# Privacy and personal data protection in Africa

## A rights-based survey of legislation in eight countries

# Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries

**Coordination team**
Koliwe Majama (APC)
Janny Montinat (APC)
Anriette Esterhuysen (APC)

**Compiled by**
Hlengiwe Dube, University of Pretoria, Centre for Human Rights
Avani Singh, ALT Advisory

**Copy editing and proofreading**
Lynne Stuart (Idea in a Forest)
Lori Nordstrom (APC)
Lynn Welburn

**Publication production and support**
Cathy Chen (APC)

**Graphic design**
Monocromo

Published by the African Declaration on Internet Rights and Freedoms Coalition
https://africaninternetrights.org
May 2021

ISBN 978-92-95113-39-8
APC-202103-CIPP-T-EN-DIGITAL-329
Supported by the Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH

# Table of contents

# Abbreviations and acronyms

| | |
|---|---|
| **ACHPR** | African Commission on Human and Peoples' Rights |
| **AfCTFA** | African Continental Free Trade Area |
| **AfDec** | African Declaration on Internet Rights and Freedoms |
| **AU** | African Union |
| **ccTLD** | Country code top-level domain |
| **CSO** | Civil society organisation |
| **DPA** | Data protection authority |
| **EAC** | East African Community |
| **ECOWAS** | Economic Community of West Africa States |
| **GDPR** | General Data Protection Regulation |
| **HRBA** | Human rights-based approach |
| **ICCPR** | International Covenant on Civil and Political Rights |
| **ICT** | Information and communications technology |
| **ISP** | Internet service provider |
| **SADC** | Southern African Development Community |
| **SDGs** | Sustainable Development Goals |
| **UDHR** | Universal Declaration of Human Rights |
| **UNHRC** | United Nations Human Rights Committee |
| **UPR** | Universal Periodic Review |

Please note that these are the abbreviations and acronyms most frequently used throughout this publication. This list is not exhaustive, as there are also numerous country-specific abbreviations and acronyms that are only used in the chapters from those particular countries.

# Introduction and overview

**Alan Finlay**
Research coordinator

Of the eight countries surveyed here, only four have comprehensive data protection privacy acts in place: Kenya, South Africa, Togo and Uganda. But as these research reports suggest, this is not necessarily a strong indicator of whether a country is committed to privacy rights, or of the efficacy of a country's legislative environment in ensuring the right to privacy and data protection.

Instead, reading across the reports, what can be described as an asymmetry between legislation and practice is evident at different levels. This asymmetry can be political – for example, Togo, an effective constitutional dictatorship marked by fierce government crackdowns on opposition and recent reports of

surveillance of religious and political leaders, enacted a data protection law in 2019, and is one of the few countries in Africa to have ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Yet, as the country author suggests, “This interest [by policy makers in digital rights] is not necessarily to protect the citizens but rather out of concern to adapt state policies to the global digital situation.”

This asymmetry also concerns the regulatory framework for the implementation of a data protection act. Amongst the countries surveyed here, South Africa was the first to pass a protection of personal information act (in 2013), but still has not implemented the necessary regulations to give practical force to the law.
In contrast, while Nigeria’s privacy law is still in draft form, it already has what the country author describes as “watershed” privacy regulations.

There is a different kind of asymmetry between many of the regional instruments that provide obligations on countries to develop corresponding legislation, with the suggestion that inter-regional laws, such as the European Union’s General Data Protection Regulation (GDPR), are more effective in shaping national legislation than instruments and conventions developed in Africa.

Global conventions and instruments provide a relatively stable framework of commitments for signatory governments to enact privacy legislation. These include the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, as well as sister conventions such as the Convention on the Rights of the Child (UNCRC) and the Convention on the Rights of Persons with Disabilities. States are

also party to the United Nation's 2013 resolution on the right to privacy in the digital age, which asserts that the ordinary rights to privacy must also be protected online.

Regional instruments and laws, particularly from the European Union (EU), also shape national privacy legislation in Africa. For example, the Council of Europe's Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data has been used in developing a draft privacy law in Namibia, while the GDPR is used as model privacy legislation and provides a necessary reference for legislative alignment – it is applicable to all EU entities, even if they are based outside of the EU.

While umbrella charters such as the African Union's Banjul Charter make no explicit mention of the right to privacy, a matrix of regional instruments on the continent can be read in the context of privacy. These include the Southern African Development Community Model Law on Data Protection, the African Commission on Human and Peoples' Rights new Declaration of Principles on Freedom of Expression and Access to Information in Africa, the African Charter on the Rights and Welfare of the Child, which uses similar but modified language to the UNCRC, the East African Community's Framework for Cyberlaws, and the African Continental Free Trade Agreement, which requires states to protect the personal data of individuals and the confidentiality of their records in the processing and dissemination of that data.

However, there is an uneven sense of the efficacy of these regional instruments in encouraging states to adopt progressive privacy legislation. For example, Ethiopia has yet to accede to any of the continent's data protection instruments but has published a Draft Personal Data Protection Proclamation. In Kenya, the

privacy rights of children are not properly legislated, despite the country's regional and global commitments. Of the countries surveyed, only Togo has ratified the Malabo Convention. Yet South Africa, as mentioned, has had a data protection law in place since 2013. Although Nigeria signed the communique adopting the Convention in 2014, it has yet to ratify it. As the country author argues: "The Convention does not have the force of law both within the country and on the continent, [and] nevertheless the national government has been taking steps towards privacy and data protection prior to and since the adoption of the Convention."

The purpose of the country reports collected here was to offer an in-depth rights-based analysis of the status of privacy and data protection legislation in the countries surveyed. The reports were part of a project by the African Declaration on Internet Rights and Freedom (AfDec) Coalition, "Strengthening a rights-based approach to data protection in Africa", whose objective was to foster a rights-based approach to the adoption and implementation of this legislation. In assessing country contexts, the authors responded to a detailed research template. This involved an analysis of a state's regional and global commitments to privacy, and of the country's legislative environment impacting on privacy, a specific analysis of the comprehensive data protection law as it exists in each country, and the identification of key privacy rights actors and institutions, including an evaluation of the data protection practices in internet country code top level domain name (ccTLD) registration and the status of the country's data protection authority. Two key frameworks used for analysis for this research were Principle 8 of the African Declaration on Internet Rights and Freedoms, which deals with privacy and personal data protection, and the human rights-based approach (HRBA) to policy and legislative development,

whose basic principles include participation, accountability, non-discrimination and equality, empowerment and legality.

The country reports offer the necessary specifics of country-level analysis which this introductory overview can merely suggest.

Table 1 summarises the status of comprehensive data privacy laws in the countries surveyed. As all country report authors point out, there is, besides this law, a mix of country-level legislation that impacts on the right to privacy. These include penal codes, competition and consumer acts, cybercrime and communications laws, health acts, freedom of information laws, and specific legislation such as those dealing with biometrics and identity documents or the registration of SIM cards. The table needs to be read in this context.

**Table 1.**

**Status of data protection legislation**

| | Status of comprehensive data protection law | Regulatory status/other |
|---|---|---|
| **Ethiopia** | No comprehensive data protection law | Draft Personal Data Protection Proclamation published in April 2020. |
| **Kenya** | Data Protection Act, 2019 | Has yet to implement the provisions of the Act, including establishing a data protection authority. |
| **Namibia** | Draft Data Protection Bill will be presented to ministers in 2021 | No regulations yet. |
| **Nigeria** | Draft Data Protection Bill published in August 2020 | National Data Protection Regulations issued in January 2019. |
| **South Africa** | Protection of Personal Information Act, 2013 | Regulations have been developed, but not implemented. Set to be fully in force mid-2021. |
| **Tanzania** | No comprehensive data protection law | Discussions on draft bill, but no draft bill has been published for public comment yet. |
| **Togo** | Data Protection Act, 2019 | Regulatory requirements, including the creation of a regulatory agency, not implemented yet. |
| **Uganda** | Data Protection and Privacy Act, 2019 | Data Protection and Privacy Regulations issued in August 2020. |

There were mixed findings on the extent to which the privacy bills and acts in the countries under study measured against AfDec's Principle 8. To a certain degree, some of the findings depended on the different interpretations of the individual country researchers, including the weight given to the relative importance of any lacunae identified.

For example, in South Africa, protections against collective "data harms" is seen as necessary – offering what the author feels is an important extrapolation of the individual data subject rights enumerated in the Declaration: "[T]his individualised empowerment may not serve marginal communities in the whole, and many forms of data harms will in fact be collective. Certainly African human rights discourse has always strongly focused on collective rights […] and the important question will become how collectivist understandings of law – facilitated by class actions or even collective forms of protection like data trusts – will emerge."

While in Kenya the right to communicate anonymously online is not guaranteed in full because "competing legislation […] waters this down," the country's Data Protection Act is also criticised because in its formulation, policy makers did not actively ensure the participation of all stakeholders. As the country author puts it, only stakeholders who were "aware" of the bill's passage participated in its creation, resulting in gaps in the legislation such as the protection of the personal data of children.

The privacy laws discussed here do appear to at least on paper strengthen the rights of individuals against unlawful state surveillance. In Namibia, the author finds that the bill caters "for the right to privacy online by protecting privacy by default, and setting out specific instances where public exemptions to the application of the Bill may apply, thereby limiting the

circumstance in which one's communication may be intercepted, surveyed or otherwise processed."

Yet there is a sense in which this should not be taken as sufficient. Ethiopia's draft proclamation is "by and large" aligned with AfDec's Principle 8, but it falls short on due process in lawful surveillance, including the ability to contest the surveillance, to seek remedies for unlawful surveillance, and in post-surveillance notification of the individual being surveilled. In Togo, where fresh evidence of unlawful surveillance of religious and political leaders has recently emerged, there is a need to strengthen oversight mechanisms, as well as independent judicial authorisation of surveillance.

Of the countries surveyed, Tanzania appears to be the least committed to actively developing a comprehensive privacy and data protection law, despite, for example, the legislated collection of fingerprint biometrics by telecoms providers for SIM card registration. These factors, including that, like Kenya, the right to communicate anonymously online is not protected, leaves Tanzania "a long way" from realising AfDec's Principle 8.

There are similarly mixed findings as to whether the privacy legislation conforms to the HRBA framework of analysis. However, both the principles of participation, and, as an extension, accountability, appear to be the weakest in application in most of the countries surveyed here.

In Ethiopia, both the current net of legislation relevant to privacy, and its draft proclamation, are seen to be generally aligned with the five HRBA principles. However, a gap in the principle of participation is observed, in that the drafting process of the proclamation has not included all relevant stakeholders, including

rights holders themselves. Participation was also seen as a shortcoming in the legislative development process in Uganda, and now there remains a need to translate the country's act and disseminate it widely. Similarly, in Togo there is a lack of broad-based public awareness of the legislation, which limits multistakeholder engagement. In Tanzania, people-centred policy and participation is dependent on the "localisation" of bills, which includes making them clear and understandable to the majority of people – a process that clearly does not happen in the country's stalled privacy bill process.

While the development of the legislation in Nigeria is said to conform with the HRBA principles, in Kenya's 12-year drafting process for that country's legislation, the principles "were not uniformly applied during the various open and closed deliberation processes." Similarly, participation is a key deficit in the law-making process there – in part due to the government's lethargy in enacting the country's Public Participation Bill (2019) in line with its constitutional requirement on public participation. As in Ethiopia, it is rights holders who are in the main excluded from participation, including people with disabilities, children and the elderly.

In South Africa, the notion of access to law-making processes should underpin participation, particularly with the creation of the country's independent data protection authority, the Information Regulator of South Africa (IRSA). Operating with insufficient funding, the IRSA is currently trying to set up an online complaints filing system in order to facilitate public complaints (and thereby strengthen accountability). Yet, as the author notes, the low level of internet penetration in rural areas in the country, and high data costs, means using the internet as a mechanism for participation is in reality limited.

As these reports point out, it is at the level of the implementation of any privacy act, including its regulations, where its efficacy as a rights enabler will become evident.

Although Togo's laws on the protection of personal data, such as in the context of biometric identification, have shown the government's willingness to develop a strong legislative environment for the use of digital technologies, the "challenge of implementing this legal framework is still considerable, especially in the field of practice." This field of practice includes, on the one hand, the private sector developing policies in line with privacy legislation, and, on the other, the strength and independence of a country's data regulatory authority – which in a country like Uganda has come under question.

The South Africa report points out that such an independent authority, while being a necessary requirement to ensure the implementation of a privacy act, also needs to be properly funded, and have on-board capacity to enact regulations.

It is also a question of political will. A key aspect of privacy legislation is that it has the potential to hold the state to account, both in terms of issues such as surveillance, but also because the state is a significant actor in the collection of personal data.

In most of the countries surveyed here, comprehensive privacy and data protection acts have yet to be tested sufficiently – some of laws are new (passed in 2019), or in draft form. Those that have been passed several years ago (as in South Africa) are only now about to enact the relevant regulations.

It is unsurprising then that a key role for civil society identified in the report recommendations is to monitor the implementation

of the privacy laws in order to hold governments to account at different levels. At the local and national level, part of this monitoring involves documenting and reporting breaches of data protection and privacy legislation. Strategic litigation may be necessary (see, for example, Ethiopia), and in South Africa the feasibility of class action suits needs to be explored. At the regional and international levels, coalitions of civil society groups need to be formed to strengthen the monitoring capacity of civil society; and civil society needs to be active at forums such as the Human Rights Council's Universal Periodic Review when countries come up for consideration.

This research provides an important benchmark for this future advocacy.

# Introduction et vue d'ensemble

**Alan Finlay**
Coordinateur de la recherche

Sur les huit pays étudiés ici, seuls quatre ont adopté des lois complètes sur la protection de la vie privée et des données : le Kenya, l'Afrique du Sud, le Togo et l'Ouganda. Mais comme le suggèrent ces rapports de recherche, cela n'est pas nécessairement un bon indicateur de l'engagement d'un pays envers la promotion du droit à la vie privée, ni de l'efficacité de l'environnement législatif d'un pays à garantir le droit à la vie privée et à la protection des données.

Au contraire, à la lecture de ces rapports, ce qui peut être décrit comme une asymétrie entre la législation et la pratique est évident à différents niveaux. Cette asymétrie peut être politique – par exemple, le Togo, véritable dictature constitutionnelle, marquée par une répression féroce de l'opposition par le

gouvernement et de récents rapports sur la surveillance des chefs religieux et politiques, a promulgué une loi sur la protection des données en 2019, et est l'un des rares pays d'Afrique à avoir ratifié la Convention de l'Union africaine sur la sécurité numérique et la protection des données à caractère personnel (Convention de Malabo). Cependant, comme le suggère l'auteur-pays, « l'[son] intérêt [des décideurs politiques pour les droits numériques] n'est pas nécessairement de protéger les citoyens, mais plutôt d'adapter les politiques de l'État à la situation numérique mondiale ».

Cette asymétrie concerne également le cadre réglementaire visant la mise en œuvre d'une loi sur la protection des données. Parmi les pays étudiés ici, l'Afrique du Sud a été le premier pays à adopter une loi sur la protection des informations personnelles (en 2013), mais n'a toujours pas mis en œuvre les réglementations nécessaires pour en assurer une application concrète. En revanche, alors que la loi sur la protection de la vie privée du Nigeria est encore à l'état de projet, elle dispose déjà de ce que l'auteur-pays décrit comme une réglementation décisive sur la protection de la vie privée.

Il existe un type d'asymétrie différent entre de nombreux instruments régionaux qui imposent aux pays l'obligation d'élaborer une législation correspondante, avec l'idée que les lois interrégionales, comme le Règlement général sur la protection des données de l'Union européenne (RGPD), sont plus efficaces pour façonner la législation nationale que les instruments et conventions élaborés en Afrique.

Les conventions et instruments mondiaux offrent un cadre relativement stable d'engagements pour que les gouvernements signataires promulguent des lois sur la protection de la vie

privée. Il s'agit notamment de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques, ainsi que de conventions connexes telles que la Convention relative aux droits de l'enfant (CDE) et la Convention relative aux droits des personnes handicapées. Les États sont également partie à la résolution des Nations Unies de 2013 sur le droit à la vie privée à l'ère du numérique, qui affirme que les droits ordinaires à la vie privée doivent également être protégés en ligne.

Des lois et des instruments régionaux, particulièrement ceux de l'Union européenne (UE), façonnent également la législation nationale sur la vie privée en Afrique. Par exemple, la Namibie a utilisé la Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel du Conseil de l'Europe pour élaborer un projet de loi sur la vie privée, tandis que le RGPD est utilisé comme modèle de lois sur la vie privée et constitue une référence nécessaire pour l'alignement législatif - il est applicable à toutes les entités de l'UE, même si elles sont basées en dehors de l'UE.

Alors que les chartes générales telles que la Charte de Banjul de l'Union africaine ne fait pas explicitement état du droit à la vie privée, une matrice d'instruments régionaux sur le continent peut être lue dans ce contexte. Il s'agit notamment de la loi type sur la protection des données de la Communauté de développement de l'Afrique australe, de la nouvelle déclaration de principes sur la liberté d'expression et l'accès à l'information en Afrique de la Commission africaine des droits de l'homme et des peuples, de la Charte africaine des droits et du bien-être de l'enfant, qui utilise un langage similaire, mais modifié, à celui de la CDE, du Cadre de la Communauté de l'Afrique de l'Est pour les droits numériques et de l'Accord de libre-échange continental africain, qui exige des États qu'ils protègent les données à caractère personnel

des personnes et la confidentialité de leurs dossiers dans le traitement et la diffusion de ces données.

Toutefois, l'efficacité de ces instruments régionaux pour encourager les États à adopter une législation progressiste en matière de protection de la vie privée reste inégale. Par exemple, l'Éthiopie n'a encore adhéré à aucun des instruments de protection des données du continent, mais a publié un projet de proclamation sur la protection des données à caractère personnel. Au Kenya, le droit à la vie privée des enfants n'est pas correctement légiféré, malgré les engagements aux niveaux régional et mondial du pays. Parmi les pays étudiés, seul le Togo a ratifié la Convention de Malabo. Pourtant, l'Afrique du Sud, comme il a été mentionné, a mis en place une loi sur la protection des données depuis 2013. Bien que le Nigeria ait signé le communiqué adoptant la convention en 2014, il ne l'a pas encore ratifiée. Comme le soutient l'auteur-pays : « la Convention n'a pas force de loi ni dans le pays ni sur le continent, [et] néanmoins le gouvernement national a pris des mesures en faveur de la protection de la vie privée et des données avant et après l'adoption de la Convention. »

L'objectif des rapports-pays recueillis ici était de proposer une analyse approfondie, basée sur les droits, de l'état de la législation en matière de protection de la vie privée et des données à caractère personnel dans les pays étudiés. Les rapports s'inscrivaient dans le cadre d'un projet de la Coalition pour la déclaration africaine des droits et libertés sur Internet (AfDec), intitulé *« Renforcer une approche basée sur les droits en matière de protection des données en Afrique »*, dont l'objectif était de favoriser une approche basée sur les droits pour l'adoption et la mise en œuvre de cette législation. Pour évaluer les contextes nationaux, les auteurs ont répondu à un modèle

de recherche détaillé. Pour cela, on a réalisé une analyse des engagements aux niveaux régional et mondial d'un État en matière de protection de la vie privée et de l'environnement législatif du pays ayant un impact sur la vie privée, une analyse spécifique de la loi globale sur la protection des données telle qu'elle existe dans chaque pays, ainsi que l'identification des principaux acteurs et institutions en matière de droits à la vie privée, y compris une évaluation des pratiques de protection des données dans l'enregistrement des noms de domaine nationaux de premier niveau sur Internet (ccTLD) et le statut de l'autorité de protection des données du pays. Deux cadres clés ont été utilisés pour l'analyse de cette recherche dont le principe huit (8) de la Déclaration africaine des droits et libertés de l'internet, qui traite de la protection de la vie privée et des données à caractère personnel, et l'approche basée sur les droits de l'homme (ABDH) pour l'élaboration des politiques et des lois, dont les principes de base comprennent la participation, la responsabilité, la non-discrimination et l'égalité, l'autonomisation et la légalité.

Les rapports-pays offrent les spécificités nécessaires à l'analyse au niveau national que cette introduction ne peut que suggérer.

Le tableau ci-dessous résume l'état d'avancement d'une législation complète sur la protection des données dans les pays étudiés. Comme le soulignent tous les auteurs des rapports nationaux, il existe, outre cette loi, un ensemble de législations nationales qui ont un impact sur le droit à la vie privée. Il s'agit notamment de codes pénaux, de lois sur la concurrence et la consommation, de lois sur la cybercriminalité et les communications, de lois sur la santé, de lois sur la liberté d'information et de lois spécifiques comme celles qui traitent de la biométrie et des documents d'identité ou de l'enregistrement des cartes SIM. Le tableau doit être lu dans ce contexte.

**Tableau 1.**

**État de la législation sur la protection des données**

| | État d'avancement de la législation globale sur la protection des données | Statut réglementaire/autre |
|---|---|---|
| **Éthiopie** | Pas de législation complète sur la protection des données | Projet de proclamation sur la protection des données à caractère personnel publié en avril 2020. |
| **Kenya** | Loi de 2019 sur la protection des données | N'a pas encore mis en œuvre les dispositions de la loi, y compris la création d'une autorité de protection des données. |
| **Namibie** | Le projet de loi sur la protection des données sera présenté aux ministres en 2021 | Pas encore de réglementation. |
| **Nigeria** | Projet de loi sur la protection des données publié en août 2020 | Règlement national sur la protection des données publié en janvier 2019. |
| **Afrique du Sud** | La loi sur la protection des informations personnelles, 2013 | Des règlements ont été élaborés, mais ne sont pas encore mis en œuvre. Prévus d'entrer pleinement en vigueur à la mi-2021. |
| **Tanzanie** | Pas de loi globale sur la protection des données | Discussions sur le projet de loi, mais aucun projet de loi n'a encore été publié pour commentaires publics. |
| **Togo** | Loi sur la protection des données (DPA) n° 2019-014 du 29 octobre 2019 | Les exigences réglementaires, y compris la création d'une agence de régulation, ne sont pas encore mises en œuvre. |
| **Ouganda** | Loi sur la protection des données et de la vie privée, 2019 | Règlement sur la protection des données et de la vie privée publié en août 2020. |

Les résultats de la mesure dans laquelle les lois et les projets de loi sur la protection de la vie privée dans les pays étudiés se mesurent au principe 8 de l'AfDec sont mitigés. Dans une certaine mesure, certaines des conclusions dépendaient des différentes interprétations des chercheurs pour chaque pays, y compris le poids accordé à l'importance relative de chaque lacune identifiée.

Par exemple, en Afrique du Sud, on juge nécessaire d'assurer une protection contre les « dommages collectifs causés aux données » - offrant ce que l'auteur estime être une extrapolation importante des droits individuels des personnes concernées énumérés dans la Déclaration : « [cette] sa responsabilisation individualisée ne servira peut-être pas les communautés marginales dans leur ensemble, et de nombreuses formes de préjudices liés aux données seront en fait collectives. Il est certain que le discours africain sur les droits de l'homme a toujours été fortement axé sur les droits collectifs... et la question importante sera de savoir comment les conceptions collectivistes du droit - facilitées par les recours collectifs ou même les formes collectives de protection comme les fonds de données - émergeront... ».

Alors qu'au Kenya, le droit de communiquer anonymement en ligne n'est pas pleinement garanti parce que « la législation concurrente édulcore la situation », la loi sur la protection des données est également critiquée parce que dans sa formulation, les décideurs politiques n'ont pas précisément assuré la participation de toutes les parties prenantes. Comme le dit l'auteur-pays, seules les parties prenantes qui étaient « au courant » de l'adoption du projet de loi ont participé à sa création, ce qui a entraîné des lacunes dans la législation telles que la protection des données à caractère personnels des enfants.

Les lois sur la protection de la vie privée dont il est question ici semblent effectivement renforcer, du moins sur papier, les droits des individus contre la surveillance illégale de l'État. En Namibie, l'auteur estime que le projet de loi « couvre le droit à la vie privée en ligne en protégeant par défaut la vie privée et en définissant des cas spécifiques d'exemptions publiques à l'application du projet de loi, limitant ainsi les cas dans lesquels une communication peut être interceptée, surveillée ou traitée ».

Cependant, on peut penser que cela ne devrait pas être considéré comme suffisant. Le projet de proclamation de l'Éthiopie est « dans l'ensemble » aligné sur le principe 8 de l'AfDec, mais il ne respecte pas les règles de procédure en matière de surveillance légale, notamment la possibilité de contester la surveillance, de demander réparation en cas de surveillance illégale et de notifier la personne surveillée après la surveillance. Au Togo, où de nouvelles preuves de surveillance illégale de dirigeants religieux et politiques sont apparues récemment, il est nécessaire de renforcer les mécanismes de surveillance, ainsi que l'autorisation judiciaire indépendante de la surveillance.

Parmi les pays étudiés, la Tanzanie semble être le pays le moins enclin à élaborer activement une loi globale sur la protection de la vie privée et des données, malgré, par exemple, la collecte légalisée d'empreintes digitales biométriques par les fournisseurs des services de télécommunications pour l'enregistrement des cartes SIM. Ces facteurs, notamment le fait que, comme au Kenya, le droit de communiquer anonymement en ligne n'est pas protégé, font que la Tanzanie est encore « loin » d'adhérer au principe 8 de l'AfDec.

Les conclusions sont tout aussi mitigées quant à savoir si la législation sur la protection de la vie privée est conforme au cadre d'analyse de l'ABDH. Mais il semble que les principes de participation et, par extension, de responsabilité, sont les moins bien appliqués dans la plupart des pays étudiés ici.

En Éthiopie, le dispositif législatif actuel relatif à la protection de la vie privée et son projet de proclamation sont considérés comme généralement conformes aux cinq principes de l'ABDH. Toutefois, le principe de participation n'est pas bien observé, dans la mesure où toutes les parties prenantes concernées, y

compris les titulaires de droits eux-mêmes, n'ont pas participé au processus de rédaction de la proclamation. La participation a également été jugée déficiente dans le processus d'élaboration de la législation en Ouganda, et il reste maintenant à traduire la loi et à la diffuser largement. De même, au Togo, le public n'est pas suffisamment sensibilisé à la législation, ce qui limite l'engagement des différentes parties prenantes. En Tanzanie, la politique et la participation centrées sur la population dépendent de la « localisation » des projets de loi, ce qui implique de les rendre clairs et explicites pour la majorité des gens - un processus qui ne se produit manifestement pas dans le cadre du projet de loi sur la protection de la vie privée du pays, qui est au point mort.

