human intervention and express their point of view. Data subjects also have the right to correct and delete false or misleading data that data controllers have about them, which is an essential means of recourse, a fundamental tenet of accountability.

---

[46] Section 29
[47] Ari Ezra Waldman. Power, process, and automated decision-making https://ir.lawnet.fordham.edu/flr/vol88/iss2/9 and Privacy law's false promise https://ssrn.com/abstract=3499913
[48] Algorithm Watch. EU Artificial Intelligence Act – recommendations on public transparency; Ensure consistent and meaningful public transparency https://algorithmwatch.org/en/wp-content/uploads/2022/04/Database-issue-paperApril2022.pdf
[49] Access Now. Trust and excellence — the EU is missing the mark again on AI and human rights https://www.accessnow.org/trust-and-excellence-the-eu-is-missing-the-mark-again-on-ai-and-human-rights/
[50] Regulation 22 (2) b and Regulation 22(2) d

When governments or private companies use ADMs, it entails heightened surveillance,[51] and can serve to exacerbate inequality and discrimination. A human rights impact assessment, ex-ante *and* ex-post *application of automated decision making, can help mitigate risks. Kenya's requirement that data controllers/processors undertake a Data Protection Impact Assessment, as well as notifying data subjects when they take a decision that produces legal effects or significantly affects the data subject based solely on automated processing, can in many respects serve to satisfy the requirement for a human rights impact assessment but only if the DPIA is done in a comprehensive manner that takes into account the impact across the broad range of human rights.[52]*

// *South Africa*

South Africa's data protection law, The Protection of Personal Information Act (POPIA),[53] prescribes the conditions for the lawful processing of personal information and automated decision making.[54] Everyone has the right to have their personal information processed in accordance with the conditions for the lawful processing, including the right to be notified that personal information about them is being collected, among others.[55]

Under the law, data subjects have a general right not to be subject to a decision that results in legal consequences or otherwise affects them to a substantial degree, if the decision is based solely on the automated processing of personal information that is intended to provide a profile of their credit-worthiness, reliability, location, health, personal preferences, or conduct.

This general premise is, however, qualified under two instances. First, use of ADMs is permitted if the decision has been taken in connection with the conclusion or execution of a contract, and (i) the request of the data subject under the contract has been met; or (ii) appropriate measures have been taken to protect the data subject's legitimate interests. The referenced appropriate measures must provide an opportunity for a data subject to make representations about an automated decision, and they require a responsible party to provide the data subject with sufficient information about the underlying logic of the automated processing to enable them to make such representations. Second, use of ADMs is permitted if it is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.[56]

South Africa's data protection regime addresses concerns regarding transparency and accountability in a manner similar to Kenya's data protection framework. The requirement that data controllers

---

[51] Virginia Eubanks. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor https://virginia-eubanks.com/automating-inequality/

[52] Gaumond and Régis. Assessing Impacts of AI on Human Rights: It's Not Solely About Privacy and Nondiscrimination https://www.lawfaremedia.org/article/assessing-impacts-of-ai-on-human-rights-it-s-not-solely-about-privacy-and-nondiscrimination

[53] Republic of South Africa Protection of Personal Information Act https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

[54] Section 71

[55] Section 5

[56] Section 71(2) b

and data processors give data subjects the opportunity to make representations about an automated decision, and give them sufficient information about the underlying logic to do so, increases transparency and accountability for ADMs. So do the general rights afforded to data subjects under the law, such as the right to request the correction, destruction, or deletion of their personal information when it is necessary, and the right to lodge a complaint to the Information Regulator for any alleged interference with the protection of their personal information .

However, unlike Kenya's data protection framework, South Africa's POPIA makes no explicit demand for the elimination of discriminatory effects and bias in the processing of personal data, nor does it require a data protection impact assessment where ADM operations are likely to result in high risk to a data subject's rights and freedoms. That said, the POPIA does not disregard data subjects' rights and freedoms, as the act's provision on ADMs requires protecting data subjects' legitimate interests, which – while not sufficient – can be interpreted to include their rights and freedoms.

V. CONCLUSION AND RECOMMENDATIONS

As we have shown, data protection laws and policies are progressing and maturing across the region, with authorities gaining their footing as they work to implement the often good laws in their respective jurisdictions. For instance, at a time when people are increasingly concerned about the impact use of artificial intelligence and automated decision making systems (ADMs) have on our rights, it is encouraging to see that data protection regimes like those in Kenya and South Africa have the potential to mitigate ADM-related risks.

In the same breath, it is clear that there is room to improve and strengthen data protection laws across the region – with particular regard to their implementation. These improvements would not only serve to better protect people's constitutional and human rights, but also help prevent foreign actors from freely exploiting Africans' personal data for profit.[57] As we have noted in our analysis, to accomplish this, it's imperative to remove dangerous exemptions from data protection regulations; enact strong regulations for both data protection and privacy, instead of conflating the two; ensure data protection authorities (DPAs) are independent; and ensure that laws that regulate use of ADMs empower affected people and do not allow governments or corporations to evade their responsibility to safeguard and respect our rights.

[57] Gent, Edd. Worldcoin launched. Then came the backlash https://spectrum.ieee.org/worldcoin-2664361259

In this view, we recommend that:

- African governments join 15 states to recognise and ratify the Malabo Convention,[58] which is now in force,[59] as a first step toward recognising the importance of data protection laws and strengthening accountability across the region;

- African governments work towards sustainable models for independent data protection offices by amending laws to remove the overbearing control of other government agencies or officials, and by making substantive provisions for the resourcing of DPAs;

- Lawmakers amend data protection laws to make provisions for specificity with regard to exemptions, as overbroad exemptions have proven time and again to be harmful to the people these laws govern;

- Governments institute public registers of where and how ADMs are being put to use to ensure transparency and accountability takes centre stage in the implementation of personal data-led programmes that have far-reaching effects; and

- Governments exercise caution in investing in ADMs to avoid worsening socio-economic challenges, prioritising the secure and responsible processing of personal data, which can serve to minimise and mitigate risks for vulnerable populations.

[58] The African Union Convention on Cyber Security and Personal Data Protection https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[59] Alt Advisory. Africa: AU's Malabo Convention set to enter force after nine years https://dataprotection.africa/malabo-convention-set-to-enter-force/