Alors que l'élaboration de la législation au Nigeria est censée être conforme aux principes de l'approche basée sur les droits de l'homme, au cours des douze années de rédaction de la législation kényane, les principes « n'ont pas été appliqués uniformément au cours des différents processus de délibération ouverts et fermés ». De même, la participation est largement insuffisante dans le processus législatif de ce pays - en partie du fait que le gouvernement tarde à promulguer le projet de loi sur la participation publique (2019) conformément à son exigence constitutionnelle sur la participation publique. Comme en Éthiopie, ce sont les détenteurs de droits qui sont le plus souvent exclus de la participation, notamment les personnes handicapées, les enfants et les personnes âgées.

En Afrique du Sud, la notion d'accès aux processus législatifs devrait renforcer la participation, notamment avec la création de l'autorité indépendante de protection des données, l'Information Regulator of South Africa (IRSA). Malgré un financement insuffisant, l'IRSA tente actuellement de mettre en place un système de dépôt de plaintes en ligne afin de faciliter

les plaintes publiques (et de renforcer ainsi la redevabilité). Pourtant, comme le note l'auteur, en raison du faible niveau de pénétration de l'internet dans les zones rurales et le coût élevé des données, l'utilisation de l'internet comme mécanisme de participation est en réalité limitée.

Comme le soulignent ces rapports, c'est au niveau de la mise en œuvre des lois sur la protection de la vie privée, y compris leurs règlements, que leur efficacité en tant que facilitateur de droits deviendra évidente.

Bien que les lois du Togo sur la protection des données à caractère personnel, comme dans le contexte de l'identification biométrique, aient montré la volonté du gouvernement de créer un environnement législatif fort concernant l'utilisation des technologies numériques, le « la mise en œuvre de ce cadre juridique représente encore un défi considérable, surtout dans la pratique. » Ce champ d'action comprend, d'une part, le secteur privé qui élabore des politiques conformes à la législation sur la protection de la vie privée et, d'autre part, la force et l'indépendance de l'autorité de régulation des données qui, dans un pays comme l'Ouganda, est remise en question.

Le rapport de l'Afrique du Sud souligne qu'une telle autorité indépendante, tout en étant une condition nécessaire pour assurer la mise en œuvre d'une loi sur la protection de la vie privée, doit également être suffisamment financée et avoir la capacité de promulguer des règlements.

C'est aussi une question de volonté politique. Un aspect clé de la législation sur la protection de la vie privée est qu'elle a le potentiel de responsabiliser l'État, en ce qui concerne notamment des questions comme la surveillance, mais aussi parce que l'État joue un rôle important dans la collecte des données personnelles.

Dans la plupart des pays étudiés ici, les lois globales sur la protection de la vie privée et des données n'ont pas encore été suffisamment testées - certaines lois sont nouvelles (adoptées en 2019) ou à l'état de projet. Pour celles qui ont été adoptées il y a plusieurs années (comme en Afrique du Sud), les règlements correspondants sont sur le point d'être promulguer seulement maintenant.

Il n'est donc pas surprenant qu'un des rôles clés de la société civile identifiés dans les recommandations du rapport consiste à surveiller la mise en œuvre des lois sur la protection de la vie privée afin de demander des comptes aux gouvernements à différents niveaux. Au niveau local et national, une partie de cette surveillance consiste à documenter et à signaler les violations de la législation sur la vie privée et la protection des données. Il peut s'avérer nécessaire de recourir à des litiges stratégiques (voir, par exemple, l'Éthiopie) et, en Afrique du Sud, il convient d'étudier la possibilité d'engager des actions collectives. Aux niveaux régional et international, des coalitions de groupes de la société civile doivent être formées pour renforcer sa capacité de surveillance et elle doit être active dans des forums tels que l'examen périodique universel du Conseil des droits de l'homme au moment de l'examen des pays.

Cette recherche représente une référence importante pour ce futur plaidoyer.

# Ethiopia

**Dr. Kinfe Micheal Yilma**[1]
Addis Ababa University Law School

## Executive summary

This country report maps the state of privacy and data protection in Ethiopia. Informed by a human rights-based approach, it explores Ethiopia's current and developing legal and institutional framework on privacy and data protection. The report begins with an analysis of the constitutional framework for the protection of privacy and data protection in the country, including in the digital context. The current Ethiopian Constitution provides a sound legal basis for the protection of privacy in that the protection appears to cover privacy and data protection in the context of digital communications. The report then surveys the extent to which other subsidiary pieces of legislation in Ethiopia protect privacy and data protection. It shows that some Ethiopian laws, particularly the Civil Code, Criminal Code and the Access

1 The author gratefully thanks Ato Gemechu Merera from Ethio telecom and Ato Manaye Alemu from the Ethiopian Institution of the Ombudsman for kindly agreeing to be interviewed during the preparation of this report.

to Information Proclamation, touch upon aspects of privacy and data protection. The report further examines Ethiopia's international and regional commitments on privacy and data protection. While Ethiopia is state party to key international human rights treaties that guarantee the right to privacy, such as the International Covenant on Civil and Political Rights (ICCPR), it is yet to accede to any of the data protection instruments including the Africa Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention).

Ethiopia does not have a comprehensive data protection law. But this report closely examines the draft Personal Data Protection Proclamation unveiled by the government in April 2020. It considers salient features of the bill, including key definitions, data subject rights, conditions for lawful processing, relevant exemptions in the public interest, data breach notification requirements and the transfer of personal data across borders, as well as provisions governing the proposed national data protection authority, the data protection commissioner. The report finds that Ethiopia's draft Data Protection Proclamation conforms by and large to international best practices, including the Malabo Convention, the African Declaration on Internet Rights and Freedoms (AfDec) and the Declaration of Principles on Freedom of Expression and Access to Information in Africa. But Ethiopia's performance in ensuring respect for and protecting privacy and data protection is yet to be closely reviewed by international mechanisms, including by relevant treaty bodies and Human Rights Council's Universal Periodic Review (UPR). This report further considers the extent to which non-governmental organisations are involved in the area of privacy and data protection. Because privacy and data protection have, up until now, generally received little policy or societal attention in Ethiopia, such organisations are yet to flourish.

The report further considers the extent to which and whether Ethiopia's current and developing legal framework on privacy and data protection conforms to the five basic principles of a human rights-based approach. It finds that the legal regime is largely in line with the principles, except for the principle of participation. The lawmaking process on matters relating to privacy, including the writing of the draft Data Protection Proclamation, falls short of being inclusive of interested stakeholders, including rights holders. But Ethiopia's existing and emerging legal and institutional framework generally embraces the principles of accountability, non-discrimination and equality, empowerment and legality. The report concludes that the country's current privacy and data protection legal and institutional framework is deeply fragmented and falls short of adequately upholding the right to privacy and data protection. With a view to make the legal framework fit its purpose, the report offers a series of recommendations to the government, civil society groups and the private sector. One suggestion is the adoption of a comprehensive data protection framework based on input from all stakeholders and in line with international best practices.

## Methodology

The report primarily employs a doctrinal research method, i.e. desk research. That means it is based on a thorough examination of relevant policies, laws and regulations – and where relevant, the literature on privacy and data protection law. But it also draws further input from interviews with personnel in relevant institutions. Potential informants and interviewees for the report are mainly from government departments that have some role in the area of privacy and data protection.

## Country context

Ethiopia is a federal republic located in the horn of Africa, one of the world's oldest independent nations. It is a founding member of major international and regional organisations, including the United Nations (UN) and the Organisation of African Unity (OAU), now known as the AU, which has its headquarters in Ethiopia. The country is the second most populous nation in Africa (next to Nigeria), with an estimated population of 110 million. It has a largely agrarian society with an estimated 80% of the population engaged in the agriculture sector. Ethiopia has one of the fastest growing economies but it is one of the least developed countries, with an estimated per capita income of USD 800. Its economic development strategy evolved over the years from agricultural-led development to industrial-led development and now to innovation and technology-driven development.

Ethiopia is not one of the least-connected countries in the world. According to World Internet Stats data, the level of internet use and penetration in 2019 was around 18%.[2] This is remarkable in light of the fact that it was one of the few countries to introduce telecommunication services shortly after their invention in 1894. The internet was introduced a little late, in 1997, in some government institutions and international organisations headquartered in Ethiopia such the UN's Economic Commission for Africa. The delay in the proliferation of internet use and access is mainly due to the monopoly of the telecom sector which has been in place until recently. As of 2005, the nation's sole telecom provider was able to roll out only 4,000 km of fibre-optic backbone in Addis Ababa. Fifteen years later in September 2020, the county's total fibre-optic cable line has reached 22,000 km.[3]

2 https://www.internetworldstats.com/africa.htm#et

3 Bekele, K. (2020, 15 August). Communication authority to float bid by September. *The Reporter*. https://bit.ly/3lyhKRn

However, the nation is said to require about 50,000 km of fibre-optic cables in the coming five years.[4] With the recent decision of the government to liberate the telecom sector – two new operators will enter the market in 2021 – and partial privatisation of the incumbent, internet use and access are bound to grow.

The slow development of the internet has played a role in delaying the formation of internet policies including legislative measures surrounding the internet. Ethiopia adopted its first information and communications technology (ICT) policy in 2002, which has since been revised in 2009 and 2016. These policy iterations have gradually been translated into a range of laws. So far, a handful of internet laws have been adopted including those dealing with cybercrime, telecom fraud, e-transactions, disinformation and hate speech online, and many others are in the pipeline such as a data protection law. But some of these laws have raised concerns around the enjoyment of human rights. For instance, the cybercrime and disinformation laws have been criticised for posing threats to the rights to privacy and freedom of expression. The Ethiopian government is often accused of abusing such laws to stifle dissent and engage in invasive practices of data collection and surveillance. Mainly because of the country's poor human rights culture, recent internet lawmaking and implementation in Ethiopia tend to overlook the need to uphold human rights in the digital environment.

Because privacy and data protection have received little policy or societal attention, there are only a few institutions involved in this field. Ethiopia currently has no comprehensive data protection law or a national data protection authority. Other government entities with some role in the protection data privacy have not been actively working in the field of privacy and data protection. Non-governmental entities working in this field have also been

4 Ibid.

few and far between. It is only recently that civil society groups with some interest in digital rights, including digital privacy, have emerged. A good case in point is the recently launched Network for Digital Rights in Ethiopia (NDRE), which operates within the auspices of the Centre for the Advancement of Rights and Democracy in Ethiopia. With the current government's ambition of bringing about digital transformation, concern for human rights online, including privacy and data protection, is likely to grow. This may be the start of an era where internet law and policy making will have human rights values as guiding principles.

## Constitutional basis for the right to privacy and data protection

Ethiopia has recognised the right to privacy throughout its brief constitutional history. From its imperial constitutions of the 1931 and the 1955 to the 1987 Constitution of the Military regime, the right to privacy has been constitutionally guaranteed. But the current Constitution of Ethiopia, adopted in 1994, guarantees the right to privacy in a more comprehensive manner. Article 26 of the Ethiopian Constitution guarantees the right to privacy in two key respects. First, it guarantees the right not to be subjected to searches and seizures. This protects the privacy of one's home, person and property against unreasonable interference. Second, it guarantees the right to the inviolability of one's notes and correspondences. The term "correspondence" is enunciated to capture modern media of communication including postal letters, telecommunications and "electronic devices". The latter phrase presumably embraces common means of communication using the internet. Thus this prong of the right protects privacy of communications, including protection of personal data. But the right to privacy in the constitution is not to be interpreted in a vacuum. Human rights guaranteed under the constitution, including the right to privacy, must be interpreted

in line with principles of the Universal Declaration of Human Rights (UDHR) and the ICCPR which guarantee the right to privacy.[5] It is important to note that the right to privacy provision is yet to be interpreted by courts in Ethiopia.

The right to privacy is not, however, absolute. It may be restricted under "compelling circumstances".[6] And any restriction should meet the following two requirements. First, the restriction must be in accordance with a law – i.e. there must be a clear legal basis for the restriction. Second, the restriction must be necessary to achieve certain legitimate aims. Such legitimate aims are listed exhaustively: safeguarding national security or public peace, the prevention of crimes, protection of health, public morality or the rights and freedoms of others.[7] It is vital to note that the constitutional protection of the right to privacy in Ethiopia clearly imposes corresponding duties on public officials. These duties are both "negative" – i.e. a duty to respect – and "positive" – i.e. a duty to protect.[8] While this provision imposes specific duties on public officials vis-à-vis the right to privacy, the Ethiopian Constitution imposes general duties to "respect and enforce" human rights guaranteed under the constitution on "all federal and state legislative, executive and judicial organs at all levels."[9]

## Subsidiary laws on privacy and data protection

Norms and principles relating to the protection of privacy and data protection are scattered across numerous pieces of legislation. What follows outlines such pieces of legislation, along with key privacy principles.

5 Constitution of Ethiopia (1994), Proclamation No 1/1995, Article 13(2) cum Article 12 (UDHR) and Article 17 (ICCPR).

6 Ibid., Article 26(3).

7 Ibid.

8 Ibid.

9 Ibid., Article 13(1).

## *Freedom of information law*

The Freedom of the Mass Media and Access to Information Proclamation addresses two themes: mass media and access to information held by public bodies.[10] Part three of the proclamation, which deals with access to information held by "public bodies" (not private bodies exercising public functions), touches on typical issues of data protection. This law provides a series of exceptional grounds by which access to data, including personal data, held by public bodies may be restricted or denied. One such ground is protection of privacy of the data subject, including a person who has been dead for no more than 20 years.[11] But there are a number of exceptions where disclosure may still be permitted. These include

- Where the data subject has expressed consent for the disclosure of the data or has not "protested" the disclosure.
- When the data subject was informed earlier that his or/her data is part of a class of data subject to disclosure.
- When the public interest in disclosure outweighs the privacy interests of the data subject.
- When the data is already publicly available.
- When data relates to a legally incapable person and the disclosure of which is in his/her best interest.[12]
- When the data is an employment record.
- When the request for disclosure is made by the deceased's next of kin or someone with the written consent of the data subject.

10 Freedom of the Mass Media and Access to Information Proclamation No 590/2008. Note that this legislation is now being revised, and a free-standing Freedom of Information Bill is expected to be released for consultation soon.

11 Ibid., Article 16(1).

12 Ibid., Article 28.

Remarkably, Article 15 of the law envisages what may be termed a "superiority clause" by which restrictions to the disclosure of (personal) information held by public bodies imposed by other laws (e.g. data protection law) would not affect the right of access recognised under this law. It stipulates that restriction to access to (personal) information may be determined only under Article 15(1), not any other legislation. In a way, this means when the draft Data Protection Proclamation becomes a law – which covers both public and private sector processing of personal data – it would essentially apply only to aspects of public sector processing of personal data. But this superiority clause would also raise a question of interpretation. One theory of interpretation is that in case of ambiguity the latest law would gain the upper hand over an older one. This is concerning because much of the data collection in Ethiopia is undertaken by the government, and hence the clause means the protection of data privacy would be seriously curtailed.

### *Civil Code*

The Ethiopian Civil Code is one of the major subsidiary pieces of civil legislation that protects the right to privacy under what it refers to as "rights of personality". At a more general level, it provides that every physical person shall enjoy the rights of personality recognised under the Ethiopian Constitution.[13] In so doing, it makes reference to civil rights guaranteed under the Ethiopian Constitution, including the right to privacy. The code further provides specific personality rights, some of which have clear privacy undertones. The privacy safeguards guaranteed within the umbrella of rights of personality recognised under the code are as follows: the right to not have one's person searched, the inviolability of domicile, the inviolability of correspondence,

13 Civil Code of Ethiopia, Proclamation No 165/1960, Article 8(1).

and the right to one's image.[14] There are also rights with some privacy undertones such as the right to refuse medical examinations, the right against unlawful molestation, and the right to keep silent.[15] No reported cases are yet available on how these provisions have played out in court, except for two recent rulings given by the Federal Supreme Court Cassation Division that implicated the right to image provisions of the Civil Code.[16] Since decisions of the cassation division have the status of precedent, the cases in effect establish a new line of case law in the field of privacy.

### *Criminal Code*

The Ethiopian Criminal Code of 2004 is another important piece of legislation that deals with privacy at some length and in a more direct fashion. Indeed, it penalises privacy violations in almost the same order the constitution guarantees the right to privacy. Perhaps this is the case because the code was enacted after the constitution. There are generally three criminal acts made punishable under the code. First, it penalises unlawful interference or restraint on the free exercise of civil rights – the right to privacy included – guaranteed under the constitution or other laws.[17] This proviso, consequently, criminalises possible violations of the privacy of persons, such as unlawful searches and violations of personality recognised under "other laws" (such as the Ethiopian Civil Code). As we have noted above, the Civil Code provides a handful of personality rights with clear privacy undertones. The violation of those personality rights results not only in liability under civil law but under criminal law as well.

---

14 Ibid., Articles 11, 13, 27-30, 31..

15 Ibid., Articles 10, 20-22, 23.

16 Ethiopian Supreme Court Cassation Division, *Riyan Miftah v Elsewdi Kebels Plc* (2013), File No. 91710; *Dashin Bank v Dorina Avakiyan* (2018), File No. 156425.

17 Criminal Code of Ethiopia, Proclamation No 414/2004, Article 601.

Second, the Criminal Code outlaws the "violation of privacy of domicile or restricted areas".[18] Notable about this provision is that it also covers violations of the privacy of premises of entities as well. Read closely, this means that Ethiopian law recognises the privacy not just of individual persons but also that of legal persons. The third criminal act in connection with privacy rights is "violation of the privacy of correspondence" such as letters and electronic communications.[19] This offence is, nevertheless, punishable only upon complaint and accusation – i.e. only where victims lodge complaints to the authorities. The cybercrime law also has some bearing on (data) privacy. More particularly, the provisions that penalise hacking and cracking of computers, computer systems, and computer networks are basically meant to protect data privacy.[20]

### *Criminal Procedure Code*

The Criminal Procedure Code also has privacy-protective rules, albeit indirectly. For instance, it provides that no person or premises may be searched without a court warrant unless under exceptional circumstances.[21] The exception includes when there is a "reasonable suspicion" that the suspect possesses any articles serving as material evidence for the offence the individual is accused of or is suspected to have committed. Also notable is that the code is commendably detailed in setting out the circumstances under which warrants may be issued, and even specifies the time during which searches and seizures may be executed.[22] It provides that the warrant shall clearly specify the property to be searched.

18 Ibid., Article 604.

19 Ibid., Article 606.

20 Computer Crime Proclamation No 958 /2016, Articles 3-4.

21 Criminal Procedure Code of Ethiopia, Proclamation No 185/1961, Article 32. Note that this law is now being revised.

22 Ibid., Article 33.

### *Tax Administration Proclamation*

Ethiopian tax laws generally impose a duty of maintaining the confidentially of tax information, which might include personal data, collected from taxpayers. An example is the Tax Administration Proclamation, which requires tax officers to keep tax information confidential.[23] But it provides a number of exceptions where disclosure may be permitted, including when the data subject consents to the disclosure or for law enforcement purposes. Yet those to whom the data is disclosed are still bound to keep the data confidential as far as possible and return it to the relevant tax authority.

### *National ID Proclamation*

Ethiopia's National Identification (ID) Proclamation is another law that contains rules protective of privacy. This legislation mandates the collection of personal data, including sensitive personal data, for registration of vital events such as births, deaths and marriages as well as registration for and issuance of national ID cards[24] But disclosure of personal information is restricted to be made only under exceptional circumstances such as upon the consent of the data subject or court order.[25] Curiously enough, the law provides that where disclosure of personal information is likely to prejudice the public interest, no disclosure will be made even with the consent of the data subject concerned.[26] Overall, these rules appear to be privacy friendly and in compliance with data protection principles.

23 Federal Tax Administration Proclamation No 983/2016, Article 8.

24 Registration of Vital Events and National Identity Card Proclamation No 760/2012, Article 57(2).

25 Ibid., Article 64(3).

26 Ibid., Article 64(5).

### *Health laws*

Ethiopia does not have a specific legislation addressing the protection of health data. The only privacy-oriented legislation is the health care administration law, which imposes an obligation of "professional confidentiality". This law requires "health professionals" to keep "personal health information" confidential.[27] But this prohibition does not apply when disclosure is (a) permitted by the written consent of the data subject, (b) warranted by the risks to public health as determined by the appropriate government organ, (c) sectioned by court order, (d) permitted by law and (e) warranted for scientific research so long as the data is anonymised or pseudonymised.[28]

## Ethiopia's international and regional commitments on (data) privacy

Ethiopia is state party to a number of international treaties that recognise the right to privacy and personal data protection. One is the ICCPR which, under Article 17, guarantees the right to privacy. Ethiopia ratified the ICCPR in June 1993.[29] But it has yet to ratify the First Optional Protocol to the ICCPR, which mandates an individual complaints mechanism by which aggrieved individuals may lodge a complaint against states for failing to respect and protect the right to privacy. Ethiopia has also ratified post-ICCPR human treaties which replicated the right to privacy, particularly the Convention on the Rights of the Child[30] and the Convention on the Rights of Persons with Disabilities (DRC).[31] As the most

27 Food, Medicine and Health Care Administration and Control Regulation No 299/2013, Article 77. Cf Food, Medicine and Health Care Administration and Control, Proclamation No 661/2009, Article 37.

28 Ibid.

29 https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en#EndDec

30 https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&clang=_en

31 Convention on the Rights of Persons with Disabilities (2006), Articles 22-23. See also Convention on the Rights of Persons with Disabilities Ratification Proclamation No 676/2020.

recent human rights treaty, the Disability Rights Convention also embodies some data protection principles. For example, the convention requires state parties to ensure protection of "personal, health and rehabilitation information of persons with disabilities".[32] Details of this proviso are furthered in a separate provision.

While requiring state parties to collect reliable information for the purposes of formulating sound policies in the interest of disabled persons, the convention attaches a number of requirements that must be complied with in the course of collecting and maintaining such statistics.[33] It requires such processes to first comply with data privacy principles to ensure privacy and confidentiality of the data; and second comply with internationally accepted norms and principles. The first requirement latently assumes the existence of data privacy law in state parties – and if there is none already, such law to be adopted. It is interesting to note that the first general proviso is provided alongside the underlying privacy provision of the convention, which is verbatim to article 17 of the ICCPR. As highlighted above, the Ethiopian Constitution requires its bill of rights provisions to be interpreted in conformity with international human rights standards. However, it also provides that international treaties to which Ethiopia is a party form an integral part of the law of the land.[34]

Ethiopia is not party to any of the regional legal instruments on privacy and data protection. The only exception is the African Charter on the Rights and Welfare of the Child, which – unlike the Africa Charter on Human and Peoples' Rights (Banjul Charter) – expressly recognises the right to privacy.[35] The Banjul Charter, to

32 Ibid., Article 22(2).

33 Ibid., Article 31.

34 Ethiopian Constitution. (1994), Article 9(4).

35 African Charter on the Rights and Welfare of the Child (1990), Article 10. See also details about the status of ratification at https://cutt.ly/UfBJn4N

which Ethiopia is a state party, does not specifically guarantee the right to privacy, but arguably other rights of the charter, such as the right of dignity, protect inherent privacy interests.[36] Ethiopia has also yet to sign and ratify the Malabo Convention. Nor has it acceded to the Council of Europe's Data Protection Convention 108 (or 108+). With a Data Protection Bill recently released by the government for public consultation, Ethiopia might move to sign and ratify the Malabo Convention as well as Convention 108. This would be in line with the approach of the current administration to accelerate accession to international treaties and institutions such as the African Continental Free Trade Area. If the Data Protection Bill is adopted and a Data Protection Commission instituted, Ethiopia might begin to play some role in the field of privacy and data protection in the African region. Ethiopia is not a member of the sub-regional economic community, East African Economic Communities (EAC) and hence not party to its human rights commitments.[37] But unlike other regional economic communities, EAC is also lagging behind in launching a sub-regional data protection instrument. Its early attempts at introducing a "Bill of Rights for the East African Community" is still to become a reality.[38]

## The development of data protection law in Ethiopia

### *General*

Ethiopia never had a comprehensive or sectoral data protection law. But there have been disjointed efforts to introduce data protection legislation since at least 2007. The first ever data

36 African Charter on Human and Peoples' Rights (1981), Article 5. See also Yilma, K., & Birhanu, A. (2012). Safeguards of the Right to Privacy in Ethiopia: A Critique of Laws and Practices. *Journal of Ethiopian Law*, *26*, 109-110.

37 Treaty for the Establishment of the East African Community (1999, as amended), Articles 6(d), 7(2) cum Article 27(2).

38 The East African. (2010, 11 July). Common Bill of Rights next for all EAC nations. *The East African*. https://cutt.ly/AfBJz0m;an earlier version of the bill is available at https://cutt.ly/NfBJvUl

protection bill was commissioned by the Ethiopian government in 2009.[39] Drafted by an Indian-based consultancy firm, the draft was released alongside other cyber legislation governing electronic transactions and cybercrime. This bill was, however, never presented before parliament for enactment. After a decade or so of hiatus, the Ministry of Innovation and Technology released a new and much improved draft Data Protection Proclamation in April 2020.[40] By and large, this bill reflects norms, principles and rights provided in international and regional data protection instruments.[41]

The need for appropriate legal framework governing data protection has been recognised in successive national policy documents. The revised ICT Policy of 2009 addressed the need for a data protection legal framework in a more elaborate fashion. One of the strategic focuses of the policy was "ICT Legal Systems and Security", which called for legislation governing data protection and security to "facilitate Ethiopia's unhindered and effective participation in the global information society."[42] This was reiterated when the national ICT Policy was revised in 2016.[43] The more recent iteration in Ethiopia's ICT policy making is the Digital Transformation Strategy of 2020. But this omnibus and ambitious document does not specifically address the issue of privacy and data protection.[44] Ethiopia's National Information Security Policy also emphasises the need to put in place "data protection and procedures" to ensure the security of personal data.[45]

39 Draft Data Protection Act, Version 1.1 (2009).

40 Draft Data Protection Proclamation (2020).

41 For more on key features of this bill, see the next section.

42 Ministry of Communication and Information Technology. (2009). *National Information and Communication Technology Policy and Strategy of Ethiopia*, 11.

43 Ministry of Communication and Information Technology. (2016). *Digital Development Strategy: ICT Policy of Ethiopia*, 25-26.

44 Ministry of Innovation and Technology. (2020). *Digital Ethiopia 2025: A Digital Strategy for Inclusive Prosperity*.

45 Information Network Security Agency. (2011). *National Information Security Policy,* 8.

A recurring issue of data protection in Ethiopia has been the allegedly unbridled and covert surveillance practices of government agencies. For many years, the Ethiopian government has been accused by human rights organisations and activists of engaging in surveillance practices as well as mass collection of personal data.[46] Another prominent issue of data protection revolved around national ID cards. What personal data should appear in ID cards, which are currently issued by local administrative units in cities, has been controversial. After Ethiopia introduced a federal system of government in 1991, ethnic and linguistic identities became prominent. This meant that ID cards would bear the ethnic identity of individuals based on the ethnic identity of their father. This has been compulsory until recently, at least in Addis Ababa. With recent changes in government, the practice of printing a person's ethnic identity on ID cards ended. But more recently, the practice took a turn and ID cards issued (at least in Addis Ababa) would bear individuals' "blood type" instead of ethnicity. Whether this change has any legal basis is not clear but it seemed that the widespread disapproval for the practice of mentioning ethnicity on ID cards led to the changes. As such, protection of privacy was not the main driving factor. This is partly because the new practice of printing blood types raises as many issues of privacy as blood type is a sensitive personal data. Under the access to information law, which provides the most comprehensive definition of "personal information" under Ethiopian law, "blood type" is categorised as personal information.[47] Thus, the question of what data ID cards should carry remains an issue of privacy and data protection in Ethiopia.

46 Human Rights Watch. (2014). *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia*. https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia; Marczak, B., et al. (2014, 12 February). Hacking Team and the Targeting of Ethiopian Journalists. *The Citizen Lab*. https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists; for more discussion on Ethiopia's surveillance practices, see: Yilma, K. (2015). Data Privacy Law and Practice in Ethiopia. *International Data Privacy Law, 5*(3), 183-184.

47 Proclamation No 590/2008, Article 2(8).

Indeed, the law governing national ID cards does not mandate such a practice.[48] Per this law, physical ID cards should not mention ethnic identities but in the electronic database the ethnic identity of individuals must be indicated.[49] Still, the envisioned national ID card database is bound to carry personal data, including sensitive data such as date of birth, sex, religion, fingerprints and signature.[50] And this makes a robust data protection framework an imperative. Ethiopia's "Ministry of Peace" has reportedly started the process towards introducing a "National Digital ID Strategy".[51] Of course, one of its statuary functions is to "lead and follow up national ID card registration and issuance."[52]

### *Salient features of Ethiopia's draft Data Protection Law*

#### Key definitions

The draft Data Protection Proclamation provides definitions of key terms that recur throughout the law in line with international best practices. One key definition concerns "personal data" which is defined broadly and includes "any information relating to an identified or identifiable natural person who can be identified from these data or from those data and other information that is in the possession of or likely to come into the possession of the data controller".[53] Going further, the bill provides that personal data includes "any expression of opinion about the individual and

48 National ID cards are yet to be implemented and ID cards are currently issued by local administrative units.

49 Proclamation No 760/2012, Articles 57-58.

50 Ibid.

51 Ministry of Innovation and Technology. (2020). Op. cit.

52 Definition of Powers and Duties of the Executive Organs of Ethiopia, Proclamation No 1097/2018, Article 14(1(k)). The National Intelligence and Security Service, which has recently become a department with the ministry, is tasked by its establishment legislation to oversee the issuance of national ID. National Intelligence and Security Service Re-establishment Proclamation 804/2013, Article 9(11). Note that this is a continuation of plans to launch a national ID both in the Growth and Transformation Plan I (2010-2015) and II (2016-2020).

53 Draft Data Protection Proclamation (April 2020), Article 2(19).

any indication of the intentions of the data controller or any other person in respect of the individual". Related to this definition is the term "sensitive personal data", which is defined in the form of an illustrative list.[54] This includes data about a person's racial or ethnic origins, genetic or biometric data, physical or mental health or condition, sexual life, political opinions, trade union membership, religious or other beliefs and criminal history and legal proceedings. But this list is not exhaustive, and as such, the commission is empowered to extend the list of sensitive personal data where necessary.[55] Another key definition concerns "consent" which is defined in the bill as "any freely given specific, informed and unambiguous indication of the wishes of a data subject" and such indication may be given either by a "statement or clear affirmation" by which she or he signifies agreement to personal data relating to them being processed.

## Data subject rights

The Data Protection Bill enshrines a broad range of data subject rights that are widely accepted in contemporary international and regional data protection instruments. These are:

- *Right to be informed* (Art 35): The right to be informed about the identity of the data controller, scope, nature, purpose and legal basis of the processing unless the processing is mandated by law or providing information would require disproportionate efforts.
- *Right of access* (Arts 36-37): The right to access free of charge and swiftly the data being processed unless such access would invade or harm the right to privacy or the

54 Ibid, Article 2(28).

55 Ibid, Article 2(28(j)) cum Article 19.

health or safety of others, or the data is privileged by law or is merely evaluative material, or the request for access is repetitive, frivolous or vexatious.

- *Right to rectification* (Art 38): The right to request correction of inaccurate, incomplete, misleading, outdated personal data held by a data controller or third parties with whom it was shared a year before the request.

- *Right of erasure of processing* (Art 39): The right to request erasure of processing of personal data that is no longer necessary for the purpose for which it was collected, or lacked any legal basis or the data subject has objected to the processing unless the data is necessary for reasons of public health, human rights-compliant historical, statistical or scientific research or for advancing legitimate interests of the data controller or the data subject.

- *Right to request restriction of data processing* (Art 40): The right to seek a temporary halt to the processing of personal data until the claims or objections of the data subject regarding the processing are verified.

- *Right to object to processing* (Art 41): The right to object to processing of personal data, including for purposes of direct marketing, unless the grounds for processing outweigh the rights and freedoms of the data subject.

- *Right not to be subjected to automated processing of personal data* (Art 42): The right not to be profiled which may have significant legal effects on the data subject, unless the automated processing is sanctioned by law or the data subject's explicit consent or is needed to conclude a contract between the data controller and the data subject.

- *Right to data portability* (Art 43): The right to receive one's personal data from data controllers in a machine-readable, structured and commonly used format, including to move the data to another controller or processor unless the transfer would affect the rights of others or undermine public interest.

## Conditions for lawful processing

Ethiopia's draft Data Protection Proclamation envisages two layers of conditions for lawful processing of personal data. First, it lays out general conditions of lawful processing. For any processing to be lawful, it should be based on the consent of the data subject that is "free, informed, specific, clear, capable of being withdrawn" and given before the start of the processing.[56] Other grounds of lawful processing are when the processing (a) is necessary to fulfil contractual obligations to which data subject and controller are involved, or (b) is necessary to uphold vital interests of the data subject or legitimate interests of the data controller that are not overridden by fundamental rights of data subjects, or (c) is necessary for achieving public interests goals such as public order.[57]

Second, the bill prescribes specific conditions for processing sensitive personal data as well as data of children. For processing of sensitive personal data (other than data in respect of racial or ethnic origin) and personal data of children to be lawful, it should be (a) based on written, specific consent of the data subject; if the data subject is a child, consent should be given by his or her parent or legal guardian, (b) in accordance with a law adopted after the coming into force of the data protection law, (c) necessary to protect the life and safety of

56 Ibid., Article 16(2(a)) cum Article 17.

57 Ibid., Article 16(2(b-f)).

the data subject who is not capable of expressing consent or of another person, (d) necessary to protect the lawful and non-commercial interests of a public entity, (e) necessary for medical treatment, (f) necessary to protect the lawful rights and interests of natural or legal persons in legal proceedings, (g) necessary to protect processing by religious institutions of data in respect of religious beliefs, or (h) necessary to protect his or her vital interests if the data subject is a child.[58]

In addition to the above highlighted conditions for lawful processing, the Data Protection Bill provides an overlay of requirements to make processing of personal data lawful. These include prior registration of data controllers and processors,[59] the appointment of a data protection officer,[60] setting of technical and organisation security measures,[61] data protection impact assessment,[62] prior authorisation[63] and data protection by design.[64] While each requirement may apply in specific circumstances, failure to meet the attendant conditions would make the processing unlawful.

### Relevant exemptions in public interest

Ethiopia's draft Data Protection Proclamation provides exemption to a certain category of data processing. Essentially, all of the exemptions concern the processing of personal data undertaken in the public interest. The exemptions are the following: (a) processing for purposes of national security,

58 Ibid., Article 18(2-4) cum Articles 18(5), 20.

59 Ibid., Article 45 *et seq*.

60 Ibid., Article 52.

61 Ibid., Article 53.

62 Ibid., Article 58.

63 Ibid., Article 59.

64 Ibid., Article 60.

defence or public security, including when exemption is granted or certified by the prime minister for those purposes,[65] (b) processing for purposes of preventing, investigating and prosecuting crimes as well as execution of penalty,[66] (c) processing for purposes of safeguarding general public interest, including economic interests of the state,[67] (d) processing of upholding judicial independence and judicial proceedings,[68] (e) processing for purposes of protecting data subjects or the rights and freedoms of others,[69] and (f) processing for purposes of historical, statistical or scientific research.[70]

There are three vital points to note regarding these exemptions. First is that the final exemption is permissible only when data controllers have put in place the required technical and organisational measures to protect the rights of data subjects.[71] Second, while the bill appears to provide an exhaustive list of exemptions, it also empowers the Data Protection Commission which may – by a directive, a subsidiary legislation in a hierarchy of laws in Ethiopia – broaden the scope of exemptions when or if the interests of data subjects or the rights and freedoms of others warrant it.[72] Third, the bill omits widely accepted exemptions in data protection law: processing of personal data for purposes of journalistic or artistic purposes.[73] But, the commission – relying on its power of adding new exemptions noted above – may include such exemptions in due course.

---

65 Ibid., Article 63(1(a)) cum Article 63(4-5).

66 Ibid., Article 63(1(b)).

67 Ibid., Article 63(1(c)).

68 Ibid., Article 63(1(d)).

69 Ibid., Article 63(1(e)).

70 Ibid., Article 63(2).

71 Ibid.

72 Ibid., Article 64.

73 For example, General Data Protection Regulation 2016/679 of the European Union (2016) Article 85 cum Recital 153.

## Data breach notification requirements

The draft Data Protection Proclamation provides two layers of notification requirements when a data breach occurs: i.e. notification for the Data Protection Commission and the data subject. But the bill adopts less stringent requirements of breach notification to data subjects. Notification of the commission is required when the breach is likely to pose a "risk" to the rights and freedoms of an "individual".[74] This proviso suggests that notification is required when the risk is not just to the rights and freedoms of affected data subjects but "any individual". Unless the use of the term "individual" is a drafting misstep, this would be slightly cumbersome and create unrealistic requirements for data controllers. Notification to potentially affected data subjects is required when the breach is likely to pose a "high risk" to the rights and freedoms of data subjects.[75] So, if the risk is not "high" enough, the data subject would not be entitled to notification, although the question of how "high" high is remains. However, there are still circumstances where "high risk" breaches may not warrant notification to data subjects.[76] One is when the data controller suffering the breach has put in place appropriate technical and organisational measures such as encryption that would render personal data unintelligible; second, when the data controller has taken subsequent measures that mitigated the risk; or third, if notifying data subjects would demand disproportionate efforts and if public notice of the breach has already been announced. But the commission is at liberty to notify the data subject when it deems it necessary.[77]

74 Draft Data Protection Proclamation (April 2020), Article 54(1).

75 Ibid., Article 55 (1).

76 Ibid., Article 55(3).

77 Ibid., Article 55(4).

In principle, breach notification should be provided to the commission and data subjects without "undue delay".[78] Notices should be given in 72 hours only when "feasible".[79] Hence, the bill gives some latitude to data controllers as to when to issue the notices. But when the notification is not provided to the commission within 72 hours, the data controller should furnish reasons for the delay.[80] This requirement does not apply for breach notification to data subjects. It is not entirely clear, however, as to what would happen if the data controller does not provide reasons or the commission is not persuaded by the reasons provided.

When providing breach notifications to both the commission and data subjects, data controllers are required to include some information such as the nature and scope of personal data breached, contact details of the data protection officer or other focal person, possible consequences of the breach and measures taken or proposed to mitigate the adverse effects of the incident.[81]

## Cross-border data transfers

Transborder transfer of personal data from Ethiopia is permitted only when there is an "appropriate level of (data) protection" in the "third-party jurisdiction".[82] The "appropriate level of protection" threshold is slightly different from the standard adopted elsewhere, for example "adequate" level of protection in the European Union (EU).[83] "Third-party

78 Ibid., Articles 54 (1), 55(1).

79 Ibid.

80 Ibid., Article 54(2).

81 Ibid., Articles 54(4) cum Article 55(2).

82 Ibid., Articles 28, 29(5).

83 General Data Protection Regulation 2016/679 (2016), Article 45.

jurisdiction" is defined broadly to include "a country other than Ethiopia, an international organisation or its subordinate bodies governed by public international law or anybody" created by an international agreement.[84] Whether a third-party jurisdiction has "appropriate level of protection" is to be determined by the commission taking into account two layers of considerations: general and particular.[85] The general consideration concerns all circumstances surrounding a specific or set of data transfer operations.[86] Particular considerations involve the nature of the data, purpose and duration of the proposed transfer and the state of rule of law in the third-party jurisdiction.[87] It is interesting to note that the commission may prohibit, suspend or set forth conditions for transfer to third-party jurisdictions found to have appropriate levels of protection to protect the rights and freedoms of the data subject.[88]

The Data Protection Bill envisages circumstances where personal data may be transferred to a third-party jurisdiction that does not, per the commission's assessment, provide appropriate levels of data protection. These are: (a) when the data subject gives explicit consent to the proposed transfer after having being informed of the lack of appropriate protection in the third-party jurisdiction, (b) when the transfer is necessary to achieve certain legitimate aims of the data subject or data controller or both, as well as for matters of public interest, and (c) when the transfer is from a public register.[89]

84 Draft Data Protection Proclamation (April 2020), Article 2(29).

85 Ibid., Article 29(3).

86 Ibid., Article 29(1).

87 Ibid., Article 29(2).

88 Ibid., Article 31(2).

89 Ibid., Article 30.

The bill also envisages "limited transfer" of personal data to a third-party jurisdiction with no appropriate level of protection when the data subject consents to the transfer and parts of the data are severed or reduced.[90] But such transfer requires the authorisation of the commission and probably concerns circumstances where the data subject is not informed in advance about the lack of appropriate level of protection at the destination.

## Privacy and data protection institutional framework

### *Data Protection Commission*

As highlighted above, Ethiopia's draft Data Protection Proclamation envisages the creation of a national data protection authority: the Ethiopian Data Protection Commission. The commission is envisaged as an independent entity answerable to the House of Peoples' Representatives, the lower chamber of parliament.[91] It is also the House that appoints the commissioner and deputy commissioners of the Data Protection Commission. The bill places emphasis on the institutional independence of the commission, including by obliging the commissioners to "act with complete independence and impartiality and not seek or accept instructions."[92]

The Data Protection Commission is tasked to undertake a broad range of regulatory functions. But the following are key aspects of its mandate:

- To oversee the implementation of data protection law, including by keeping a register of data controllers and

90 Ibid., Article 29(4).

91 Ibid., Article 5.

92 Ibid., Article 13(1).

processors, undertaking audits of practices and policies of data controllers and processors, investigating complaints, and conducting search and seizure.[93]

- To issue enforcement notice against data controllers found to have violated their duties under the law.[94]
- To issue an injunction to preserve data vulnerable to loss or alteration.[95]
- To make determination whether a third party jurisdiction has an appropriate level of protection in the context of cross-border data transfer.[96]
- To approve or deny cross-border transfer of sensitive personal data.[97]
- To order local processing or storage of "critical personal data" based on strategic interests of the state.[98]
- To raise public awareness regarding data subject rights and obligations of data controllers and processors.[99]

But it is vital to note that the Data Protection Bill envisions the possibility that the commission may be entrusted with the powers of overseeing other laws.[100] One possibility for an such additional role is when future sector or domain specific data protection legislation is enacted, be it on health, communication or health data processing.

93 Ibid., Articles 6, 45-51, 67-68.

94 Ibid., Articles 6, 65.

95 Ibid., Article 6.

96 Ibid., Articles 29, 31.

97 Ibid., Article 32(2).

98 Ibid., Article 32(1).

99 Ibid., Article 6.

100 Ibid., Article 6(18).

### *Other regulatory entities*

As rules of data protection in Ethiopia are scattered across various pieces of legislation, a number of institutions currently have statutory responsibilities of overseeing these rules. The following are key among those institutions. One is the Ethiopian institution of the ombudsman. The ombudsman is an independent body tasked primarily to address problems of maladministration and enhance good governance in public institutions.[101] However, this role is largely recommendatory and hence wields no power to issue binding decisions against non-complying public bodies. It is the access to information legislation that vests in the ombudsman the power to make binding decisions. A person aggrieved by the decision of a public relations officer in a public body (either to allow or deny disclosure of [personal] information) may appeal, first, to the head of the public body and second, to the institution of the ombudsman and finally to court.[102] That means the ombudsman may order a public body not to disclose personal data held by public bodies to third parties. Moreover, the ombudsman is charged with preparing a "Code of Custody, Management and Disposal of Records",[103] which was adopted by the ombudsman in mid-2020. In an interview with the head of the Ombudsman's Access to Information Law Implementation Directorate, it was revealed that the institution is yet to properly carry out its statutory functions relating to data privacy.[104] Mr. Manaye noted that because public bodies do not generally comply with the access to information requests, appeals alleging privacy interference due to disclosure of information have never been

101 Ethiopian Institution of the Ombudsman Establishment Proclamation No 211/2000, Articles 5-6 .

102 Freedom of the Mass Media and Access to Information Proclamation No 590/2008, Articles 31-32, 34.

103 Ibid., Article 38.

104 Interview with Mr Manaye Alemu, director of the Access to Information Law Implementation Directorate of the Ethiopian Institution of the Ombudsman, 9 October 2020.

presented to the ombudsman. In other words, complaints of privacy violation arise when public bodies disclose information, but they generally do not.

Other government institutions have some role in the protection of privacy and data protection. The Communications Service Proclamation, for instance, tasks the Ethiopian Communications Authority (ECA) with promoting "data privacy and protection" in the telecom sector.[105] As a telecom sector regulator, ECA has recently issued a draft consumer protection directive which embodies some protection of data privacy.[106] The Information Network Security Agency (INSA) would also be involved in data protection as its nation's prime cyber command and root certificate authority.[107] The Financial Intelligence Center (FIC), a body mandated to regulate money laundering and the financing of terrorism, also has some role. In particular, the FIC is required by law to put in place "information management systems" to ensure the protection of sensitive and confidential financial information.[108] The Ministry of Innovation and Technology is also entrusted by law to initiate policy and law in the field of information technology.[109] As highlighted above, the recently introduced Data Protection Bill was drafted under the aegis of the ministry. After the draft is enacted, the ministry is likely to play a key role in the implementation of the data protection law. The Ministry of Peace will also have the sole role of overseeing data protection while administrating the upcoming national ID.

105 Communication Services Proclamation No 1148/2019, Article 6(25). Note this statutory function of ECA is reinforced by the newly adopted e-transaction legislation, although the law appears to obfuscate the distinction between a registry and a registrar in domain name administration. See Electronic Transaction Proclamation No 1205/2020, Articles 38-40 cum Article 5(3).

106 Consumer Rights and Protection Directive (Draft, 2020), Articles 15-16.

107 Information Network Security Agency Re-establishment Proclamation No 808/2013, Article 6.

108 Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation No 780/2013, Article 13(5) cum Article 23.

109 Proclamation No 1097/2018, Article 10 cum Article 20.

## *Data privacy and non-governmental entities*

There are no local organisations or associations that are actively involved in the field of privacy and data protection in Ethiopia. For so long, this area has generally been overlooked by academics, civil society organisations and human rights advocacy groups in the country. In the recent past, there were a few organisations with a potential to engage in the field but they seem to have become defunct. One example is the Ethiopian Free and Open Source Software Network (EFOSSNET), launched in 2005, but this network appears to have been disbanded for a while now.[110] Another potentially relevant entity is the Ethiopian Information and Communication Technology Association (ICT-ET), established in 2010, which is still active.[111] While it is yet to engage in the field of privacy and data protection, it has recently began to call on its members to comment on the draft internet laws tabled for public consultation such as the draft E-transaction Regulation.[112] But no such call has been made so far on the draft Data Protection Proclamation. In part, this may be because the Data Protection Bill has not officially been released for wider public consultation.

However, recent years have seen the rise of some interest in "digital rights" and a group of activists have founded the NDRE.[113] But the extent to which this network has been involved in advocating for the protection of the right to privacy and data protection in Ethiopia is unknown. This is partly because the network was established only recently. In contrast, international organisations such the Internet Society (ISOC) have advocated

110 The network's website www.efossnet.org is offline but preliminary information about EFOSSNET is available at https://bit.ly/3jjEcw9

111 https://ictet.org/about

112 https://ictet.org/2020/10/05/request-for-comment-on-electronic-transaction-regulation

113 https://ndrethiopia.org/2019/09/23/about-us

in the area of privacy and data protection in some occasions. More recently, the African Bureau of ISOC has offered extensive comments and suggestion on, *inter alia*, the draft Data Protection Proclamation and the draft Consumer Rights and Protection Directive.[114] The latter governs consumer rights in the telecom sector, and as such, stipulates some sector-specific data protection norms and principles. In March 2020, the Ethiopian Chapter of ISOC was launched.[115] Once the chapter becomes fully operational, it will certainly have some role in advancing privacy and data protection rights in Ethiopia.

## Data privacy and ccTLD

The newly established ECA is responsible for the management of the nation's country code top level domain (ccTLD), .et.[116] But the law allows ECA to delegate or contract out the task of managing the ccTLD to third parties subject to general supervision of the authority.[117] Before the creation of ECA, a regulatory department within the Ministry of Innovation and Technology was mandated by law to manage the domain name.[118] But the law had mandated a form of multi-stakeholder governance framework by which the ministry would coordinate "pertinent stakeholders" for the creation and proper utilisation of the ccTLD system.[119] Within this framework, the ministry would oversee the implementation of the rules and procedures set out through multistakeholder governance processes.

114 For example, Bekele, D. (2018, 12 October). Internet Society Submits Comments for the Revision of the Ethiopian Cybercrime Law. *Internet Society*. https://www.internetsociety.org/blog/2018/10/internet-society-submits-comments-for-the-revision-the-ethiopian-cybercrime-law

115 Necho, A. (2020, 2 March). Internet Society Ethiopia Chapter Launched Today! *Internet Society*. https://www.internetsociety.org/blog/2020/03/internet-society-ethiopia-chapter-launched-today

116 Proclamation No 1148/2019, Article 6(12) cum Article 27(2).

117 Ibid., Article 27(9).

118 Proclamation No 1097/2018, Article 20(1(o)).

119 Ibid.

In practice, Ethio telecom – the nation's sole telecom provider thus far – is currently the de facto registry of the .et domain name. Ethio telecom's terms and conditions govern the sharing of personal data collected during domain name registration. Terms and conditions provide that such data may be shared with "legally mandated authorities" or be used for "any other related purposes", including for marketing or research by Ethio telecom itself.[120] This suggests that granting access to WHOIS data for law enforcement purposes, for instance, is permissible without any safeguards. There is also no publicly known procedure by which requests are entertained by Ethio telecom. In an interview with a legal officer at Ethio telecom's Criminal Follow-up and Support Unit, it emerged that Ethio telecom entertains law enforcement requests for user personal data – including WHOIS data – through what it is called "information provisioning directive".[121] Gemechu Merera noted that legal officers would review requests in light of the right to privacy provision of the constitution. But he noted that no such request has, to his knowledge, been made regarding WHOIS data as requests often concern the identity or addresses of individuals holding certain phone numbers and the content of their text messages. But it is vital to note that most registrants of the .et domain are government institutions, be it ministries, public enterprises or public universities. This means that a search in the WHOIS does not as such reveal personal data. But in some cases, it does reveal personal data of registrants when public bodies use personal data or details for domain registration. A search on WHOIS database, for example, of the ECA's domain (eca.et) reveals the personal email address, name and personal telephone number of ECA's director general.[122]

120 https://www.ethiotelecom.et/domain-name-webhosting-email-services

121 Interview with Mr. Gemechu Merera, Legal Officer at Ethio telecom's Criminal Follow-up and Justice Unit, 9 October 2020.

122 http://whois.ethiotelecom.et

## Comparing Ethiopia's data privacy framework with regional standards

This section compares Ethiopia's legal framework on privacy and data protection with regional standards in Africa, namely, AfDec, the Malabo Convention and the Declaration of Principles on Freedom of Expression and Access to Information in Africa (Declaration of Principles). But the discussion does not consider the Personal Data Protection Guidelines for Africa. This is because the guidelines are not structurally and substantively normative, and as such, provide sheer elaboration on the provisions of the Malabo Convention. Moreover, the guidelines are not adopted by the AU but by a not-for-profit organisation, i.e. Internet Society. As a result, it is not suitable to use them as a benchmark to assess Ethiopia's legal framework. As highlighted above, Ethiopia does not currently have a comprehensive and fully-fledged data protection law. But its recently released draft data protection legislation is clearly influenced by other regional data protection instruments such as the EU's General Data Protection Regulation and the Council of Europe's Data Protection Convention 108 (or 108+). This section focuses on African instruments.

### *In light of Principle 8 of AfDec*

The scope of "privacy and personal data protection" under Principle 8 of AfDec has three layers. First, it guarantees the right to privacy online to "everyone", and this right shall include the right to protection of personal data. As discussed above, the Ethiopian Constitution guarantees the right to privacy for "everyone" regardless of nationality.[123] Moreover, the right to privacy is framed in a manner that applies in the digital context.

123 Ethiopian Constitution (1994), Article 26(1).

For instance, it specifically stipulates that the right includes "the right to the inviolability of [...] correspondence including [...] communications made by means of telecommunications and electronic devices."[124] This phrasing clearly suggests that the right to privacy online is guaranteed under the Ethiopian Constitution. Moreover, references in Article 26 that the right to privacy includes the right not to be subjected to searches and seizures arguably protect privacy in the digital context, such as the search and seizure of one's digital accounts, records and activities. Furthermore, the way in which this provision is framed suggests that the right to privacy includes the protection of personal data. And of course, without meaningful constitutional protection of unlawful or arbitrary collection, processing, profiling, retention and disclosure of personal data, the right to privacy would mean little in the data-driven digital age. At the core of digital privacy is the protection of personal data. Therefore, the right to privacy under the Ethiopian Constitution applies in the digital context, and embodies a sub-right to personal data protection.

Second, Principle 8 of AfDec enshrines that the right to privacy includes the right to communicate anonymously including through the use of privacy-enhancing technologies. This principle essentially reflects the "right to use encryption", a right increasingly emerging as a distinct digital right in internet bill of rights instruments. Such a right is not explicitly recognised under Ethiopian law. Because the right to privacy provision of the constitution has not been tested in courts, it is unclear whether the right to privacy embodies the right to use encryption or not. However, this right is implicit in the right to privacy. Securing the right to privacy in the digital age – where surveillance and data collection are ubiquitous – would be hard without the use of privacy-enhancing technologies such as

124 Ibid., Article 26(2).

encryption and anonymity tools. As such the right to privacy under Article 26 of the constitution arguably embodies a sub-right to use privacy-enhancing technologies. This is plausible because this sub-right would be merely a “negative right” which requires states to respect the right to privacy, particularly a duty to refrain from any act that would restrict the “use” of privacy-enhancing technologies.

The right to use privacy-enhancing technologies is also being recognised in international law. In the wake of the Snowden revelations, the UN General Assembly has adopted a series of resolutions on the “Right to Privacy in the Digital Age”. These resolutions appear to grant the right to use encryption and anonymous technologies in the right to privacy in international human rights law, particularly Article 17 of the ICCPR.[125] While resolutions of this type are merely soft international law with no legally binding force, they arguably constitute authoritative interpretation of the ICCPR, to which Ethiopia is a state party. Resolutions bear legal effect and may be referred to by courts when interpreting the scope of the right to privacy. As such, it might be held that the right to privacy under Ethiopian law includes the right to communicate anonymously using privacy-enhancing technologies. But it is vital to note that the use of privacy-enhancing and digital security technologies has been prosecuted by Ethiopian authorities in the recent past.[126] Such measures were potentially unlawful and interfered with the right to privacy.

Third, Principle 8 outlines the conditions that must be met for restricting the right to privacy on the internet: legality, legitimate aim and necessity or proportionality. The Ethiopian Constitution

125 For example, The Right to Privacy in the Digital Age, GA Res 73/179, 17 December 2018.

126 Human Rights Watch. (2015, 13 April). Ethiopia: Free Zone 9 Bloggers, Journalists. https://bit.ly/2HIteTJ

enshrines similar requirements for permissible restrictions of the right to privacy, including in the online context.[127] First, any restriction must be in accordance with specific laws. Second, the restriction must be sought to achieve one of the legitimate aims: safeguarding national security or public peace, prevention of crimes, protection of health, public morality or the rights and freedoms of others. Third, the restriction must be proportionate and necessary to achieve one or more of those legitimate aims.

Overall, Ethiopian law is consistent with Principle 8 of AfDec. But because Ethiopia's privacy and data protection jurisprudence is thin, the exact normative contours of the right to privacy in the digital context are not entirely clear. The scope of the right to privacy, and whether it protects personal data and the right to communicate anonymously online, is yet to be fleshed out by courts. As concerns for digital privacy grow with increasing digitalisation and internet access in Ethiopia, the boundaries of the right to privacy in the digital age will hopefully be clearer.

### *In light of the Malabo Convention*

Ethiopia has yet to sign and ratify the Malabo Convention, the only pan-African data protection treaty. The convention is by and large a framework treaty and hence relegates a number of regulatory details of personal data protection to state parties. But there are some variations between Ethiopia's Draft Data Protection Proclamation – which is more detailed – and the convention. As a founding member of the AU, it is befitting to accede to the convention and hence to put the bill in line with the convention. The major variations are the following:

127 Ethiopian Constitution (1994), Article 26(3).

- The convention adopts a relatively broad scope of "sensitive personal data" in that it includes two types of sensitive personal data not included in the bill. These are "parental affiliation" and "social measures".[128]
- The convention adopts a relatively broad scope of exemptions in that it includes a set of exemptions not included in the bill. These are: processing for household or domestic processing of personal data,[129] and processing of personal data as part of temporary storage and transmission of date over an intermediary network.[130]
- The convention prohibits, in principle, processing of personal data for research, artistic, literary or journalistic expression unless the processing is first solely for those purposes or second in line with the applicable professional conduct.[131] Such exemptions are generally granted to support the enjoyment of free expression. But Ethiopia's bill neither exempts – like other jurisdictions – nor prohibits processing for those purposes. The conventional juristic wisdom in Ethiopia is that what is not prohibited is permitted.
- The convention requires processing of personal data for purposes of, *inter alia*, state security, defence or public security should be based on a sector or domain-specific law to be adopted with the "informed advice" of the national data protection authority.[132] In contrast, such types of processing are exempted from Ethiopia's Data Protection Bill.[133]

128 AU Convention on Cyber Security and Personal Data Protection (2014), Article 14(1) cum Article 1.

129 Ibid., Article 9(2(a)).

130 Ibid., Article 9(2(b)).

131 Ibid., Article 14(3).

132 Ibid., Article 10(5).

133 Draft Data Protection Proclamation (April 2020), Article 63(1(a)).

- The convention imposes "sustainability obligations" on data controllers to ensure further utilisation of processed personal data regardless of technical devices used.[134] While Ethiopia's bill guarantees the right to data portability by which data subjects may receive and move their personal data from one controller to another in commonly used and machine-readable format,[135] it does not specifically include such a duty. But the right to data portability is subject to exceptions, for example when the rights and freedoms of others may be affected.

### *In light of the Declaration of Principles*

While the Declaration of Principles – adopted by the African Commission on Human and Peoples' Rights (ACHPR) in 2019 – focuses primarily on freedom of expression and access to information, it addresses privacy and data protection in part IV. It does so in three steps. First – and in line with Principle 8 of AfDec – the declaration guarantees the right to privacy online, including communicating anonymously through the use of privacy-enhancing technologies.[136] But it goes a little further than AfDec when it requires states to refrain from engaging in arbitrary measures that would undermine secure and private communications such as weakening encryption, mandating key escrows and backdoors or data localisation. As highlighted above, the Ethiopian Constitution guarantees the right to privacy online as well as offline. But while the digital privacy jurisprudence is thin, if not non-existent, the right to privacy arguably protects the use of privacy-enhancing technologies and imposes a negative duty on the government to refrain from

134 AU Convention on Cyber Security and Personal Data Protection (2014), Article 23.

135 Draft Data Protection Proclamation (April 2020), Article 43.

136 Declaration of Principles on Freedom of Expression and Access to Information (2019), Principle 40.

taking measures that would undermine the enjoyment of the right to privacy, such as weakening encryption or requiring back doors or key escrows.

Second, the Declaration of Principles prohibits mass surveillance and bulk collection, storage, analysis or sharing of personal data.[137] Moreover, it stipulates that even when the surveillance is targeted, a series of safeguards must be put in place to prevent or remedy arbitrary practices. Such safeguards include prior independent oversight, due process, restriction on the time, manner and scope of the surveillance, and *post facto* notification to the surveilled subject. Ethiopia currently has no comprehensive legal regime on surveillance. Rules governing electronic surveillance are scattered across several pieces of legislation such as the anti-terrorism, telecom fraud offence and intelligence and security services laws. It is not entirely clear if mass surveillance is prohibited by Ethiopian law but a closer look at relevant pieces of legislation suggests that it is. Key rules governing digital surveillance are provided in the Anti-terrorism Proclamation which mandates electronic surveillance – referred to as special investigative techniques – in terrorism investigations only as a measure of last resort.[138] It is only when (a) the investigation concerns terrorist acts that pose serious danger to the nation and (b) regular investigative techniques provided in criminal procedure laws are inadequate that surveillance will be carried out.

This suggests that surveillance in anti-terror investigations must be targeted, not at a massive scale. This is further espoused by a series of safeguards provided by law. One is that surveillance

137 Ibid., Principle 41.

138 Prevention and Suppression of Terrorism Proclamation No 1176/2020, Article 46. See also Article 8(7) cum Article 24 of Proclamation No 804/2013.

may be undertaken only with a prior court warrant unless in urgent cases where the police must first seek approval, from the prosecution department and later from courts, within 48 hours.[139] Moreover, the law states that when issuing wiretap warrants, courts must specify the technique to be employed and the time and manner of surveillance.[140] If courts are convinced of the necessity of the surveillance, they may grant three months, which may later be extended for one more month after having evaluated the performance of investigators.[141] By and large, these rules on government surveillance are consistent with Declaration of Principles, except for two important safeguards. One is a due process safeguard by which surveilled subjects may challenge the measure or even seek remedy against arbitrary or unlawful surveillance and the other is a post-surveillance notification to the subject. It is vital to note that the Ethiopian government has been accused in the past of engaging in mass telecom surveillance and bulk collection of data.[142] But it is not clear if the above highlighted prohibitions have been respected in practice.

Third, the Declaration of Principles requires states to adopt data protection laws that stipulate principles of processing of personal data guarantee data subject rights and institute a national data protection authority.[143] As highlighted above, Ethiopia does not have a comprehensive data protection law but only rules scattered across various pieces of legislation. But its recently released data protection law – discussed above – embodies almost all of the data protection principles, data subject rights and mandates the creation of a national data protection authority. Perhaps the only variation is that the declaration addresses

139 Ibid., Article 42(3).

140 Ibid., Article 42(4).

141 Ibid., Article 42(7).

142 Human Rights Watch. (2014, 25 March). Op. cit.

143 Declaration of Principles on Freedom of Expression and Access to Information (2019), Principle 42.

revenge and child pornography, requiring states to criminalise such "harmful sharing of personal information". However, these conducts are already criminalised by Ethiopian cybercrime law.[144]

Overall, the current Ethiopian legal framework by and large complies with the ACHPR's Declaration of Principles rules on privacy and data protection. When it does not, it is because Ethiopia is yet to adopt comprehensive data protection and surveillance legislation. If the declaration constitutes an authoritative interpretation of the Banjul Charter to which Ethiopia is a state party, Ethiopia is bound to make its laws in line with the declaration, including by enacting the draft data protection law soon.

### *International review of Ethiopia's data privacy commitments: UPR and beyond*

Ethiopia has been reviewed in the Universal Periodic Review (UPR) mechanism three times: first cycle in December 2009, second cycle in May 2014 and third cycle in May 2019.[145] But the right to privacy was rarely mentioned during the review process. In the latest UPR cycle, for example, the single instance where privacy surfaced was when Germany recommended that Ethiopia amend the Computer Crime Proclamation, arguing that it threatened the right to privacy.[146] Ethiopia has "supported" this recommendation.[147] Perhaps partly as a follow-up to this expression of a will to amend the law, the government started the process of revising the cybercrime law in 2019.

The UN Human Rights Committee has rarely commented on issues of privacy in Ethiopia. One such instance was in a 2011

144 Computer Crime Proclamation No 958 /2016, Articles 12-13.

145 https://www.ohchr.org/EN/HRBodies/UPR/Pages/ETIndex.aspx

146 Report of the Working Group on the Universal Periodic Review: Ethiopia, UN Doc A/HRC/42/14 (5 July 2019), paras 163.62.

147 Universal Periodic Review: Ethiopia (3rd Cycle, 2019), Recommendation No 44. https://bit.ly/3lGs6Ph

concluding observation where it noted that the criminalisation of homosexuality and other indecent acts violated the right to privacy. Accordingly, the committee recommended that Ethiopia "decriminalise sexual relations between consenting adults of the same sex in order to bring its legislation in line with the ICCPR and to put an end to the social stigmatisation of homosexuality".[148] Thus, other privacy issues, particularly data privacy in Ethiopia, have not been considered by the committee. But its General Comment 16 on Article 17 of the ICCPR – while slightly outdated – addresses important data protection and digital surveillance principles.[149] As an authoritative interpretation of Article 17, Ethiopia is arguably bound by General Comment 16, which remains a non-legal soft law.

Privacy and data protection also never surfaced during Ethiopia's review at the ACHPR. The more recent concurring observation of the ACHPR is from 2015, and the right to privacy was not among the human rights considered by the commission.[150] In part, this is because the review follows human rights guaranteed in the Banjul Charter and – as already highlighted – does not expressly protect the right to privacy. But with the adoption of the Declaration of Principles, which as discussed above addresses privacy, the commission's privacy jurisprudence and its review of state parties is likely to closely consider the right to privacy.

## A human rights-based approach to privacy and data protection in Ethiopia

What follows examines the development and application of Ethiopia's data protection framework in the light of the five

148 Concluding observations of the Human Rights Committee: Ethiopia, UN Doc CCPR/C/ETH/CO/1 (19 August 2011), para 12.

149 General Comment 16: The Right to Privacy (Human Rights Committee, April 1988), paras 8-10.

150 Concluding Observations and Recommendations on the 5th and 6th Periodic Report of Ethiopia (African Commission on Human and Peoples' Rights, August 2015).

fundamental principles of a human rights-based approach.[151] The discussion is, however, circumscribed by the fact that Ethiopia currently has only a draft data protection law and that existing rules are scattered across various pieces of legislation.

### *Principle of participation*

This principle concerns the right of everyone to actively participate in decision-making processes that affect the enjoyment of their rights. Ethiopia's legislative processes of introducing data protection legislation did not comply with this principle. As highlighted above, Ethiopia has been in the process of developing comprehensive data protection legislation since 2007, with the first draft released two years later and the latest in 2020. But the processes of developing these two pieces of legislation were not demonstrably inclusive and much of the work was undertaken behind closed doors. For instance, not only was the process of writing the 2020 draft a closely guarded secret but the draft was also only released to a small circle of individuals and groups. So far, no meaningful public consultation has been held on the draft. The Ministry of Innovation and Technology sought feedback in a call sent out to a mailing list in April 2020, and those invited were asked to provide their comments in Google Forms.[152] No public consultation has been held since then on the draft data protection law. This suggests that not everyone whose rights would be affected by the enactment of the law had the opportunity to participate in the development of the law. This is part of an apparent tendency in the past few years to rush bills for legislative imprimatur. A number of important pieces of legislation, including the Communications Service Proclamation – which opens up the telecom sector for

151 http://ennhri.org/about-nhris/human-rights-based-approach

152 https://bit.ly/3ltXsZg

the private sector – have been adopted without meaningful public consultation.[153] Relatively better public consultation was held on a series of subsidiary telecom pieces of legislation. Relevant to data protection is the Consumer Rights and Protection Directive (2020), which appears to embody sector-specific data privacy rules. Unlike the Data Protection Bill, the directive has been available for public consultation by ECA for a reasonable period of time.[154] Until the ministry takes a turn and holds meaningful consultation before the bill becomes a law, it would fail to meet the principle of participation.

### *Principle of accountability*

This principle concerns the mechanism by which duty bearers – in the context of data protection, data controllers, data processors and even national data protection authorities – may be held to account for violating the rights of right holders – in the data protection context, data subjects. A key component of this principle is that there should be effective redress to remedy rights violations. Ethiopia's draft data protection law offers mechanisms by which data controllers and processors would be held to account and remedies are also recognised to right wrongs. One is that the bill imposes a number of obligations on data controllers and processors,[155] and mandates the institution of data protection officers.[156] The national data protection authority, the Data Protection Commission, would also have a central role in holding duty-bearers to account.[157] Of course, decisions of the commission, as any administrative adjudicator, may also be appealed to the courts, although it is not clear if

153 Yilma, K. (2020, 16 May). Beware of Overboard Cyber Legislation. *Fortune*. https://bit.ly/3nCP7Ex

154 https://eca.et/public-consultations

155 Draft Data Protection Proclamation (2020), Articles 16-44, 53-62.

156 Ibid., Article 52.

157 Ibid., Articles 6, 65-80.

the appeal would be only on a point of law.[158] Other existing laws, particularly the access to information legislation, similarly provides an accountability mechanism. As discussed above, any person aggrieved by the decision of a public relations officer of a public body (either to allow or deny disclosure of a personal data) may appeal: first, to the head of the public body and second, to the Institution of the Ombudsman and finally to a court.[159]

Despite recognition of the right to privacy as a constitutional human right in Ethiopia, whether it is justiciable or not is unclear. There has been no privacy or data protection case based on the right to privacy in the Ethiopian Constitution. But the right of image guaranteed under the Civil Code has been tested in courts in recent years where data subjects have been awarded damages for violation of this right. In *Riyan Miftah v Elsewedy Cables Plc*, the Cassation Court ruled that no image or photograph of a person may be publicly exhibited, sold, or disseminated without the consent of the person, and the latter is entitled to damages for violation of the right to their own image.[160] In *Dashin Bank v Dorina Avakiyan,* the same court affirmed lower court decisions including the amount of damages, holding that (a) the display of the plaintiff's image was without consent and that impugned exhibition does not fall under the exceptions and that (b) the respondent was the focus of the advert in that the message conveyed (i.e. customers with overseas bank cards could use Dash Bank's services with their cards) deliberately emphasised that the respondent is a foreigner.[161] But interestingly, in tracing the constitutional source of the Civil Code's right of image provisions, it made reference to Art 14 of the constitution: "rights

158 Ibid., Article 81.

159 Ethiopian Institution of the Ombudsman Establishment Proclamation No 211/2000, Articles 31-32, 34.

160 *Riyan Miftah v Elsewedy Cables Plc.* (2013).

161 *Dashin Bank v Dorina Avakiyan. (2018)*.

to life, the security of person and liberty". But this assertion completely overlooks the fact that the right of image, as one element of the bundled rights of personality, relates more to the right to privacy guaranteed under Art 26 of the constitution. Indeed, although the Civil Code was adopted in 1960, it provides that "every physical person shall enjoy the rights of personality and the liberties guaranteed by the Ethiopian Constitution."[162]

### *Principle of non-discrimination and equality*

The principle of non-discrimination and equality holds that the rights of all individuals should be guaranteed without discrimination of any kind. The right to equality is unequivocally guaranteed under the Ethiopian Constitution.[163] "All persons" are treated as equal before the law and are entitled without any discrimination to the equal protection of the law. Moreover, the constitution prohibits discrimination on an illustrative list of grounds, including race, religion, sex, political opinion or social status.[164] This is on top of international and regional human rights commitments by which Ethiopia is bound to uphold the right to equality and prohibit, prevent and eliminate discrimination of all types.

Similarly, the right to privacy in the constitution is guaranteed to "everyone" regardless of nationality or any other status. This means that the state's duty to respect and protect the right to privacy, including protection of data privacy, must be discharged equally to every rights holder without discrimination. Subsidiary pieces of legislation similarly uphold the right to equality and the principle of non-discrimination. For instance, the rights of personality under the Ethiopian Civil Code, as noted above, are

162 Civil Code of Ethiopia, Proclamation No 165/1960, Article 8(1).

163 Ethiopian Constitution (1994), Article 25.

164 Ibid.

guaranteed to “every physical person”. The draft Data Protection Proclamation follows suits in this regard. When defining its “object and purpose”, the bill provides that it objective is to “secure in Ethiopia for every individual, whatever his nationality or residence, respect for his rights and freedoms, and in particular his right to privacy [...].”[165] In line with the above highlighted constitutional proviso, the bill upholds the right to equality and the principle of non-discrimination.

### *Principle of empowerment*

The fourth principle in the human rights-based approach is empowerment, which concerns the ability of individuals to claim and exercise their rights. To be empowered, individuals should be able to understand their rights, and the ways and means of exercising them. And to understand one’s rights, individuals should have the opportunity to know their rights. In this respect, human rights education plays a key role. In Ethiopia, the national human rights institution – the Ethiopian Human Rights Commission – has a statutory role to “educate the public, using the mass media and other means, with a view to enhancing its tradition of respect for, and demand for enforcement of, rights upon acquiring sufficient awareness regarding human rights”.[166] Human rights education would empower individuals to know, claim and exercise their rights, including the right to privacy and data protection. In the data protection context, the draft Data Protection Proclamation tasks the Data Protection Commission to “promote public awareness of ‘the rights of data subjects and the exercise of such rights’ as well as promote its ‘functions and powers as well as activities’.”[167] Education about what rights data subjects are entitled to and

165 Draft Data Protection Proclamation (April 2020), Article 3.

166 Ethiopian Human Rights Commission Establishment Proclamation No 210/2000 (as amended by Proclamation 1224/2020), Articles 6(3) cum Article 5.

167 Draft Data Protection Proclamation (April 2020), Article 6(5).

where they could go to have them enforced would empower individuals. An aspect of empowerment is the ability of lawful heirs and guardians of legally incapacitated individuals to exercise the rights of the data subject.[168] The bill also requires data controllers to bring to the attention of data subjects their rights, particularly their right to object to the processing of personal data.[169]

### *Principle of legality*

In a human rights-based approach, the principle of legality provides that measures or approaches should be in line with legal rights guaranteed in domestic and international laws. In some respects, the principle of legality is not complied with in Ethiopia. For example, Ethiopia's current data protection law, as highlighted above, does not provide accepted exemptions for certain data processing activities.[170] Good cases in point are the processing of personal data for journalistic and artistic purposes. Because such processing activities are not exempted, media organisations or journalists and artists would be treated as data controllers and/or processors and hence subject to a series of obligations. And being subjected to cumbersome regulatory rules may significantly restrict freedom of expression. Thus, Ethiopia's draft data protection legislation tends to restrict the right to free expression guaranteed under domestic law (e.g. Article 29 of the Ethiopian Constitution) and international human rights law (e.g. Article 19 of the ICCPR).

In sum, Ethiopia's current and developing legal framework on privacy and data protection conforms by and large to the five principles of the human rights-based approach. As the above

168 Ibid., Article 44.

169 Ibid., Article 41(4).

170 Ibid., Article 63.

analysis has shown, it is mainly in relation to the principle of participation and legality that Ethiopia's data protection law and regulation slightly fails to meet the standards.

## Concluding observations and recommendations

This report has explored the state of privacy and data protection in Ethiopia. A salient feature of the country's current privacy and data protection framework is that it is deeply fragmented and hence unfit for purpose. While Ethiopia currently has no compressive data protection law, there are some data protection standards scattered across various pieces of legislation. This means that not only does Ethiopia have no dedicated national data protection authority but also that the role of overseeing the protection of privacy and data protection falls on disparate entities. Moreover, with the recent rapid progress in the field of data protection law, this set of fragmentary data protection standards is largely outmoded. Nor is there jurisprudence that progressively interprets these fragmentary privacy and data protection standards. But the Ethiopian Constitution which came into force in 1995 provides a sound legal basis for the protection of privacy and data protection. As shown in the report, the constitution envisages a comprehensive and progressive vision of the right to privacy in that it protects the right to privacy in online and offline contexts. It also provides an enabling clause for the adoption of a comprehensive data protection law that governs the processing of personal data both in the public and private sector and creates a national data protection authority.

In line with this constitutional proviso, the government has recently released a draft Data Protection Proclamation. The content of this bill contains widely accepted data protection principles and data subject rights and proposes the creation

of a national data protection authority. As shown in this report, the bill is generally consistent with international best practices including regional standards like the Malabo Convention. Indeed, introducing a data protection legislation that protects the right to privacy and data protection is also arguably required in international human rights treaties to which Ethiopia is a party, particularly the ICCPR. The analysis of the developing legal framework on privacy and data protection in light of the human rights-based approach revealed that except for the principle of participation, the legal framework is overall compliant with the principles of accountability, non-discrimination and equality, empowerment and legality. This report closes by offering the following recommendations to the three key stakeholders: the government, civil society groups and the private sector:

To the government:

- Adopt a comprehensive data protection legislation in light of international best practices, existing privacy and data protection standards and based on input from stakeholders.
- Ensure respect for the rights of data subjects when processing of personal data is undertaken by the public sector.
- Foster international cooperation for effecting the protection of data privacy in the transnational context.
- Adopt a comprehensive surveillance legislation with adequate safeguards against arbitrary collection of personal data, surveillance and interception of communications.

To civil society groups:

- Raise public awareness about data subject rights, remedies and recourse mechanisms.

- Pursue strategic litigation against persistent violations of data protection principles and data subject rights as well as surveillance legislation.
- Actively advocate for changes to and adoption of laws protective of data privacy.

To the private sector:

- Ensure respect for the protection of data subject rights and data protection principles in the course of collecting, processing and disclosing personal data.
- Adopt codes of conduct on practices of data collection, processing and dissemination.
- Issue transparency reports on data collection, processing and sharing practices as well as requests for user data by the government.

# Kenya

Sigi Waigumo Mwanzia[1]

## Executive summary

Kenya's legislative data protection framework, the Data Protection Act (DPA) of 2019, and practice are still in their nascent stages. This offers many opportunities and challenges to promote the entrenchment of best practices in the data protection and privacy arena and to advocate for the simultaneous application of the human rights-based approach framework as outlined in the report below.

Since 2007, various stakeholders including civil society organisations (CSOs), private sector entities and international organisations, amongst others, have been at the forefront of advocating for a comprehensive information privacy framework.

1 The author would like to express appreciation to Ben Roberts (Liquid Telecom), Mercy Mutemi (Nzili and Sumbi Advocates), Grace Bomu (Centre for Intellectual Property and Information Technology Law, Strathmore University) and Gloria Madegwa and Esban Muthoni (Defenders Coalition) who participated in the interviews that supplemented and enriched this country report with multistakeholder perspectives.

In recent times, these advocacy efforts have involved the filing of judicial petitions seeking the implementation of constitutional provisions on privacy and data protection, strengthening of the provisions of the DPA, prevention of the abuse of state powers and/or the infringement of privacy rights by the national government and its agencies during the COVID-19 pandemic, among others.

This report notes that the main challenge in Kenya's data protection and privacy sphere includes a reluctance and failure to internalise and implement the provisions of the DPA by both state and non-state actors, nearly a year after the framework was enacted in November 2019. This will be a key issue for the data protection (regulatory) authority tasked with overseeing the implementation of the DPA, which the government is in the process of establishing.

This report is intended for African Declaration on Internet Rights and Freedoms (AfDec) Coalition members, regional bodies, national human rights institutions, data protection authorities, digital rights activists, CSOs, media rights journalists and bloggers concerned with human rights and internet governance.

## Methodology

This country report was generated using primary information received from Kenya-based partners (individuals and organisations), and secondary information sourced online.

The primary information was collected via semi-structured interviews using a set of carefully tailored questions which were specific to each interviewee, as well as general questions addressed to the entire group. These questions sought the interviewee's

individual and organisational perceptions about Kenya's data protection and privacy sphere, including the DPA's enactment process, implementation challenges and opportunities noted so far. The interviewees were selected according to commonly-recognised stakeholder groupings, and included the government, CSOs, academia, private sector and the technical community, as well as sectoral expertise at the policy, technology, human rights, research and legal levels. The interviewees were selected using random (stratified) sampling and interviews were all conducted using a secure teleconferencing platform, namely Zoom.

The secondary information was collected via online desk research which was restricted to the 2007 to 2020 period, given the significance of this timeline for the data protection (legislative) process. This information included the Constitution of Kenya, 2010, the DPA, 2019 and other relevant administrative, policy, regulatory and legislative documents, international and regional material (treaties, instruments, standards, review processes), litigation material from national courts (pleadings and determinations), research reports and other assessments expounding on Kenya's political, economic, social and rights context for purposes of the DPA, 2019.

## Country context

The period from 2007 to 2020 in Kenya was characterised by significant social, political and economic advancements and changes. These triple indicators of developmental progress have all been affected by shocks occasioned by the COVID-19 global pandemic.

Kenya's development blueprint, Vision 2030, was launched in 2008 and encapsulates Kenya's broad economic, social and

political strategies.[2] This developmental blueprint is being implemented in stages through five-year medium-term plans and complements Kenya's commitments under the Sustainable Development Goals (SDGs)[3] and the African Union Agenda 2063.[4]

Politically, the Constitution of Kenya (2010) provides for the transformative interpretation and application of civil, political, economic, social and cultural rights across all 47 counties in the Republic of Kenya. This transformative potential is further encapsulated in the Bill of Rights which contains numerous human-rights (including internet-related rights) guarantees which are indicative of Kenya's firm commitment to the human rights-based approach, at least at the theoretical level.

The Constitution of Kenya, 2010 was promulgated following mass calls for democratic reforms, pluralism, ceasure of the presidency's dominance and the state's practice of secrecy and information controls. These calls were also heavily influenced by the effects of the 2007 elections and post-election violence,[5] which was itself symptomatic of systemic post-independence challenges. These challenges – most of which persist to date – included economic disparities,[6] governance failures, mass corruption, land grievances, and the "political manipulation of ethnic tensions,"[7] amongst others. All these challenges led to a desire and strong push for "the second liberation."[8]

2 https://vision2030.go.ke/

3 https://sustainabledevelopment.un.org/memberstates/kenya

4 https://au.int/en/agenda2063/overview

5 This election, and the processes which arose subsequently, were marred by electoral irregularities, violence and the politicisation of international criminal processes.

6 Brownsell, J. (2013, 3 March). Kenya: What went wrong in 2007? *Al Jazeera*. https://www.aljazeera.com/features/2013/3/3/kenya-what-went-wrong-in-2007

7 Human Rights Watch. (2008, 16 March). Ballots to Bullets: Organized Political Violence and Kenya's Crisis of Governance. https://www.hrw.org/report/2008/03/16/ballots-bullets/organized-political-violence-and-kenyas-crisis-governance

8 Interview with Grace Mutung'u, research fellow at the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, 12 October 2020.

On the socioeconomic front, Kenya maintained her position as "one of the fastest growing economies in Sub-Saharan Africa"[9] in 2019. Despite this, the country's burgeoning public debt (external and domestic) rose from KSH 5,607.91 billion (USD 51.523 billion) in May 2019 to KSH 6,282.82 billion (USD 57.718 billion) in May 2020.[10] This has further been met by challenges of a fluctuating currency[11] and dwindling foreign exchange reserves.[12] These challenges continue to affect Kenya's social environment, as well as fledgling "green economy" and "smart city" drives.

Kenya continues to promote and protect internet-related human rights through its Bill of Rights and via the extensive expansion of the nation's information, technology and communications (ICT) policy and legislative frameworks. Secondly, Kenya has invested heavily, either through state-sponsored initiatives or public-private partnerships, in ICT infrastructure which continues to promote individuals' ability to access and use digital platforms and communication technologies. ICT policy making, and in some instances, regulatory powers, continue to be relegated to either the ICT Ministry, the National Communications Secretariat[13] or the Communications Authority of Kenya, which all have divergent mandates. On the other hand, legislative powers rest exclusively with Kenya's bicameral legislature, which has enacted numerous frameworks promoting the protection of internet-related human rights.

9 https://www.worldbank.org/en/country/kenya/overview

10 Central Bank of Kenya. (2020). *Monthly Economic Indicators, May 2020*. http://www.centralbank.go.ke/monthly-economic-indicators

11 Guguyu, O., & Ambani, B. (2020, 23 September). Central Bank loses grip on the Kenyan shilling. *Nation.* https://nation.africa/kenya/business/cbk-loses-grip-on-the-kenyan-shilling-2305786

12 Omondi, D. (2020, 29 March). CBK boss goes all out to protect Shilling. *The Standard.* https://www.standardmedia.co.ke/business/article/2001366051/cbk-boss-goes-all-out-to-protect-shilling

13 The NCS is tasked with "advising the Government on the adoption of a communication policy" under section 84 of the Kenya Information and Communications Act. (1998). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%201998

The establishment of a data protection framework in Kenya has been driven and stalled by numerous incentives and barriers. Economic and trade considerations, following the imposition of extraterritorial responsibilities located in the GDPR and Kenya's desire to retain her "competitive edge" against African countries with established data protection frameworks, shaped the government's priorities and reinforced political will.[14] Crucially, these considerations were solidified following Kenya's voluntary championing of the "digital economy" agenda,[15] as part of her Smart Africa Alliance membership.[16] It is crucial to note that these twin considerations shattered the government's initial legislative reluctance, and watered down the perception that a framework would erect barriers affecting the government's previously unchecked collection and processing of individuals' personal data for numerous agendas, including the registration of persons.

Conversely, civil society organisations "strengthened their coordination efforts"[17] and solidified their calls for the legislative framework following two fundamental events: the data-driven 2017 election – and the petition which was subsequently lodged – and the government's introduction of digital identity drives in 2019. Private sector actors and the technical internet community were largely motivated by the desire to maintain their competitive edge, in an increasingly consumer-aware and privacy-hungry market.

Multiple stakeholders from different sectors continue to impact and shape Kenya's personal data protection landscape, and either influence or retard the entrenchment of a human rights-based

14 Interviews with Grace Mutung'u, research fellow at the Centre for Intellectual Property and Information Technology Law, Strathmore University, 12 October 2020 and John Walubengo, lecturer and member of the National Taskforce on Blockchain & AI, 10 October 2020.

15 ICT Ministry. (2019). *Digital Economy Blueprint.* https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf

16 https://smartafrica.org

17 Interview with Grace Mutung'u, 12 October 2020. Op. cit.

approach to data protection. These include, but are not limited to, members of the public,[18] state agencies,[19] civil society organisations,[20] constitutional commissions,[21] private sector entities (including those without a physical presence in Kenya)[22] and academics.[23]

## Constitutional underpinning

The right to privacy and data protection is explicitly guaranteed under Article 31, Constitution of Kenya, 2010. This right is limited and derogable, subject to the legality, necessity and proportionality limbs under Article 24, and provides as follows:

> Every person has the right to privacy, which includes the right not to have:
>
> - their person, home or property searched
> - their possessions seized
> - information relating to their family or private affairs unnecessarily required or revealed
> - the privacy of their communications infringed.

18 These include, but are not limited to, Abraham M. Kilonzo (ICT personnel), Alex Gakuru (technology rights defender), Michael Gitagia, Mugambi Laibuta (trained mediator and policy and legislative drafting professional), Nicholas Kanyagia, Mark Tum, and Peter Muya (ICT consultant). See the Communications Authority of Kenya's "Published Findings": https://ca.go.ke/consumers/public-consultations/published-findings

19 These include, but are not limited to, the ODPC, the ICT Ministry, the CA, the CAK, the National Cohesion and Integration Commission, the National Security Advisory Committee. During the taskforce deliberations (2018), external state agencies from the United States provided comments, including the US Department of Commerce's International Trade Administration and the US Chamber of Commerce. Ibid.

20 These include, but are not limited to, Amnesty International Kenya, ARTICLE 19, the Kenya ICT Action Network, the National Coalition of Human Rights Defenders (Kenya), Privacy International, Research ICT Africa, and FSD Kenya, between 2018 and 2019. Ibid.

21 These include, but are not limited to, the KNCHR and the CAJ. Ibid.

22 These include, but are not limited to, Google Kenya, Facebook, Technology Service Providers of Kenya, CODE-IP, the Kenya Private Sector Alliance, Mozilla, Amazon Web Services, Airtel, GSMA, IBM, KENIC, Microsoft, MultiChoice Kenya, Safaricom PLC, Savannah Training Solution Limited, Seven Seas Technologies Group, the Foschini Group Kenya Limited, Uber East Africa, AIG Kenya Insurance Company Ltd, Allan Gray Kenya Limited, ATLANCIS Technologies, Branch International Limited, InVenture Mobile Limited (Tala), KCB Bank Kenya, Mastercard, M-Kopa Solar, between 2018 and 2019. Crucially, law firms also actively submitted comments during the 2018-2019 processes. Ibid.

23 This includes, but is not limited to, the Centre for Intellectual Property and Information Technology Law.

Crucially, Article 19 (2) reiterates that the "purpose of recognising and protecting human rights and fundamental freedoms is to preserve the dignity of individuals and communities and to promote social justice and the realisation of the potential of all human beings."

The judiciary continues to interpret this right, as far back as 2007 and as recently as 2020, with most cases being raised against mass or closely-affiliated data controllers and processors including the state, private entities and individuals. These have been centred on issues affecting human dignity generally; inter-sex persons in prison;[24] privacy rights accruing to state corporations and third parties in the context of illegally-obtained information with a public interest;[25] waiving of consent during warrantless search-and-seizure investigations by the national police service[26] and the use of (thin SIM) technology;[27] the distribution of private photographs;[28] the installation of the device management system with alleged capabilities to interfere with private communications;[29] search-and-seizure of data stored on a computer system without mandatory judicial oversight;[30] Kenya Revenue Authority's sourcing of tax information, including from third parties, without warrants;[31] and the privacy risks latent in Kenya's digital ID system (NIIMS),[32] amongst others.

24 *R.M v Attorney General & 4 others* [2010] eKLR. http://kenyalaw.org/caselaw/cases/view/72818

25 *Okiya Omtatah Okoiti & 2 others v Attorney General & 3 others* [2014] eKLR. http://kenyalaw.org/caselaw/cases/view/103808

26 *Samson Mumo Mutinda v Inspector General National Police Service & 4 others* [2014] eKLR. http://kenyalaw.org/caselaw/cases/view/94430

27 *Bernard Murage v Fineserve Africa Limited & 3 others* [2015] eKLR. http://kenyalaw.org/caselaw/cases/view/109772

28 *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* [2016] eKLR. http://kenyalaw.org/caselaw/cases/view/129282

29 *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/193383/

30 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/191276/

31 *Okiya Omtatah Okoiti v Attorney General & another* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/191427/

32 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/189189/

Notably, Kenyan courts took notice of the lack of a comprehensive legislative framework but refrained from exercising judicial discretion given the existence of the "separation of the powers" principle in the constitution. Instrumentally, the High Court in the latter case took judicial notice of the DPA, 2019 and issued two crucial statements: the need for an "effective implementation and enforcement" of the DPA, 2019, and the existence of various "gaps" in the framework with implications for children. These judgments continue to have varying effects on the protection of personal data and privacy, and the implementation of the human rights-based approach in Kenya.

## Existence of other laws dealing with privacy and data protection online

Kenya's legislative arena is laden with frameworks containing insufficient offline and online privacy and data protection provisions. These include the National Payment System Act (2011),[33] the Consumer Protection Act (2012),[34] amendments to the KICA, 1998 and its regulations, including the Consumer Protection Regulations (2010) and the Registration of SIM Cards Regulations (2015).

Additionally, the Access to Information Act (ATI Act) (2016)[35] contains various data protection provisions, and empowers the CAJ with dual data protection and access to information powers. As noted above, this linkage was part of drives to push for "the second liberation", where stakeholders recognised and affirmed the mutually-reinforcing nature of the right to privacy and

33 http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2039%20of%202011

34 Section 2, Consumer Protection Act (2012) defines personal information as "information other than credit information about a consumer's character, reputation, health, physical or personal characteristics or mode of living or about any other matter concerning the consumer." http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2046%20of%202012

35 Section 21 (1) (a to h), Access to Information Act (2016). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016

data protection and access to information. Despite this, these provisions do not offer comprehensive guarantees protecting the right to privacy and data protection, and the CAJ has not allocated the same amount of resources to the data protection components of its mandate.

While Articles 31 and 33, Constitution of Kenya, 2010 are interpreted as promoting the right to digital anonymity and "pseudonymous expression",[36] mandatory SIM card registration drives by the Kenyan government have watered down these protections. Despite Kenya avoiding the implementation of "real-name policies", as proposed in the KICA (Amendment) Bill, 2019,[37] and refraining from barring the use of anonymity tools in legislative frameworks, the "unauthorised interference" provision in the Computer Misuse and Cybercrimes Act (2018) affects encryption rights. As ARTICLE 19 noted in its 2015 report, "encryption rights are crucial for various stakeholders, including human rights defenders, whistleblowers, journalists and activists who are often the subject of surveillance by intelligence or law enforcement agencies."[38]

## Regional and international commitments on privacy and personal data protection

Kenya, by virtue of Articles 2(5) and (6), Constitution of Kenya, 2010, recognises that the "general rules of international law shall form part of the law of Kenya" and that "any treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution." By virtue of international law and these constitutional provisions, Kenya is bound to numerous regional and international commitments on privacy and data protection.

36 Monteiro, A. (2014, 13 June). Access intervenes at ECtHR for the right to be anonymous online. *Access Now*. https://www.accessnow.org/access-intervenes-at-ecthr-for-the-right-to-be-anonymous-online

37 http://kenyalaw.org/kl/index.php?id=9091

38 ARTICLE 19. (2015). *Right to Online Anonymity.* https://www.article19.org/resources/report-the-right-to-online-anonymity

At the regional (AU) level, Kenya's data protection and privacy responsibilities can be inferred under various provisions, including Articles 4 to 6, of the African Charter which guarantee the "inviolability of the human being," "human dignity" and individual "liberty and security". The continued failure to insert an explicit right to privacy in the African Charter has resulted in numerous countries, including Kenya, being "implicitly bound" under other instruments, including the ACERWC, 1990, which Kenya ratified and deposited in 2000.[39]

Kenya is one of 44 AU member states which have not ratified the AU Convention. However, in 2018, Kenya's ratification of the region's free trade agreement, the AfCFTA, imbued the state with privacy and data protection responsibilities. Article 15 (a)(ii), AfCFTA provides that states must take measures to ensure "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[40]

Furthermore, Kenya stands guided by Principles 40 and 41 of the ACHPR Declaration due to its soft law status which maintains that "everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information" and protections from both targeted and mass surveillance.[41] Kenya also stands guided by the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa[42] which recognised that "privacy online is

39 ACERWC. (2020). *Ratifications Table*. https://www.acerwc.africa/ratifications-table/

40 The Africa Union. (2018). *Agreement Establishing the African Continental Free Trade Area*. https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area

41 African Commission on Human and Peoples' Rights. (2019). *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019.* https://www.achpr.org/legalinstruments/detail?id=69

42 ACHPR. (2017) *Recommendations and Resolutions Adopted by the African Commission on Human and Peoples' Rights - ACHPR/Res. 362(LIX) 2016: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa*. https://www.achpr.org/adoptedresolution

important for the realisation of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."

At the sub-regional (EAC) level, the heads of states continue to withhold their assent to the EAC Human and Peoples' Rights Bill (2011), which would have provided the peoples of the sub-region, including Kenya, with an explicit (sub-regional) right to privacy under Article 19 of this bill.[43] Out of the six EAC member states, Kenya surprisingly failed to offer its usual sub-regional leadership on the legislative front, following Uganda's enactment of its data protection framework in February 2019 as well as Rwanda's ratification of the AU Convention in October 2019, before Kenya enacted her own data protection framework in November 2019.

Internationally, Kenya is bound by Article 17, ICCPR which guarantees individuals' right to privacy (over their) "family, home or correspondence." Positively, Kenya reaffirmed its commitment to the promotion of internet freedom, including the right to privacy online, through its Freedom Online Coalition membership.[44] The Republic of Kenya pledged, in conjunction with multiple stakeholders, to "adopt and encourage policies and practices, nationally and internationally, that promote the protection of human rights and fundamental freedoms online."[45]

Lastly, despite efforts by the Council of Europe (Data Protection Unit), to convince various states, including Kenya, to accede to and integrate the "international standards as enshrined

43 Greenleaf, G., & Cottier, B. (2020). *Comparing African Data Privacy Laws: International, African and Regional Commitments*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478

44 https://freedomonlinecoalition.com/about-us/members

45 Freedom Online Coalition. (2014). *The Tallinn Agenda - Recommendations for Freedom Online*. https://freedomonlinecoalition.com/underpinning-documents

in Convention 108+,"[46] Kenya is still one of the many non-EU member states which have not yet ratified Convention 108.[47]

## Existence of a comprehensive data protection law

Kenya's Data Protection Act, 2019 (DPA) received presidential assent on 8 November 2019 and came into force shortly thereafter on 25 November 2019. The decision to formalise the data protection process commenced, at least for some stakeholders, in 2007, following calls for the "second liberation", and the desire for democratic, right-respecting, transparent and accountable processes and institutions in Kenya.

Between 2016 and 2018, civil society organisations working or interested in information rights (including the right to access information, expression and privacy under Articles 31, 33 and 25, Constitution of Kenya, 2010) converged efforts, resources and interests. This convergence witnessed the successful enactment of an information access legislation, i.e., the ATI Act, 2016, and led to a diversion of their calls for an exclusive informational privacy legislative framework.

These calls were formally responded to by the ICT Ministry, following its constitution of the "Taskforce on the Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya."[48] This task force prepared the Privacy and Data Protection Policy 2018[49] and the Data Protection Bill

46 Council of Europe. (2018, 2 October). Data Protection Unit provides support to the Kenyan authorities in drafting legislation on protection of privacy and personal data. https://www.coe.int/en/web/data-protection/-/data-protection-unit-provides-support-to-the-kenyan-authorities-in-drafting-legislation-on-protection-of-privacy-and-personal-data

47 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Reference, ETS No.108. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

48 The Kenya Gazette. (2018). *Gazette Notice No. 4367, Vol. CXX - No. 56.* http://kenyalaw.org/kenya_gazette/gazette/volume/MTcwNg--/Vol.CXX-No.56

49 Ministry of ICT. (2018). *Privacy and Data Protection Policy 2018*. http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf

# A BRIEF HISTORY OF
# DATA PROTECTION IN KENYA

**2007**

2007 elections and calls for **"the second liberation."**

**2009**

The **Data Protection Bill (2009**) is released by the ICT Ministry.

**2010**

Kenya promulgates the **2010 Constitution of Kenya**. Article 31 explicitly protects the right to privacy and data protection.

**2011**

The **Data Protection Bill, 2009** is received and considered by the Commission for the Implementation of the Constitution. Stakeholder consultations are held in 2012.

**2013**

The **Data Protection Bill, 2013** is released by the ICT Ministry.

**2016**

The **Access to Information Act, 2016** is enacted. Under section 21, CAJ possesses dual access to information and data protection powers.

**2018**

**Data Protection Taskforce** releases the Privacy and Data Protection Policy & the Data Protection Bill (2018). Public consultations are held.

**2018**

The **Data Protection Bill, 2018** is tabled before the Senate in May 2018.

**2019**

The **Data Protection Bill, 2019** is passed by the National Assembly, the President assents the Data Protection Act, 2019 on 8 November 2019 and takes effect on 26 November 2019.

(2018)[50] which were released for public commentary by the ICT Ministry in August 2018. Between 2018 and 2019, public consultation meetings were held and the Data Protection Policy and Bill, 2018 were forwarded to the cabinet for approval. This was obtained on 18 April 2019. The National Assembly received, deliberated on, and approved the Data Protection Bill, 2019, despite the existence of a similar legislative process before the senate.

## Implementation of the DPA, 2019: Extent and challenges

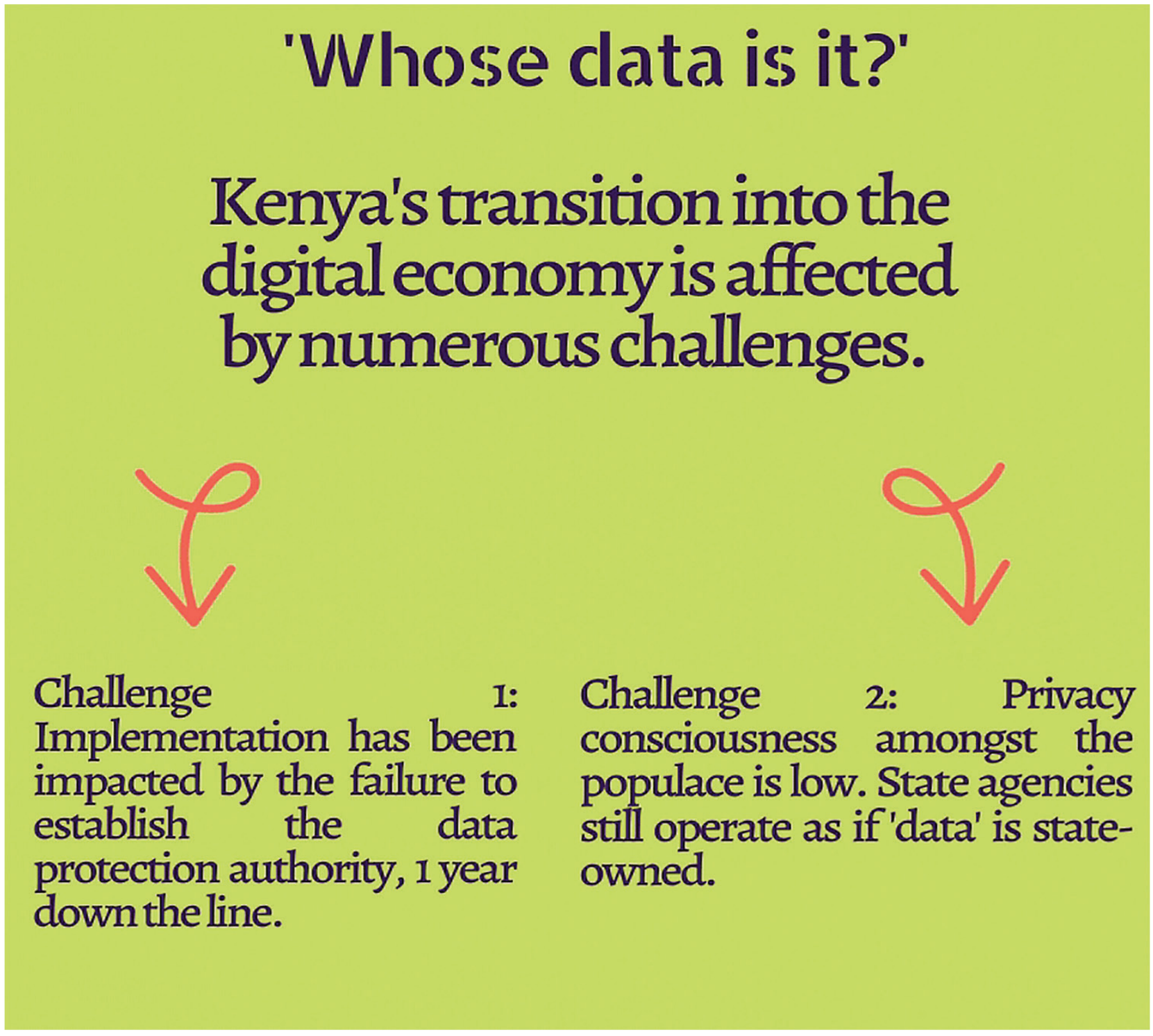
Despite the provisions of the DPA, coming into effect last year, differing opinions persist about the extent and sustainability of its implementation. On one hand, some stakeholders opine that the non-operationalisation of the office of the data protection commission (ODPC) and the attendant "institutional framework" envisaged under the DPA is synonymous with a framework which hasn't been implemented, nearly one month shy of the one-year mark. Drawing on this, some entities noted that they have neither conducted internal data protection impact assessments nor incorporated the DPA's provisions into their policies, structures, processes and general "way of doing things". As one private sector interviewee noted, the "instruments defined in the Act have yet not been put in place."

On the other hand, other stakeholders have been extremely vocal about its ongoing enforceability and implementation and the current enjoyment of rights by data subjects, irrespective of the delayed appointment of the data protection watchdog.[51] This is best evidenced by the petition against

50 Ministry of ICT. (2018). *The Data Protection Bill 2018*. http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf

51 Interview with Gloria Madegwa and Esban Muthoni, case officer and wellness officer at the Defenders Coalition, 12 October 2020.

Edgar Obare, who was charged in August using section 72 of the DPA.[52] As one private sector interviewee noted, they have already "reviewed their internal policies and updated the advice they provide to external parties", despite being bound by confidentiality rules in other legislative and sectoral frameworks.[53]




These divergent opinions on the implementation of the DPA are symptomatic of a deeper attitudinal challenge. While the digital ID conversation heightened county-based awareness about privacy and data protection rights, the COVID-19 pandemic demonstrated

52 The charge sheet read as follows: "On diverse dates between July 9 and July 13, 2020 at an unknown place, within the Republic of Kenya, using your social media accounts , domain name www.bnn.ke and verified Instagram account @edgarobare, unlawfully disclosed to your online followers personal data to wit visa belonging to one Natalie Wanjiru Githinji without her consent." Kimuyu, H. (2020, 3 August). Edgar Obare charged with publication of private data. *Nation.* https://nation.africa/kenya/news/edgar-obare-charged-with-publication-of-private-data-1912154

53 Interview with Mercy Mutemi, legal practitioner at Nzili & Sumbi Advocates, 12 October 2020.

that Kenyans are willing to temporarily shelve their rights[54] and refrain from questioning the wanting safeguards inherent in existing policy frameworks, including the national CCTV Policy.

While no "privacy consciousness" studies have been conducted in the Kenyan jurisdiction, the results of a 2020 Japanese study[55] offer crucial insights into the public awareness and civic education challenges – across different sectors and for different stakeholders – for the ODPC, once operationalised. As two interviewees noted, amongst the HRDs and journalist communities, "low knowledge levels" exist which may impact their work.[56]

These challenges are not merely restricted to the general public, but also private sector and state agency employees. While the former[57] have rolled out internal training and capacity-building initiatives for staff – including GDPR compliance – and are aware of the liability, customer loyalty and business profitability risks,[58] the latter are still driven by the mentality that individuals' personal data "belongs to them." Despite this daunting mentality challenge, the DPA, 2019, if properly implemented, will promote a sustainable paradigm shift,[59] where the balance of power between subjects and controllers/processors is redirected to the individual themselves.

---

54 This is often promoted in the name of grand ideals, namely public interest, public health, and national security, as evidenced by the unchecked roll-out of contact tracing applications by the government and private sector entities.

55 Tabata, N., & Sato, H., & Ninomiya, K. (2020). *Comparison of Privacy Consciousness Between Younger and Older Adults.* Wiley. https://onlinelibrary.wiley.com/doi/full/10.1111/jpr.12284

56 Interview with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

57 This includes ISPs, and entities in the medical, financial and retail sector. Interview with John Walubengo, 10 October 2020. Op. cit.

58 Interview with Ben Roberts, chief technology officer at Liquid Telecom, 9 October 2020. He further stated the need for the ISP sector to "really think about its shared systems and its cloud-based architecture." This was framed around sovereignty issues and the impact of this on client data.

59 Interview with John Walubengo, 10 October 2020. Op. cit.

Building on this, the ongoing compliance at the government level and its current privacy and data protection priorities have been narrowed down to the ongoing digital ID drive,[60] despite the recognition that the government is "not a monolith."

Secondly, there are concerns that the vague and loosely-worded language in the DPA, 2019 not only deviates dramatically from the GDPR (which it is largely modelled on), but also significantly waters down data subjects' rights, controllers/processor responsibilities, and introduces uncertainty into the Office of the Data Protection Commission's (ODPC) mandate. These challenges are core barriers for the proper implementation of the DPA, using the GDPR as a benchmark, and are extensively addressed below.

## Data Protection Act: Litigation

The DPA is currently being contested before the High Court of Kenya (Constitutional and Human Rights Division) by Okiya Omtatah. The constitutional petition, which was lodged on 14 November 2019, challenges the constitutional validity of the act as well as the validity of sections 5, 6, 51 (2)(b) and 54, DPA 2019. ARTICLE 19 Eastern Africa successfully intervened as an interested party, and raised additional issues about definitional discrepancies, the failure to balance the right to privacy with freedom of expression and media freedom under section 52, DPA, 2019 and excessively broad exemptions.[61] The petition will be mentioned on 15 December 2020.

60 Ibid.

61 ARTICLE 19. (2019, 25 November). Kenya: Protect the data protection framework. www.article19.org/resources/kenya-protect-the-data-protection-framework

## Key data protection issues in Kenya

Key data protection issues persist in Kenya, including issues which were commenced or flagged before the DPA was enacted, but whose determination will shape the trajectory of data protection and privacy in Kenya for years to come. This includes heightened digitisation drives at the state and non-state levels, including drives to roll out a smart city, digital identity drives, the draft CCTV policy,[62] as well as ongoing petitions affecting the right to privacy and data protection.

On the petition front, the High Court in the NIIMS petition issued two crucial orders. The first was the averment that the "collection of biometric (DNA and GPS) data for purposes of identification is intrusive and unnecessary, unconstitutional and a violation of Article 31, Constitution of Kenya, 2010, to the extent that it is not authorised and specifically anchored in empowering legislation."[63] Despite this, biometric (fingerprint) data collection and storage for authentication purposes by private entities, including banks, mobile network operators, health and insurance businesses, continues unabated.

Secondly, the court stalled the continued implementation of Kenya's digital identity system and the utilisation of the NIIMS data, subject to "an appropriate and comprehensive regulatory framework [...] first (being) enacted."[64] On 13 October 2020, the government gazetted the Huduma Namba regulations[65] which

62 Wanyama, J., & Sataar, J. (2019, 7 November). A Commentary on Kenya's Draft National CCTV Policy. *CIPIT*. https://cipit.strathmore.edu/a-commentary-on-kenyas-draft-national-cctv-policy; Amnesty Kenya. (2019, 14 August). Kenya: Desist from Indiscriminate and Invasive Mass Surveillance. https://www.amnestykenya.org/kenya-desist-from-indiscriminate-and-invasive-mass-surveillance/

63 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020]. Op. cit.

64 Ibid.

65 These include the Registration of Persons (National Integrated Identity Management System) Rules, 2020 and the Data Protection (Civil Registration) Regulations, 2020. Kenya Gazette Supplement No. 176 - Legal Notices No. 195 & 196. https://ict.go.ke; see also Mutua, J. (2020, 16 October). New regulations pave way for Huduma Namba cards. *Business Daily.* https://www.businessdailyafrica.com/bd/economy/new-regulations-pave-way-huduma-namba-cards-2482494

were heavily criticised by stakeholders. [66] Prior to this, the government announced a second round of "mass registration and the mass production of the Huduma Namba cards" following a "data clean up process and the creation of a data centre"[67] in September.

## Key features of the comprehensive data protection law

### Definitions

Key definitions have been provided under section 2 (interpretation) of the DPA, 2019 but several fundamental weaknesses have been noted. On one hand, it has been noted that the DPA's, 2019 definition of "personal data" is "inconsistent with the definition under the ATI Act, 2016."[68] This comment stems from the fact that the ATI Act, 2016 contains a more detailed definition compared to the constricted definition available under section 2 of the DPA, 2019.

It has also been noted that the definition of the term "sensitive personal data" omits key factors, including "membership of a trade union, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings."[69]

66 ARTICLE 19. (2020, 20 March). Kenya: Digital identity regulations must satisfy constitutional requirements. https://www.article19.org/resources/kenya-digital-identity-regulations-must-satisfy-constitutional-requirements

67 Tanui, C. (2020, 16 September). Huduma Namba e-cards production to begin in December: PS Kibicho. *Capital News*. https://www.capitalfm.co.ke/news/2020/09/huduma-namba-e-cards-production-to-begin-in-december-ps-kibicho

68 ARTICLE 19. (2019, 25 November). Op. cit.

69 Defenders Coalition, Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN), Dr. Robert Muthuri and Privacy International. (2020). *Analysis of Kenya's Data Protection Act, 2019*. https://privacyinternational.org/advocacy/3348/analysis-kenyas-data-protection-act-2019

## Data subject rights

The rights of data subjects are mainly provided under section 26, DPA 2019 (rights of a data subject). However, other rights which data subjects possess are scattered in other sections of the framework. These include: the right to data portability and the rights in relation to profiling and automated decision making under section 38 and section 35 of the DPA, 2019 respectively. It has been noted that other rights to guarantee empowerment of data subjects need to be included in the DPA, including an explicit "right to an effective remedy", and a "right to compensation and liability."[70]

## Purpose limitations

The principles guiding personal data processing are explicitly set out under section 25 (principles of data protection) which provides that personal data can only be collected for "explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes." This purpose limitation is present throughout the DPA, including section 30 (lawful processing of personal data); section 31 (data protection impact assessment); section 37 (commercial use of data); and section 39 (limitation to retention of personal data), amongst others.

## Conditions for lawful processing

The conditions for lawful processing are provided under section 30, DPA, 2019. The conditions required prior to processing include prior consent from the data subject to the "processing for one or

70 Ibid.

more specified purposes." Other scenarios are provided where lawful processing may be permitted.[71]

## Relevant exemptions in the public interest

The exemptions applicable under the DPA, 2019 are located under Part VII – Exemptions, and other sections interspersed throughout the framework, including section 30 (1) (b)(iv) and (vi), section 52, amongst other sections.

Specifically, these wide and blanket exemptions are present throughout the whole DPA, 2019, including under section 51 (2) (b), which contentiously exempts the processing of personal data where this is necessary for "national security or public interest". As one interviewee noted, the "government always has a caveat in all laws."[72] Notably, these terms are not defined in the act and risk being abused by state agencies and/or private agencies working conjunctively with the state on public affairs.

This exemption is currently being contested in the data protection constitutional petition, which notes that this provision conflicts with Article 59 (2)(d), Constitution of Kenya, 2010.

Conversely, ARTICLE 19 EA noted that the "journalistic exemption" located under sections 30, 39 and 51, DPA, 2019 inadequately protects the right to free expression. It was noted that this exemption is limited to the processing of personal data and

71 Section 30 (1)(b), DPA, 2019: where the processing is necessary for "for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; for compliance with any legal obligation to which the controller is subject; in order to protect the vital interests of the data subject or another natural person; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; the performance of any task carried out by a public authority; for the exercise, by any person in the public interest, of any other functions of a public nature; for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or for the purpose of historical, statistical, journalistic, literature and art or scientific research."

72 Interview with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

retention provisions, but not to other crucial aspects, including the "requirements of registration of data processing, the processing of sensitive data, the limits on the transfer of personal data outside Kenya and the application of criminal offences."[73] This exposes journalists to serious consequences, including the risk of criminal penalties for articles published in good faith.

## Breach notification requirements

The notification and communication of breach requirements are set out under section 43, DPA, 2019. This section inserts a worryingly low notification threshold, when there is "real risk of harm to the data subject." A joint analysis revealed that this threshold is vague and no criteria of risk and likelihood is provided in the section. This vagueness can constitute a loophole for data controllers who hide behind subjective determinations of risk.[74]

## Cross-border data transfers

The transfer of personal data outside Kenya is provided under Part VI of the DPA, 2019. Section 48 provides for the "conditions for transfer out of Kenya", Section 49 provides for "safeguards prior to transfer of personal data out of Kenya" and Section 50 provides for the contentious data localisation requirement, or "processing through a data server or data centre in Kenya". Notably, Regulation 38 of the Data Protection (Civil Registration) Regulations, 2020 provides that civil registration entities "shall not transfer personal data collected for civil registration purposes outside of Kenya, except with the written approval of the Data Commissioner."

73 ARTICLE 19. (2019, 25 November). Op. cit.

74 Defenders Coalition, Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN), Dr. Robert Muthuri and Privacy International. (2020). Op. cit.

It is crucial to note that interviewees maintained that the Taskforce Bill (2018) – which relied on the GDPR as the reference document – did not contain the "data localisation" provision under section 50, DPA, 2019. It is unclear whether this was introduced during the cabinet approval stage, and therefore not subjected to public participation, or during the deliberations of the National Assembly, where the committee and the house possess ultimate decision-making powers, irrespective of the public's sentiments.

## Other relevant features

Other features have drawn the attention and concern of stakeholders. These include the penalties for breach under section 63, DPA, 2019 (administrative fines), and the use of loose language which will have an impact on data subjects' rights and controllers' or processor responsibilities.

The former provision curiously states that the data commissioner can impose a maximum penalty of "up to five million shillings (approximately USD 50,000), or in the case of an undertaking, up to one per cent of its annual turnover of the preceding financial year, whichever is lower." This poorly-phrased section may permit entities with parent-subsidiary arrangements to negotiate the amount of fines they will pay, which fails to promote their use as a redress mechanism for data subjects.

The use of the word "may" also waters down significant protections in the DPA, 2019. For example, under section 24 (designation of the data protection officer), data controllers and processors have the option to appoint a data protection officer, as opposed to the mandatory appointment envisaged under Article 37 of the GDPR. This is an issue because the DPA, 2019 is supposed to be compliant with international standards.

In preparing this report, responses from interviewees about the financial, regulatory and compliance costs of adhering to rights-frameworks, including the DPA, 2019 were sought. While most interviewees noted that the failure to implement the DPA in a staggered manner[75] for entities with different capabilities may impose a disproportionate burden on all entities, especially micro, small, or medium enterprises, compared to their larger private counterparts, it was also affirmed that one should refrain from "putting a cost on human rights, given Kenya's fledgling entry into the digital economy."[76]

Lastly, it was noted that, in the COVID-19 context, numerous entities have had to shift their way of doing things, including upgrading from paper-based to cloud-based services.[77] This latter point magnified that rights protections and their attendant costs will always be equalised by the free market.[78]

## Data protection authority (DPA) or other institutions assigned with the responsibility to oversee rights to personal data protection

### Establishment and composition of the DPA and other institutions

The ODPC, which is constituted as a state office rather than a constitutional commission, is established under Part II — Establishment of the Office of Data Protection Commissioner. This office is steered by the data commissioner, and other supporting staff appointed by the data commissioner. The

75 Interview with Grace Mutung'u, 12 October 2020. Op. cit.

76 Ibid.

77 Interview with Ben Roberts, 9 October 2020. Op. cit.

78 Interview with John Walubengo, 10 October 2020. Op. cit.

commissioner is expected to establish relevant directorates, in conjunction with the cabinet secretary (section 5, DPA, 2019).

The recruitment of the data commissioner is initiated by the Public Service Commission, which puts out the call for recruitment and shortlists "three qualified applicants in the order of merit for the position of Data Commissioner" for presidential nomination, subject to the approval of the national assembly (section 6, DPA, 2019). The qualifications required for the data commissioner are elucidated under section 7, DPA, 2019 and unlike other jurisdictions, the commissioner will serve for a "single term of six years" without the possibility of reappointment.

On 14 April 2020, the Public Service Commission issued a public notice for the position[79] and subsequently shortlisted 10 candidates for the position in July 2020. This process was halted by the Employment and Labour Relations Court in July following a petition lodged by Adrian Kamotho. The petitioner contested, among other issues, the time taken by commission (two months) to conclude the recruitment process, in contravention of the 21-day statutory period provided under section 6 (3), DPA, 2019. Reports indicate that petitioner and the commission filed a consent before the court, and the commission "agreed to start the process afresh 'in accordance with the law.'"[80] This fresh recruitment process resulted in 12 candidates being shortlisted.[81]

On 13 October 2020, reports emerged that Immaculate Kassait had been nominated by the President of Kenya for the position of data commissioner, pending the approval of the national

79 https://www.careerpointkenya.co.ke/2020/03/data-commissioner-psc

80 Kiplagat, S**.** (2020, 28 July). PSC back to drawing board on Data Commissioner recruitment. *Business Daily*. https://www.businessdailyafrica.com/bd/economy/psc-back-to-drawing-board-on-data-commissioner-recruitment-2297110

81 Otieno, B. (2020, 15 September). SC shortlists 12 candidates for data commissioner post. *Business Daily*. https://www.businessdailyafrica.com/bd/news/psc-shortlists-12-candidates-for-data-commissioner-post-2301252

assembly's Departmental Committee on Communication, Information and Innovation.[82] It is unclear who the other two shortlisted candidates were. Finally, it is unclear how the High Court will determine the grounds raised in the data protection petition, which raises issues about the recruitment process.

## Mandate of the DPA/other institutions

Under section 8, DPA, 2019 (functions of the Office), the ODPC is tasked with "increasing legal certainty"[83] by overseeing the general implementation of the DPA, exercising oversight over data controllers and processes via registration, investigating complaints of privacy and data protection infringements, public education and awareness, promoting international cooperation in matters, and undertaking research on data developments, amongst others. Under section 9, DPA 2019 (powers of the office), the ODPC possesses regulatory, investigative, dispute-resolution, inspection, audit and sanction powers, amongst others.

## Effectiveness and challenges of the DPA/other institutions

The ODPC – once operationalised – will face pre-existing challenges which will drastically affect its effectiveness, and limit its ability to work independently.

The first challenge of the ODPC's office is its lack of independence and its situatedness as a state office under the ICT Ministry, which is itself a state agency and a data controller/processor. While some interviewees noted the need to recall practical realities within the Kenyan jurisdiction, including the

82 https://www.youtube.com/watch?v=kFgmxsvG2qs

83 Internet Society & Commission of the African Union. (2018). *Personal Data Protection Guidelines for Africa.* https://www.internet-society.org/resources/doc/2018/personal-data-protection-guidelines-for-africa

## Kenya's Data Commissioner

**General function under section 8, DPA, 2019:**

- Oversee the implementation of and be responsible for the enforcement of this Act.

**General powers under section 9, DPA, 2019:**

- Regulatory, investigative, dispute-resolution, inspection and audit, and sanctions powers.

**Challenges and Risks:**

- The Commissioner faces pre-existing restrictions, including power-sharing with the Cabinet Secretary, ICT Ministry. This will drastically affect its effectiveness and limit its ability to work independently.
- This risks affecting Kenya's nascent privacy and data protection practice, and consequently, the rights of Kenya's 47.6 million data subjects.

fears of a constitutional commission being subjected to arbitrary budgetary cuts in a similar manner to constitutional commissions (i.e. KNCHR and CAJ) and parastatals which may interfere with the governments operations, it is concerning that these realities took precedence over the full protection and promotion of the right to privacy and data protection in Kenya.

Secondly, as noted above, the ODPC faces the challenge of combating attitudinal problems within the government itself, which still possess copious privileges in the data collection, processing and storage arena.[84]

Thirdly, interviewees queried the ability of the ODPC to effectively deal with an anticipated case-load challenge in a timely manner, including complaints, which will likely be placed before it.[85]

84 Interviews with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

85 Ibid. This query, prior to the establishment of the ODPC, led to a pertinent statement about the "type of measures which can be created before the Commissioner takes office."

Fourthly, Section 8 (1)(d), DPA 2019 promotes self-regulation among data controllers and data processors. This provision risks eroding the protections contained in the DPA, given the failure to specify instances where self-regulation is permitted, for what types of controllers and processors, and the safeguards which will be implemented to prevent abuses. It is also unclear how this self-regulation will be aligned with the codes and guidelines which the ODPC must issue under section 74, DPA, 2019.

Lastly, it is unclear why the cabinet secretary, ICT Ministry possesses wide powers under the DPA and the justification for this. However, it is certain that this risks disempowering the ODPC and may permit the ICT Ministry to interfere in the functions of the ODPC, without the need for prior consultation.

This is evidenced by the following provisions; section 35, DPA, 2019 (automated individual decision making) empowers the cabinet secretary, rather than the ODPC, to "make such further provision to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of decisions based solely on automated processing." Section 37, DPA, 2019 (commercial use of data) empowers the cabinet secretary, in consultation with the commissioner, to "prescribe practice guidelines for commercial use of personal data in accordance with this Act." Section 50, DPA, 2019 (processing through a data server or data centre in Kenya) grants the cabinet secretary *exclusive* powers to "prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya."

## Data protection practices in internet country code top level domain name (ccTLD) registration

Kenya's .ke ccTLD (domain) registration services are "administered by KENIC" and the communications authority of Kenya acts as the "trustee [...] on behalf of the Government of Kenya".[86]

KENIC has an interactive WHOIS search query webpage permitting access to domain, contact, host and registrar information.[87] Further, KENIC's .ke Domain Name WHOIS Policy stipulates that the registry is permitted to publish certain personal data, including: "name, address and telephone and fax number of the Registrant; technical contact person; email address of Registrant; technical data (such as status of the Domain Name or the name servers)."[88] The policy further asserts that the contact information for private individuals is "restricted to the email address, unless they request otherwise."[89] Individual registrants are explicitly informed about the ability to "create and use a specific functional email address for publication in the WHOIS as an alternative to the use of their personal email address."[90]

The policy also specifies that it will only transfer personal data to third parties where it is "ordered to do so by a public authority, carrying out its legitimate tasks."[91] Third parties are required to fill in an application form and provide supporting information, as well as agree to certain disclaimers.

86 https://ca.go.ke/industry/e-commerce-development/domain-name-system

87 https://whois.kenic.or.ke/whois.jsp

88 https://kenic.or.ke/policies

89 Ibid.

90 Ibid.

91 Ibid.

Lastly, KENIC provides third parties with access to personal data, where it has been ordered to do so by a "judicial authority in Kenya". It is unclear whether KENIC has dealt with such requests, including from law-enforcement agencies, whether court-sanctioned warrants were produced beforehand, and whether it publicly discloses this practice on its website. An email request for information was submitted to KENIC on 9 October 2020, but no response had been received as at 19 October 2020.

## Analysis in line with AfDec and other relevant instruments

Kenya's DPA, 2019 is a representation of the tireless efforts by numerous internal and external stakeholders. Despite this, the legislative framework lacks full informational privacy protections, as evidenced by the extensive loopholes documented above. This is also informed by the fact that the DPA does not conform with international and regional best practices and standards, including those on protection and privacy.[92]

Notably, Principle 8 of the AfDec mandates that the right to personal data protection must be provided for *all* stakeholders. Despite this, Kenya's DPA, 2019 falls below this standard by failing to provide adequate protections for children. Secondly, the right to communicate anonymously on the internet and using digital technologies is not fully guaranteed, given the existence of competing legislation which waters down this right. Thirdly, the DPA, 2019 fails to meet the three-part test and includes broad, vague and ill-defined restrictions on personal data protections which are inconsistent with these permissible restrictions.

92 Interview with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

Fourthly, the DPA, 2019 fails to comply with other regional guidance, including the AU Convention, the Personal Data Protection Guidelines for Africa and the ACHPR Declaration. Despite Kenya not being bound by these three documents, all of them emphasise the need for an independent data protection authority as a "vital element of the legal and institutional framework for building trust online."[93] As noted above, Kenya falls far below this standard.

Crucially, Kenya supported recommendations to "revise and enact the draft data protection bill and create a data protection framework in line with international standards on the right to privacy,"[94] despite the enactment of the DPA, 2019. This is a crucial recognition by the state that its current framework is not on a par with these regional and international commitments, which was echoed in CSO reports.

Lastly, despite Kenya's DPA being modelled on the GDPR, Kenya has not taken further measures to address the inconsistencies noted above by aligning and updating the framework.

## Analysis of the status of a human rights-based approach to personal data protection in the country

The draft "Privacy and Personal Data Protection in Africa – Advocacy Toolkit" magnifies the utility of the human rights-based approach, and notes that this helps "policy makers perform better at meeting their human rights obligations, and have better outcomes that benefit rights-holders."[95] This

93 Internet Society & Commission of the African Union. (2018). Op.cit.

94 "142.28 Revise and enact the draft data protection bill and create a data protection framework in line with international standards on the right to privacy (Estonia); 142.176 Ensure that surveillance and profiling of citizens respect the right to privacy, including judicial oversight (Germany)". UNHRC. (2020). *National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21 - Kenya*. https://undocs.org/A/HRC/WG.6/35/KEN/1

95 https://africaninternetrights.org

approach is underpinned by the "PANEL" principles (participation, accountability, non-discrimination and equality, empowerment, legality),[96] which will be explored below.

Despite Kenya's 12-year-old informational privacy journey, the five principles were not uniformly applied during the various open and closed deliberation processes.

## Participation and non-discrimination and equality

On the participation front, the formation of the task force commendably opened up processes permitting more individuals and organisations to actively take part in the public participation processes. However, the selection criteria used to identify the members of this task force remains unknown. Secondly, the continued failure to enact the draft Public Participation Bill (2019)[97] means that public consultation hearings giving effect to public participation provisions in the Constitution of Kenya, 2010, left out various stakeholders. This included persons with disabilities, children and the elderly, amongst others, whose voices were glaringly absent from the data protection process between 2007 and 2019.

Commendably, the National Assembly process prioritised public *county* meetings, which encouraged a shift towards a more holistic, nation-based rather than Nairobi-based, approach to data protection and privacy in Kenya. This helped shatter the existence of geographical barriers, and the exclusion of individuals on this basis, in ICT policy processes in Kenya.

96 http://ennhri.org/about-nhris/human-rights-based-approach

97 http://kenyalaw.org/kl/index.php?id=9091

## Accountability

Under the “accountability” umbrella, the lack of appropriate mechanisms capable of holding duty bearers to account for this failure to include all voices as mandated under the Constitution of Kenya, 2010, resulted in individuals turning to the courts. Kenya’s judicial process is not only expensive, and time-consuming, but also adversarial. These factors reveal the need to enact out-of-court redress and accountability mechanisms, during bill formation processes, given the inadequacy of existing mechanisms.

Secondly, as magnified above, Kenya does not mandate data controllers and processors to appoint data protection officers capable of promoting institutional compliance, at the state and private entity levels.

## Empowerment

Empowerment is synonymous with an individual’s ability to *know* and to *choose*. As noted above, one of the core implementation challenges awaiting the ODPC is the pressing lack of “privacy consciousness”. This will require the office to actively and deliberately tailor specific education and awareness-raising campaigns, across the country, which must be available in both official languages in Kenya, Kiswahili and English. This, as noted in the draft toolkit, will provide a threshold against which to measure the “effectiveness (i.e. use) of the law”.

Secondly, easily accessible platforms must be available to individuals permitting them to exercise their data rights, which requires on-the-ground harmonisation and interoperability of systems and processes.

## Legality

The challenges of the legality of the DPA, 2019 have been enumerated extensively above. These legality challenges, which are being contested before the High Court, will have an impact on the viability and effectiveness of the DPA, including for future generations.

## Concluding observations and recommendations

The documented information reveals that Kenya's DPA, 2019, whilst a step in the right direction for informational privacy, leaves a lot to be desired. Despite the Kenyan government affirming the existence of gaps in the draft Data Protection Bill, during its UPR review, it still failed to enact a framework "in line with international standards on the right to privacy".[98] Kenya's framework does not offer data subjects the panacea and liberation proponents sought, given the existence of internal and external inconsistencies, including on issues which are central to its practical and sustainable implementation and competing legislation.

As noted above, the various open and closed processes – from 2007 to 2019 – which led to the enactment of the DPA, 2019 were marked with notable successes and failures which impacted Kenya's "PANEL" assessment. On one hand, positive efforts were made to shatter the Nairobi-centric nature of the data protection conversations during the 2019 National Assembly deliberations, and to solicit the input of vast stakeholders during the 2018 taskforce deliberations. However, the inability to promote participation by *all* rather than *aware* stakeholders affects the conclusion that Kenya's DPA, 2019 offers data protection "for *all* stakeholders" (Principle 8 of the AfDec). Further, the existence of

98 UNHCR. (2020). Op. cit.

a constitutional petition casts a still undetermined shadow on the constitutionality of the DPA, 2019.

Lastly, Kenya's ODPC faces the challenge of rousing "privacy consciousness" amongst rights holders and duty bearers in the Kenyan jurisdiction. Where this is collaboratively pursued, an accountable, participatory and trust-laden transition into the digital economy may be possible.

## Recommendations: Strengthening the privacy and data protection framework and application of the human rights-based approach.

To the government:

- Commence a stock-taking review of the DPA, 2019 to assess what progress and challenges exist in the Kenyan jurisdiction, nearly a month to the one-year mark.
- Urgently commence sensitisation and public-awareness training and capacity-building sessions to combat state agencies' perceptions (individual and organisation level) about the ownership status of personal data.
- Actively promote the inclusion of excluded stakeholders to ensure a deeper, and wider level of participation.

To civil society organisations and academia:

- Continue advocating for the sealing of loopholes and inconsistent provisions in the DPA, 2019, including before national, regional and international judicial fora.
- Continue monitoring ongoing behaviour by data controllers and processors in Kenya and utilise right-to-information requests to solicit information from state and non-state actors.

- Continue documenting data protection and privacy successes and challenges in shadow reports, including before the UNHRC (ICCPR state review), the OHCHR (UPR) and the ACHPR (observer status reporting mechanism), amongst others.

To the private sector (ISPs and MNOs):

- Internalise DPA, 2019 responsibilities and take initiatives to ensure compliance, irrespective of the non-operationalisation of the ODPC.
- Commence user and client sensitisation about updated privacy policies.
- Promptly inform users and clients – using online and offline platforms – about  the occurrence of data breaches.

To the technical community:

- Publicly disclose the number of WHOIS law enforcement requests and their resolution.
- Implement the data protection by design and default provisions into internet and technology infrastructural systems and processes.

# Namibia

**Pria Chetty and Alon Alkalay**[1]
EndCode

## Executive summary

Namibia recognises the right to privacy as a fundamental human right under Article 13 of the Namibian Constitution. The Information Technology Policy of Namibia, 2008 undertakes to develop legislation that addresses information security, data protection and the protection of privacy. Furthermore, the policy emphasises that in order to ensure that the interface between information security and rights to privacy are well regulated, the protection of data, information security and lawful interception should comply with international standards.

Between 24 and 26 February 2020, the Council of Europe along with the Commonwealth Secretariat held a data protection legislation drafting workshop in the capital city of Windhoek.[2]

1 The authors are grateful to national respondents and experts in Namibia for their time and involvement, with special thanks to the team at EndCode, particularly Daniel Batty.

2 Council of Europe. (2020, 26 February). GLACY+: Stakeholders' Consultation Workshop on the Data Protection Bill in Namibia. https://www.coe.int/en/web/cybercrime/-/glacy-stakeholders-consultation-workshop-on-the-data-protection-bill-in-namibia

The resulting Data Protection Bill proposes the establishment of a data protection authority and seeks to create provisions for the use, processing and collection of personal information in order to protect citizens' right to privacy. In March 2020, the Council of Europe and the Commonwealth Secretariat, jointly with the Ministry of Communication, held a consultative workshop with stakeholders on proposed data protection legislation. The workshop participants examined the key provisions of the General Data Protection Regulation (GDPR), the Southern African Development Community (SADC) Data Protection Model Law, the African Union Convention on Cyber Security and Data Protection and the Council of Europe's Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data. This workshop has been succeeded by a series of stakeholder consultations with a view to present a draft bill to the Namibian Cabinet in 2021.

This report is timely. It draws comparisons between the Namibian Data Protection Bill, 2020 and regional and international instruments influencing data protection regulation in Africa and globally. In particular, and unique to the scope of this study, the report examines the Namibian Data Protection Bill in the context of human rights-based approaches to data protection. Secondly, the report collects views and perspectives from national stakeholders that were interviewed on the key considerations for Namibian data protection regulation. In the context of this study, constraints and threats to privacy and personal data protection were collected.

The report concludes that the Namibia Data Protection Bill is a positive step toward realising data protection rights for Namibians and conferring obligations to safeguard Namibian citizens' personal data. The proposed establishment of a Data

Protection Authority and the identification of powers to receive and investigate complaints is welcomed furthermore as a positive step to the realisation of rights of privacy and privacy online. Effective and broad stakeholder consultation is, however, crucial to ensuring that the bill is responsive to the constraints and barriers identified by respondents to data protection regulation and to ensure that Namibia adequately aligns with regional and international instruments governing data protection to which the country is bound. The draft Namibia Data Protection Bill is commendable for the public interest exceptions provisioned and the extent to which it meets emerging standards for human rights-based policy setting.

Ultimately, however, Namibia's data protection law must be passed, must be operationalised and must be effectively governed to offer the assurance of privacy redress for Namibian citizens.

This report is one in a series of country studies carried out for the African Declaration on Internet Rights and Freedoms (AfDec) Coalition that aim to increase the understanding of the importance of a rights-based approach to data protection and privacy among national and regional human rights institutions establishing regulation amongst institutions in this area. The report also aims to increase the understanding of the importance of a rights-based approach to data protection among duty bearers and rights holders. It is hoped that this report will inform and strengthen national policy making and legislative processes, regional and policy debates and advocacy initiatives in the region and promote the idea of using human rights-based approaches in internet-related policy and regulation.

## Methodology

This research has been undertaken to determine and understand the state of data protection in Namibia and to provide an understanding of the barriers that have to be overcome in order to develop and adopt a data protection framework in the country. The research culminates in an analysis of the extent to which the personal data protection and privacy framework in Namibia (the proposed Namibian Data Protection Bill), applies a human rights-based approach.

The majority of the content in this report was compiled through desktop research and informed by stakeholder interviews. Sources consulted include primary, secondary and tertiary sources.

A total of five interviews were conducted covering a full range of relevant data protection stakeholder categories including, government, civil society, media, academia and private sector.

Interview respondents' submissions have been kept anonymous and are referenced in this report as follows:

- First respondent: Data protection expert and private sector stakeholder
- Second respondent: Research associate and public policy advocate
- Third respondent: Government official
- Fourth respondent: Data protection expert and academic
- Fifth respondent: Journalist, researcher and civil society advocate.

## Country context

Namibia is a former German colony that was administered by South Africa after the defeat of the German empire at the end of World War I.[3] For the period from 1910 to 1990 Namibia was subjected to South African law which included the racial policies of apartheid.

On 21 March 1990 Namibia gained independence.[4]

When Namibia attained independence from South Africa in 1990 the country adopted the constitution which was developed to reflect a pro-democracy, human rights agenda that dominated at the time.

Article 1(1) of the constitution states:

> The Republic of Namibia is hereby established as a sovereign, secular, democratic and unitary State founded upon the principles of democracy, the rule of law and justice for all.[5]

Article 1(2) further states:

> All power shall vest in the people of Namibia who shall exercise their sovereignty through the democratic institutions of the State.

Chapter 3 of the constitution, entitled Fundamental Human Rights and Freedoms, is referred to as the Bill of Rights and outlines the human rights of all Namibian citizens.

3 https://www.britannica.com/place/Namibia/History#ref44015

4 https://www.sahistory.org.za/place/namibia

5 Constitution of the Republic of Namibia, 1990.

Namibia is governed by the SWAPO (South West Africa People's Organisation) Party, a former independence movement which gets its name from a time when Namibia was referred to as South West Africa.[6] The SWAPO party continues to rule Namibia following the recent 2019 general elections which saw President Hage Geingob elected with a 56.3% majority vote.[7] Today, Namibia has a small population relative to its geographical size, with a total population of 2,630,073 people.[8] The Namibian economy is largely dominated by raw mineral resource extraction with mining contributing 12.5% of the Namibian GDP,[9] and 50% of the foreign exchange earnings.[10]

## Namibia's standing on internet-related human rights

Namibia has a national internet governance forum, NamIGF, which seeks to raise awareness about internet governance issues as well as influence the public policy making process concerning the internet and more broadly information and communications technology (ICT) in general.[11]

The Ministry of Information and Communications Technology (MICT) is the primary government institution responsible for promoting the use and effective regulation of ICT services in Namibia.[12] While the ministry does not give express acknowledgement to all internet-related human rights, a stated strategic objective is to "Enhance unhindered access

6 https://www.sahistory.org.za/article/south-west-africa-peoples-organisation-swapo

7 Electoral Commission of Namibia. (2019). Presidential Election Final Results. https://www.ecn.na/wp-content/uploads/2019/12/NA-ELE-RESULTS-UPDATE-2019.pdf

8 https://www.cia.gov/the-world-factbook/countries/namibia/#people-and-society

9 https://www.cia.gov/the-world-factbook/countries/namibia/#economy

10 https://www.heritage.org/index/country/namibia

11 https://namibia.intgovforum.org/content/namibia-igf-home

12 https://mict.gov.na

to information for an informed nation".[13] At the inaugural 2017 Namibian IGF, themed: "Shape Your Digital Future", Minister of Information and Communication Technology, Tjekero Tweya, highlighted that Namibia endeavoured to achieve a knowledge-based economy through its Vision 2030. To this end, the minister pointed to various legal reform initiatives with the aim of establishing appropriate legal frameworks for achieving the country's digital goals and the country's initiatives to increase citizens' access to the internet.

The Parliamentary Standing Committee on Information, Communication, Technology and Innovation acts as an oversight body to ensure that the MICT, among other ministries, is achieving its mandate. Additionally the committee advises parliament on new legislation and policies that should be adopted to further ICT development in Namibia.[14]

Namibia has committed to recognising privacy as a fundamental human right in both national frameworks such as the constitution and international commitments such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights.[15] Notwithstanding such commitments, Namibia has not effected data protection legislation. In 2013 the International Telecommunications Union (ITU) assisted in the development of a Data Protection Bill and Data Protection Policy, however neither of these documents have been subject to amendments or updated since the initial draft.[16]

13 https://mict.gov.na/strategic-plan

14 https://www.parliament.na/index.php/committee-on-information-and-communication-technology-na

15 Council of Europe. (2020, 16 March). GLACY+: Situation report on the current state of legislation in Namibia on data protection and related recommendations.

16 Ibid.

In 2018, the Namibian Media Trust (NMT), a civil society organisation in Namibia involved in promoting media freedom and related issues as well as the regulation of the media (print, broadcast and online) in line with international best practice, made submissions[17] on the proposed Review and Amendment of Information and Communication Technologies (ICT) Policies and the Communications Act (collectively, the ICT Review) that was undertaken by an ITU expert on instruction of the Government of Namibia, more specifically, the MICT. The submission called for an approach to ICT policy and legislative reforms that reflects a commitment to: upholding the Constitution of Namibia, meeting Namibia's human rights obligations under international law, including with respect to its obligations as a member of the United Nations (UN) and of the African Union (AU) and providing its people with policies and laws that meet the highest international best practice standards "as a mark of respect for the inherent dignity of every Namibian." In the submission, NMT notes that Namibia does not have "personal data protection policies let alone enacted statutes" and advocates for a rights-based approach to internet regulation, relevant to both freedom of expression as well as the right to access information.

Article 21(1)(a) of the Constitution of Namibia guarantees "freedom of speech and expression, which shall include freedom of the press and other media." Further, under Article 144 of the constitution, Namibia is bound to a number of international human rights instruments that endorse access to information as a fundamental human right. These include the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (ACHPR). Namibia is, however, prejudiced by the failure to pass or implement

17 https://www.nmt.africa/uploads/5be58699f3d58/NMTSubmission-2018ICTReview.pdf

laws advancing access to information and media freedom. Namibia's Access to Information Bill has finally been tabled in parliament after years of lobbying the Namibian government. The Whistleblower Protection and Witness Protections Acts of 2017 have not been implemented.

Digital rights and online protection for women in particular are in a parlous state as the lack of regulation means that online harassment and the non-consensual sharing of images has gone unpunished. The 2020 Women's Rights Online Report Card for Namibia[18] requests that legislation be passed to protect personal data and information online while it also notes that the criminal justice system (in the form of the police and judiciary) requires capacity-building to address online gender-based violence. That the report notes that online harassment has gone unpunished and the request that the police and the judiciary receive training, is also an indication that the Namibian legal system has struggled to grapple with privacy issues.

## Constitutional underpinning and case law

Namibia recognises the right to privacy as a fundamental human right under Article 13 of the Namibian Constitution:

Article 13(1) states:

> No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of

18 Internet Society Namibia Chapter. (2020). *Womens' Rights Online Report Card: Namibia.* https://webfoundation.org/docs/2020/08/GenderReport-Namibia.pdf

> health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.

Article 13(2) states:

> Searches of the person or the homes of individuals shall only be justified: (a) where these are authorised by a competent judicial officer; (b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.

Article 144 of the constitution provides that unless otherwise provided for in the constitution or another act, the general rules of international public law and international agreements binding on Namibia shall form part of Namibian law.

An examination of the available case law indicates that privacy has been a factor in certain cases. The courts have confirmed a right to privacy of communications whilst rendering it subordinate to the ends of achieving justice, established a test for intent to establish liability for a violation of privacy and in an anti-corruption case, upheld the right to privacy to render certain records inadmissible.

| Citation | Case description | Aspects relative to privacy |
|---|---|---|
| **Nghimwena v Government of the Republic of Namibia** | The appellant brought an action in the High Court in which she claimed from the government, the respondent in this matter, damages in the amount of NAD 200,000 (USD 123,22) for alleged unlawful arrest and detention and a sum of NAD 500,000 (USD 32,453) for alleged assault and torture. | Despite confirming the constitutional right to privacy:<br>"Every citizen has a fundamental right to privacy of communications, inter alia, by virtue of the Namibian Constitution."<br>"The principle in our Courts and under The Namibian Constitution is that the right to privacy is fundamentally enshrined."<br>The court nonetheless rejected the plaintiff's claim and held that the breach of her right to privacy "pales into insignificance as against the goal of achieving justice." |
| **Erica Beukes and another v Daniël Petrus Botha and 3 Others** | Multiple causes of action including defamation and a violation of privacy following assertions made by trustees to donors of the trust that a fellow trustee has misappropriated funds. The trustee so accused was dismissed and the remaining trustees issued a statement to donors confirming the dismissal and raising the grounds of fraud and incompetence. The dismissed trustee filed a case against the remaining trustees. | The court held that the claim of a violation of privacy should fail on procedural grounds as the plaintiff failed to avert all the elements necessary for the claim. In this regard the court laid down a test for the violation of privacy as follows:<br>"Apart from the wrongfulness of the infringement of privacy, intent is also required before liability can be established."<br>"This means that the perpetrator must have directed his will to violating the privacy of the prejudiced party, knowing that such violation would be wrongful."<br>Without these elements intent cannot be found and therefore neither can the claim for a violation of privacy. |
| **S V Lameck And Others** | This case is a matter of a trial within a trial where the primary trial involves an investigation by the anti-corruption commission and the secondary case involved an assessment of evidence in the primary case relating to bank account information obtained directly from the accused's bank. The accused alleged that such actions were in violation of his right to privacy. | The court upheld the view that the right to privacy is not absolute and can be limited by the provisions of another act, including the Anti-Corruption Act.<br>However, "any such limitation must be interpreted in such a way that it least impinges on the rights and values of a person."<br>The court found that the procedural elements in the Anti-Corruption Act for the procurement of evidence had not been adequately followed and accordingly the right to privacy had not been justifiably limited, therefore the evidence had been unjustifiably obtained and was inadmissible in the primary case. |

In the area of online digital rights (of which privacy and data protection is an important component) there is a dearth of case law. In the absence of clear jurisprudence or digital rights litigation pertaining to privacy rights, it is difficult to anticipate the

courts' approach where data protection violations occur. Without case law, it is also challenging to imagine that a litigant might rely on Namibia's international obligations where their privacy or personal data is compromised.

## Regional and international commitments

### International Covenant on Civil and Political Rights

Namibia became a signatory to the International Covenant on Civil and Political Rights (ICCPR) in November 1994. Article 17 provides that no person should be subjected to the arbitrary or unlawful interference with his privacy, family, home or correspondence. In addition, Article 17(2) provides that everyone is entitled to legal protection against the infringement of the right to privacy.

### Harmonisation of the ICT Policies in Sub-Saharan Africa

In 2013, as part of the ITU Harmonisation of the ICT Policies in Sub-Saharan Africa (HIPSSA) initiative, the ITU engaged the Namibian government to assist the nation in drafting a data protection policy and data protection legislation with the objective being the eventual passing of dedicated data protection legislation. The policy has not been available for public consultation, according to respondents, and the draft legislation arising from the HIPSSA initiative, is obsolete (considering it has not been revisited in several years).

### African Union Convention on Cyber Security and Personal Data Protection

Namibia ratified the African Union Convention on Cyber Security and Personal Data Protection (AUCC) in 2019. Article 8 provides

that states' parties must commit to the establishment of legal frameworks which protect fundamental rights and freedoms, particularly the protection of physical data. Further, without prejudice to the free flow of data, violations of privacy must be punished. The legal framework must provide that data processing upholds natural persons' fundamental rights while acknowledging state prerogatives, local communities' rights and the purposes for which businesses were established.

## Southern African Development Community Model Law

Namibia is a member of the Southern African Development Community (SADC) and signatory to the SADC Model Law. As a model law, Namibia may benefit from the model (guidance) provisions for the purposes of drafting domestic data protection law but is under no legal obligation to incorporate the provisions into domestic data protection legislation. On the other hand, Namibia's ratification to the AUCC read with section 144 of the constitution that renders international obligations binding on Namibia, is assured to harmonise its data protection law, at least at the principal level, with the AUCC. Similarly, as a signatory to the ICCPR, Namibia's data protection law when effected must assure in accordance with Article 17 that restricts the arbitrary or unlawful interference with privacy and requires legal protection against the infringement of the right to privacy.

## Commonwealth Cyber Declaration

Namibia is a member of the Commonwealth. The Commonwealth heads of government approved the Commonwealth Cyber Declaration in 2018 and this provides that members commit to strengthening data protection and security frameworks "in order to promote public trust in the

internet, confidence for trade and commerce, and the free flow of data." This is a component of the objective of the development of a cyberspace which supports socioeconomic development and online rights in member states. As part of implementation of the declaration, the Commonwealth initiated the African Cyber Resilience Project to support Namibia (among other nations) to review and reform its cybercrime law. To this end, the Commonwealth and the MICT jointly held a workshop in February 2020 to discuss the drafting of a national cybersecurity strategy.

## Budapest Convention

Namibia is currently deliberating the ratification of the Budapest Convention on Cybercrime following a drive from the MICT and preliminary approval from the Attorney General's Office. While the process is in the advanced stages, the convention was not ratified at time of publishing.

## CoE Convention on Automatic Processing of Personal Data

While a number of African nations have acceded to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Namibia is not a signatory.

Notably, in 2016, the United Nations urged Namibia to strengthen privacy protections due to its concerns on surveillance and the lack of legal safeguards to protect privacy rights.

## Namibian Data Protection Bill, 2020

In 2020, the Council of Europe and the Commonwealth Secretariat collaborated with MICT to jointly hold a data


Stakeholders' consultation workshop on the Data Protection Bill in Namibia

protection legislation drafting workshop from 24 to 26 February 2020.[19] A variety of stakeholders participated and these included representatives from parliament, the presidency, the vice-president, the prime minister's offices and representatives from the private sector, government departments and civil society groups. The participants discussed the right to privacy and fundamental rights entrenched in the constitution and also reviewed the SADC Model Law on Data Protection, the AU Convention on Cyber Security and Personal Data Protection and the Council of Europe Convention 108+. The participants concluded that both the data protection policy and legislation must be drafted in a manner which upholds constitutional

19 Council of Europe. (2020, 24 September). Online Drafting and Consultation Workshops on Data Protection. *Global Action on Cybercrime Extended*.

imperatives and is in compliance with international and regional data protection instruments.

The Council of Europe, operating in accordance with the Global Action on Cyber Crime Extended (GLACY+) Project, has developed a two-phase process for the development of the new Data Protection Bill. Phase 1 took place between 1 and 18 September 2020 and involved engagement with high level Namibian institutions including the Ministry of Justice and nominated local experts. The first phase involved drafting workshops which considered regional and international data protection frameworks including the SADC model law, the AUCC and Convention 108+. Concluding the workshop, the first draft of the bill was finalised on 21 September 2020.[20]

Phase 2 began on 28 September 2020 and was to conclude on 15 October 2020. This phase involves expanded stakeholder drafting workshops with civil society, mass media, law enforcement, presidential advisors and financial institutions. Upon completion of these workshops, the bill will be amended to account for insights gained during the workshops, ultimately culminating in another round of stakeholder consultations on the second draft of the bill scheduled for October 2020.[21]

Upon completion of the second draft of the bill and receipt of further stakeholder submissions following the engagements, it will be submitted to cabinet for review and if approved it could be before parliament in 2021.[22] It is important to note that before the bill can be approved by parliament, further rounds of public stakeholder engagements will take place, in accordance

20 Ibid.

21 Ibid.

22 Interview with first respondent, 29 September 2020; interview with third respondent, 2 October 2020.

with the proposed approach. Given the process that lies ahead it is difficult to anticipate a clear time frame for promulgation and commencement even if the bill is accepted by cabinet and ultimately passed by parliament following further rounds of broader public engagement which are likely to only take place in 2021.[23]

## Key features of the comprehensive data protection law

Namibia's Data Protection Bill, dated 25 September 2020, aims to function as an omnibus, dedicated data protection and privacy law for Namibia. When passed as law, the bill would apply to all "processing of personal data wholly or partly by automated and by non-automated means, where the personal data form part of a structured set of data and are accessible or retrievable according to specific criteria"[24] by controllers and, where applicable, processors, in the private and public sectors.[25] Notably, the bill also has extra-territorial application to "the processing of personal data undertaken outside the territory of Namibia where such processing relates to individuals resident within the jurisdiction of Namibia."[26]

## Key definitions under the bill

The bill adopts similar terminology to that contained within European and United Kingdom data protection legislation, including terminology relating to key stakeholders and processors such as "data subject", "controller", "joint-controllers", "processor", "supervisory authority", "consent" and "processing".

23 Interview with first respondent, 29 September 2020.

24 Data Protection Bill, 2020., s2(1).

25 Ibid., s 2(3).

26 Ibid., s 2(4).

The bill includes various specialised technical definitions such as “biometric data”, “genetic data”, “special categories of personal data”, “data concerning health”, “direct marketing”, “restriction of processing”, “personal data breach”, “automated individual decision-making and profiling”, “profiling”, “anonymisation” and “pseudonymisation”.

## Data subject rights

The bill includes the following rights:

- The right to know and access
- The right to rectification, erasure, restriction of processing
- The right to object
- The right not to be subject to automated decision making, including profiling
- The right to obtain assistance from a supervisory authority
- The right to compensation
- The right to be represented (representation of the data subject).

## Conditions for processing

The bill contains five basic principles relating to the processing of personal data. These include: (1) fair, transparent and lawful processing,[27] (2) specific legitimate purpose and purpose limitation,[28] (3) data minimisation,[29] (4) accuracy[30] and (5) storage limitation.[31]

27 Ibid., s 3(1).

28 Ibid., s 3(2).

29 Ibid., s 3(3).

30 Ibid., s 3(4).

31 Ibid., s 3(5).

The principles of fairness, transparency and lawfulness are also located under controller and processor obligations under the bill. Thereunder, controllers and processors are explicitly required to process personal data subject to transparency (section 16) and accountability provisions (section 19).

The bill also provides for special conditions for the processing of "Special Categories of Personal Data", which is by default, prohibited[32] – subject to various derogations contained in section 7(1)(a)-(f).

## Breach notification requirements

The breach notification requirements of the bill are modelled very closely on the GDPR's requirements, which amongst other things:

- Require that breaches are reported to the supervisory authority, without any undue delay, and not later than 72 hours after becoming aware of any personal data breach.[33]
- Provide for exceptions to breach notifications to both the supervisory authority and data subjects, where the breach is unlikely to result in a high risk to the rights and freedoms of data subjects,[34] or where one of the grounds listed under section 23(3) is present.
- Require controllers, where notification is not made within 72 hours, to provide reasons to the supervisory authority for the delay.[35]

32 Section 7(1) provides that: "the processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and personal data relating to criminal offences, including criminal records, may entail risks to data subjects independently of the context of the processing, and is prohibited…"

33 Data Protection Bill. 2020., s 22(1).

34 Ibid., s 22(1) as read with s 23(1).

35 Ibid., s 22(2).

- Require a processor who becomes aware of a personal data breach, to notify the controller, without undue delay, of any such breach affecting the personal data he/she/it processes on behalf of the data controller.[36]
- Require controllers to document any personal data breach, recording all facts relating to the breach, the effects of the breach, and any remedial action taken by the controller.[37]
- Require controllers, when notifying data subjects of a personal data breach, to communicate in clear and plain language the nature of the personal data breach and recommend measures to address the personal data breach, including, where appropriate, measures to mitigate the possible adverse effects of the breach.[38]

## Cross-border data transfers

Like many other data protection laws,[39] the bill provides for a general prohibition on the transfer of personal data across borders to other countries. However, in the same manner as the GDPR, the bill also makes provision for transfers to international organisations. In both cases, such transfers are prohibited "unless an appropriate level of data protection is guaranteed."[40] The bill deems appropriate levels of protection as including: (i) laws, (ii) applicable international treaties and agreements, or (iii) ad-hoc or approved standardised safeguards provided by legally binding and enforceable instruments that have been adopted and implemented by a receiving country or international organisation.

36 Ibid., s 22(3).

37 Ibid., s 22(5).

38 Ibid., s 23(3).

39 See for instance, South Africa's Protection of Personal Information Act, 2013, as well as the European Union's General Data Protection Regulation, 2018.

40 Data Protection Bill, 2020., s 24(1).

Under the bill, the test to determine whether the level of protection afforded by a receiving country is appropriate is dynamic, and takes into account various factors[41] including: (i) the nature of the personal data to be transferred, (ii) the purpose and duration of the envisaged transfer, (iii) the data protection laws, both general and sectorial, in force in the receiving country or international organisation in question, and (iv) the recipient or recipients to whom the personal data are transferred.

Section 24(3) of the bill provides for various derogations where third countries or international organisations do not ensure an appropriate level of protection – deemed as such by section 24(2). These derogations may be summarised as including instances where the transfer:

- Is based on explicit, specific and freely given consent.
- Is required based on a data subject's specific interests.
- Is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- Is in response to a legitimate interest, in particular an important public interest, which is provided for by law.
- Constitutes a necessary and proportionate measure in a democratic society for the freedom of expression.

Other observations concerning cross-border transfers of personal data include those relating to an obligation on controllers to document their own assessments of appropriate safeguards and/or derogations, as well as powers given to supervisory authorities to "prohibit transfers to other countries

41 Ibid., s 24(2).

and international organisations, suspend them or subject them to additional conditions"[42] in order to protect the rights and fundamental freedoms of data subjects.

## Public interest exemptions

Exceptions to the application of the bill are limited to the provisions of section 3 (basic principles), section 8 (data breach notification), section 16 (transparency of processing) and Part III (rights of the data subject). Section 15 of the bill lists various grounds for exception which include: national security; defence; public safety; important economic and financial interests of the state; the impartiality and independence of the judiciary of Namibia; the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the protection of the data subject or the rights and fundamental freedoms of others, notably the freedom of expression. All exceptions must be provided for by law, and must pursue a legitimate purpose, respect fundamental rights and freedoms and must be necessary and proportionate in respect of the grounds of exception.

Commendably, section 15(3)-(6) sets out various checks and balances on the use of exceptions under the bill which include limitations such as:

- A requirement that the use of exceptions and restrictions are subject to objective and adequate safeguards in order to be considered lawful and to guard against their arbitrary application.
- A prohibition on the insertion of blanket or unnecessarily broad exceptions in a Namibian law.

42 Ibid., s 24(6).

- A requirement for controllers to document and make available to the data protection supervisory authority on request, any restriction invoked.
- A requirement for independent and effective review and supervision of processing activities that are carried out for national security and defence purposes.

## Establishing a Namibian Data Protection Authority

The Namibian Data Protection Bill proposes an independent Data Protection Supervisory Authority (section 25) with various enforcement and investigation powers (section 34), as well as powers to impose penalties and fines. However, whilst the bill provides for sanctions and penalties (Part VIII), the bill, in its current draft form, does not list any such penalties, despite providing a placeholder for penalties under section 41.

Section 27(1) of the bill requires that the Data Protection Supervisory Authority must "be provided with the necessary resources to enable it to appoint skilled staff in the field of ICT technologies, security, law and digital technologies, to build internal capacity to enable the effective performance of its functions." The DPA will also consist of a board of directors with five members who shall sit for a term not exceeding five years.

The bill in its current form does not specify a minimum age requirement for members of the board but does require that members of the board "must have knowledge of data protection law acquired from relevant professional experience and be qualified for judicial office or higher administrative service." Furthermore, section 28 of the bill requires that members may not be attached to parliament, government or any ministry or other statutory body.

## Proposed functions of the Data Protection Authority

Section 34 of the bill provides that the functions of the supervisory authority include:

- To promote and enforce fair processing of personal data in accordance with this act.
- To promote public awareness and understanding of the risks, rules, and rights in relation to the processing of personal data.
- To promote the awareness of controllers and processors of their obligations under this act and give advice upon request.
- To submit to the court any administrative act which is not compliant with the fundamental principles of the protection of the privacy and the personal data protection.
- To advise the minister, the parliament, the government and other institutions and bodies on matters relating to the right to privacy and data protection and related fundamental rights.
- To conduct inquiries and investigations.
- To investigate any complaint received.
- To perform the functions relating to transborder transfers of personal data provided for, notably the approval of standardised safeguards.
- To encourage the drawing up of codes of conduct and internal rules in relation to the processing of personal data and provide opinions and approve such codes of conducts and internal rules.
- To cooperate and share information with other supervisory authorities and participate in any international negotiations on matters of data protection.

## Funding of the DPA

Section 37 of the bill provides that the data protection supervisory authority (DPA) shall be funded partly by monies appropriated by parliament and partly by way of charging fees payable by a controller, unless exempt as set out in this act. The DPA shall also be allocated a separate and independent annual budget that shall consist of adequate financial resources to carry out its mandate.

According to the bill, the budget of the DPA shall neither be subject to influence by government during the initial allocation of funds nor with regard to the manner in which the funds are spent. The annual budget of the DPA is to be authorised by parliament.

## Notable provisions

Despite not being referred to as a principle, controllers and processors are required to consider the technical principle of "data protection and privacy by design and by default"[43] as well as conduct data protection impact assessments.[44]

## Analysis in line with AfDec and other instruments

At their core, and despite their nuances, all national, regional and international instruments concerning the protection of personal data and privacy contain: (i) fundamental concepts, (ii) basic principles governing the processing of personal data, (iii) general rights bestowed upon data subjects, and (iv) statutory obligations on a fixed set of stakeholders.

43 Ibid., s 17.

44 Ibid., s 21.

A number of national and international privacy frameworks have largely converged to form a set of core, baseline data protection principles. These are implemented in national privacy frameworks in over 100 countries.[45]

The analysis below compares key regional and international instruments against the bill. For brevity, the substantive content of the bill will not be repeated but rather, reference is made to the section above on key features of the comprehensive data protection law.

## The African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection (AUCC)[46] was drafted in 2011 to establish a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime. The AUCC encompasses, in cybersecurity, three main areas: (1) electronic transactions, (2) personal data protection, (3) cybersecurity and cybercrime. The Convention will enter into force 30 days after the 15th instrument of ratification or accession is deposited. The current status is eight ratifications out of 55 AU member states (Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal), while 14 more member states have signed the Convention.

Chapter II of the AUCC is dedicated to personal data protection, comprising three core sections. Section I relates to personal data protection generally (providing for preliminary aspects of the AUCC as it relates to personal data protection), section II

45 Internet Society & Commission of the African Union. (2018). *Personal Data Protection Guidelines for Africa*. https://www.internet-society.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

46 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.pdf

outlines the institutional framework for the protection of personal data of state parties who have acceded to the AUCC and section III provides for basic principles governing the processing of personal data and data subject rights. The substantive content and requirements on state parties under chapter II of the AUCC may be summarised as follows:

- Establish a legal framework that strengthens the fundamental rights and freedoms of citizens, particularly the protection of their personal data and provide penalties for the violation of privacy whilst balancing against the need to ensure the free flow of data (Article 8.1).
- Ensure that specific activities related to the processing of personal data are subject to the authorisation of an administrative authority (Article 10.4).
- Establish an institutional framework for personal data protection, by inviting states parties to establish an independent administrative authority in charge of protecting personal data in their national mechanism (Article 11).
- Establish obligations relating to conditions governing personal data processing, thus making it possible, on the one hand, to lay down the basic principles governing the processing of personal data (Article 13) and, on the other hand, specific principles (Article 14) for the processing of sensitive data, as well as the supervision of personal data files interconnection. Article 13 contains six basic principles governing the processing of personal data. These are: consent and legitimacy; lawfulness and fairness; purpose, relevance and storage; accuracy; transparency; and confidentiality and security. Article 14 provides for a general prohibition on the processing of sensitive data subject to various exceptions.[47]

47 Ibid., arts 14(3) and 14(4).

- Provide for data subjects' rights, namely the right to information,[48] the right of access,[49] the right to object[50] and the right of rectification or erasure.[51] In addition, Article 14(5) provides for a negative right wherein data subjects may not be subject to an automated decision based on solely automated processing under certain circumstances.
- Provide for obligations of the personal data controller, namely the confidentiality obligations,[52] security obligations,[53] storage obligations[54] and sustainability obligations,[55] which reflect the rights of the persons concerned and are consistent with personal data processing principles.

To begin the comparison, the Namibian Data Protection Bill satisfies the AUCC's requirements to establish a legal framework for the protection of personal data and establish an independent administrative authority in charge of protecting personal data. Specifically, the bill establishes an independent data protection supervisory authority (section 25) entrusted with various enforcement and investigation powers (section 34), as well as powers to impose penalties and fines. However, whilst the bill provides for sanctions and penalties (part VIII), the bill, in its current draft form, does not list any such penalties, despite providing a placeholder for penalties under section 41. The bill also makes provision for cross-border flows of personal data, subject to stringent requirements (section 24). Further, in some cases, the bill goes beyond the AUCC's requirements, for example insofar as

48 Ibid., art 16.

49 Ibid., art 17.

50 Ibid., art 18.

51 Ibid., art 19.

52 Ibid., art 20.

53 Ibid., art 21.

54 Ibid., art 22.

55 Ibid., art 23.

the application of the bill is concerned and its exceptions, having extra-territorial application (section 2(4)), strong restrictions on the exceptions to the application of the bill (section 15(3)-(4)) and obligations on exempt parties under the bill (section 15).

As canvassed above, the bill also includes various basic principles, special principles relating to sensitive data, numerous data subject rights and various obligations on data controllers and processors. The extent to which these areas of the bill satisfy these areas of the AUCC are canvassed hereunder:

- The basic principles under the bill, for the most part mirror those within the AUCC. In their application, they provide for the same rationales governing the processing of personal data. The only principle that the bill does not have is that of "confidentiality and security". However, whilst the bill does not have an explicit "confidentiality and security" principle, the substance of the AUCC's principle is located and amplified (extensively) within the bill's confidentiality and security obligations on controllers and processors.[56]
- Furthermore, like the AUCC, the bill provides for a general prohibition against the processing of sensitive data (which it refers to as "special categories of personal data"), subject to various legislated exceptions. However, on a granular level, differences appear between the bill and the AUCC insofar as the scope of exceptions and the scope of what is considered sensitive data are concerned. In particular, the bill provides for varied exceptions[57] to the general prohibition, and does not extend its definition of special categories of personal data to "parental filiation", as required by the AUCC.

56 In particular, s 18(1) lays down a general obligation on both controllers and processors to "implement appropriate technical and organizational measures to protect personal data and special categories of personal data against accidental or unauthorized access to, use, loss, damage, alteration, disclosure and destruction of the data, transmitted, stored or otherwise processed." S 18(2) also requires controllers and processors to take into account various factors in complying with their s 18(1) obligations. Lastly, s 18(4) provides for detailed obligations on controllers when processing is required to be carried out by a processor.

57 Data Protection Bill. 2020., s 7(1)(a)-(f).

- When considering the extent of data subject rights under the bill as compared to the AUCC, the bill clearly provides for all data subject rights provided for under the AUCC, and more. Specifically, the bill provides for additional rights, such as the rights to obtain assistance from a supervisory authority,[58] compensation,[59] representation of the data subject,[60] and the right not to be subject to automated decision making, including profiling.[61]
- In regard to obligations on controllers and processors, the bill meets the AUCC's confidentiality, security and storage obligations, whilst going beyond by placing additional obligations on controllers relating to: data protection and privacy by design and by default,[62] records of processing activities,[63] data protection impact assessment,[64] and breach notification requirements.[65] However, the bill does not meet the AUCC's requirement on two other fronts. On the one hand, the bill does not place any sustainability obligations on controllers (which effectively serve as a right to data portability). On the other hand, the bill does not provide for an obligation on controllers to receive prior authorisation from the DPA under certain legislated circumstances.

In the majority, the bill complies with data protection and privacy requirements found in the AUCC, it has been found that with exception of the requirements for sustainability obligations and prior authorisation procedures, the bill fulfils the requirements of the

58 Ibid., s 12.

59 Ibid., s 14.

60 Ibid., s 13.

61 Ibid., s 11.

62 Ibid., s 17.

63 Ibid., s 20.

64 Ibid., s 21.

65 Ibid., s 22-23.

AUCC and in various instances, goes beyond such requirements with stricter and more comprehensive rights and obligations.

## The Personal Data Protection Guidelines for Africa

The Personal Data Protection Guidelines for Africa[66] were developed out of a joint initiative between the Commission of the African Union and the Internet Society in 2018. The guidelines emphasise the importance of ensuring trust in online services, as a key factor in sustaining a productive and beneficial digital economy. They also offer guidance on how to help individuals take a more active part in the protection of their personal data, while recognising that in many areas, positive outcomes for individuals depend on positive action by other stakeholders.

The guidelines directly incorporate the principles contained within the AUCC (Malabo Convention) (discussed above) and also synthesise data protection principles from other data protection and privacy instruments such as the Organisation for Economic Co-operation and Development (OECD) privacy guidelines; the Council of Europe's Convention 108; and the Asia-Pacific Economic Cooperation (APEC) privacy framework. The guidelines expressly highlight the close similarity between the AUCC's principles and those synthesised[67], whilst placing an emphasis on the differences between the AUCC and the other instruments. In particular, "consent" being considered a separate principle in the AUCC, and the presence of explicit requirements for "accountability" within the other instruments.

66 Internet Society & African Union. (2018). Op. cit.

67 The synthesised principles are: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; Individual participation and accountability.

In assessing the bill against the guidelines, the following has been observed:

- The bill meets all of the data processing principles identified in the guidelines. In addition, the bill, unlike the AUCC, has a specific accountability provision for controllers, and where applicable, processors.
- The substantive and procedural features of the bill (detailed in section 8 of this report) align with various recommendations to government, policy makers and data protection authorities that are made within the guidelines. These recommendations include: “Respect for privacy online and offline”; “Greater consistency in personal data protection across Africa”; “Role and independence of data protection authorities”; and “Exceptions to data protection and privacy laws”.

## The South African Development Community (SADC) Model Law on Data Protection

The SADC Model Law on Data Protection[68] (the Model Law) was developed by the Southern African Development Community in 2010 and officially adopted in 2013. The preamble of the model law points to an objective to harmonise data protection across member states, whilst reiterating the need for specific data protection and privacy principles to govern the processing of personal data.

It is important to underscore that the initial Namibian Data Protection Bill, 2013, was predicated on the SADC Model Law, which, in 2013, did not contain various data processing principles, data subject rights, and controller and processor obligations that the current revision contains. In this regard, it is noted that the current bill has been influenced by and closely modelled off of various regional

68 HIPSSA. Draft Southern African Development Community (SADC) MODEL LAW ON DATA PROTECTION. (2011). http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data protection.pdf

and international instruments (including the AUCC, Convention 108 and the European Union's General Data Protection Regulation, 2018).

Considering the foregoing, an analysis of the bill against the 2013 SADC Model Law is not warranted for the purposes of this report.

## Analysis against Convention 108

Convention 108 (modernised)[69] is "the only international legally binding instrument on the protection of private life and personal data open to any country in the world."[70] Convention 108 was established by the Council of Europe and sets out to "protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy."[71] Convention 108, amongst other things, provides for:

- Requirement of signatory parties to provide for one or more authorities to be responsible for ensuring compliance with the provisions of Convention 108.[72]
- Obligations relating to conditions governing personal data processing, namely that processing be legitimate (Article 5) and transparent (Article 8). Convention 108 also explicitly requires that signatory parties provide for processing to be authorised when carried out on the basis of free, specific, informed and unambiguous consent, or based upon another legitimate basis laid down by law. Article 5 of convention provides for various obligations in order for processing to be considered legitimate. In this regard, processing must be:

69 Council of Europe. (2018, 18 May). Modernised Convention for the protection of Individuals with Regard to the Processing of Personal Data. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

70 Council of Europe. (2018). Convention 108+ : the modernised version of a landmark instrument. https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108.

71 Council of Europe. (2018). Op. cit., art 1.

72 Council of Europe. (2018). Op. cit., art 15.

lawful; proportionate in relation to the legitimate purpose; fair and transparent; collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; adequate, relevant and not excessive; accurate; and preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed. Article 6 of Convention 108 also provides for the protection of special categories of data.

- Data subjects' rights, namely: the right to object; to obtain confirmation of processing activities; to rectification or erasure; to have a remedy; to obtain assistance from a supervisory authority; and the right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.

- Obligations on the personal data controller and processor relating to data security[73] which include a requirement that at the least, notifications of security breaches must be made to supervisory authorities.

- Rules around cross-border transfers of personal data, with a prohibition on signatory parties to "prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention."[74]

When assessing the bill against Convention 108, the following has been observed:

- In terms of an institutional framework for the protection of personal data in Namibia, the bill establishes an independent

73 Council of Europe. (2018). Op. cit., art 7.

74 Council of Europe. (2018). Op. cit.,art 14.

data protection supervisory authority (section 25) that is bestowed with various enforcement and investigation powers (section 34), as well as powers to impose penalties and fines. However, whilst the bill provides for sanctions and penalties (part VIII), the bill, in its current draft form, does not list any such penalties, despite providing a placeholder for penalties under section 41. The bill also makes provision for cross-border flows of personal data, subject to stringent requirements (section 24).

- In comparison to Convention 108, the bill provides for equal principles and obligations relating to personal data processing. Furthermore, and like Convention 108, the bill regulates the processing of sensitive data and provides for a general prohibition against the processing of sensitive data (which it refers to as “special categories of personal data”). The scope of what the bill considers to be “special categories” of personal data mirror those which Convention 108 deems to be sensitive data.
- When considering the extent of data subjects’ rights under the bill as compared to Convention 108, the bill provides for equal data subject rights. However, whilst the bill does not explicitly provide a right to “obtain confirmation of processing activities”, the bill does nonetheless provide for a right to know and access[75] which includes “the right to obtain, on request and at reasonable intervals: (a) confirmation as to whether or not personal data relating to him or her are being processed”. A nuance does, however, arise between the rights concerning automated processing in Convention 108 and the bill. Unlike Convention 108, the bill explicitly extends the right to include profiling.[76]

75 Data Protection Bill. 2020., art 8.

76 Ibid., art 11.

- The bill adequately meets Convention 108's requirements for "data security" obligations on controllers and processors by requiring security of processing,[77] as well as breach notification requirements[78] that include notifications to the supervisory authority. The bill also goes further and provides for additional obligations including data protection and privacy by design and by default,[79] records of processing activities,[80] and data protection impact assessments.[81]
- In the case of cross-border transfers, the bill differs from the convention in that it does not, by default,[82] place a prohibition on prohibiting transfers between signatory parties of Convention 108, but rather, prohibits cross-border transfers except for under stringent requirements and derogations.[83]

In concluding the above analysis of the extent to which the bill complies with data protection and privacy requirements found in Convention 108, it has been observed that the bill meets (and in certain cases, exceeds) these requirements with minor exceptions (these being the scope of the right relating to automated processing, and prohibitions on cross-border transfers).

## Analysis against the GDPR

Having been in force since 25 May 2018, the European Union's General Data Protection Regulation, 2018, repealed the EU's prior Data Protection Directive of 1995 and standardised

77 Ibid., art 18.

78 Ibid., s 22-23.

79 Ibid., s 17.

80 Ibid., s 20.

81 Ibid., s 21.

82 Article 14(1) of Convention 108 does provide for exceptions for the prohibition on a transfer of personal data where "there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation."

83 Data Protection Bill, 2020., s 24.

data-protection laws across EU member states. The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data and protects fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.[84]

The GDPR, amongst other things, provides for:

- A requirement to establish an institutional framework for personal data protection by establishing an independent administrative authority in charge of monitoring application of, and enforcing the regulation.[85]
- Principles relating to personal data processing,[86] namely lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality. Article 9 of the GDPR also provides for specific rules relating to the processing of special categories of personal data, with a default prohibition on such processing.
- Data subjects' rights, namely the rights of access,[87] rectification,[88] erasure,[89] restriction of processing,[90] data portability,[91] and the right to object.[92]
- Obligations on the personal data controller and processor, including security of processing,[93] notification of personal

84 EU. (2018). General Data Protection Regulation, art 1. https://gdprinfo.eu/

85 Ibid., art 51.

86 Ibid., art 5.

87 Ibid., art 15.

88 Ibid., art 16.

89 Ibid., art 17.

90 Ibid., art 18.

91 Ibid., art 20.

92 Ibid., art 21.

93 Ibid., art 32.

data breaches to supervisory authorities,[94] communication of personal data breaches to data subjects,[95] and other additional obligations are placed on controllers concerning data protection impact assessments[96] and data protection by design and default.[97]

- A requirement that specific activities related to the processing of personal data are subject to prior consultation from a supervisory authority.[98]
- Rules around cross-border transfers of personal data.[99]

When assessing the bill against the GDPR, the following findings have emerged:

- The bill, like the GDPR, provides for the creation of an institutional framework for the protection of personal data in Namibia. In this regard, an independent data protection supervisory authority is established in section 25 and is bestowed with various enforcement and investigation powers[100], as well as powers to impose penalties and fines. However, whilst the bill provides for sanctions and penalties (part VIII), the bill, in its current draft form, does not list any such penalties, despite providing a placeholder for penalties under section 41. In a similar vein to the GDPR, the bill also provides for co-operation and assistance requirements. In particular, it provides that:

94 Ibid., art 33.

95 Ibid., art 34.

96 Ibid., art 35.

97 Ibid., art 25.

98 Ibid., art 36.

99 Ibid., arts 15(2); 44; 45(1) and 45(2).

100 Data Protection Bill, 2020., s 34.

> The Data Protection Supervisory Authority shall perform the data protection functions that are necessary to give effect to any international obligations such as those required by the Malabo Convention, the SADC Data Protection Model Law, the African Union Convention on Cyber Security and Personal Data Protection as well as any obligations arising from international data protection instruments.[101]

- The bill provides for equal principles governing personal data processing to those contained within the GDPR.
- Concerning the processing of sensitive or special categories of personal data, the bill also prohibits the processing of such data by default, subject to various derogations contained within section 7(1)(a)-(f) of the bill. A nuance has been observed between the GDPR and the bill in that the bill also lists "personal data relating to criminal offences, including criminal records" as a special category of personal data whereas the GDPR does not. Instead, the GDPR provides for an explicit provision relating to the processing of "personal data relating to criminal convictions and offences".[102]
- The bill provides for the same categories of data subject rights as those contained in the GDPR, save for the GDPR's right to data portability.
- Concerning obligations on personal data controllers and processors, the bill, for the most part, mirrors the obligations found in the GDPR. However, it is important to note that the bill approaches the allocation of obligations differently to the GDPR in that the GDPR separates obligations for controllers and processors, respectively, whereas the bill groups them. Nevertheless, the bill contains the same

101 Ibid., s 36.

102 EU. (2018). Op. Cit., art 10.

"security of processing" requirements for controllers, and in some cases, more stringent requirements for processors. The bill also closely models the GDPR's breach notification clauses and therefore satisfies the requirements placed upon controllers and processors concerning breach notifications. Notably, whilst the bill provides for data protection impact assessments,[103] it does not have provisions relating to prior authorisation or prior consultation with the future Namibian Supervisory Authority.

- In a similar vein to the GDPR, the bill prohibits cross-border transfers except for under stringent requirements and derogations.[104] The bill also, like the GDPR, includes a differentiation between third countries (which the bill refers to as "receiving countries") and international organisations.

The above analysis suggests that the bill complies with data protection and privacy requirements found in the GDPR, it has been observed that the bill meets and satisfies many of the requirements, obligations and features of the GDPR. However, distinctions are observed relating to the inclusion of criminal records and offences as special category personal data in the bill, as well as the lack of prior authorisation or prior consultation provisions in the bill.

## Analysis of the status of a human rights-based approach to personal data protection in the country

### What is a human rights-based approach?

Essentially, the human rights-based approach is "a conceptual framework developed to help promote and protect human rights

103 Data Protection Bill, 2020., s 21.

104 Ibid., s 24.

through putting state's obligations with regard to human rights at the centre of policy and regulation in any sector."[105] The human rights-based approach is underpinned by five key human rights principles, also known as PANEL:

- Participation: Everyone is entitled to active participation in decision-making processes which affect the enjoyment of their rights.
- Accountability: Duty bearers are held accountable for failing to fulfil their obligations towards rights holders. There should be effective remedies in place when human rights breaches occur.
- Non-discrimination and equality: All individuals are entitled to their rights without discrimination of any kind. All types of discrimination should be prohibited, prevented and eliminated.
- Empowerment: Everyone is entitled to claim and exercise their rights. Individuals and communities need to understand their rights and participate in the development of policies which affect their lives.
- Legality: Approaches should be in line with the legal rights set out in domestic and international laws.

## Analysis of the bill through the lens of a human rights-based approach

The analysis below the Namibian Data Protection Bill against each of the human rights-based approach principles.

Participation: In assessing alignment between the bill and the principle of participation, it is important to consider aspects of

105 https://unsdg.un.org/2030-agenda/universal-values

participation at the substantive level of the bill, as well as during the surrounding procedural aspects of drafting and legislating the bill. In terms of the former aspect of participation, the bill features two instances where decision making may impact the rights of a data subject:

- The first instance relates to scenarios where a data subject may be subject to an automated decision by a solely automated process. A strong feature of the bill is the presence of a right not to be subject to automated decision making, including profiling. In particular, data subjects have the right "not to be subject to a decision significantly affecting him or her based solely on the automated processing of his or her personal data without having his or her views taken into consideration."[106] Whilst there are exceptions to the application of this right, data subjects are given an opportunity in certain cases[107] to participate in a decision reached by obtaining human intervention on the part of the controller and to put forward his or her point of view and to challenge the decision.
- The second instance relates to scenarios where a data subject may be subject to a decision of the future Namibian data protection supervisory authority. In such cases, the data subject would be entitled to seek recourse with a judicial authority, or mandate a permitted organisation under section 13 to "pursue an effective judicial remedy on behalf of the data subject, against a legally binding decision of the Data Protection Supervisory Authority."[108]

106 Data Protection Bill, 2020., s 11(1).

107 Where an exception arises under s 11(2)(a) or (c) of the bill.

108 Data Protection Bill. 2020., s 13(1)(b).

Accordingly, in both such cases, the bill provides for a form of participation and recourse and therefore aligns with the human rights-based approach principle of participation.

Concerning the latter aspect of participation in the drafting and legislative process of the bill, it is apparent that a wide range of stakeholders have participated[109] in the early consultations on the drafting of the bill, including representatives from parliament, the presidency, the vice-president's and prime minister's offices, and representatives from the private sector, government departments and civil society groups. A second phase of legislative drafting was to be held from 28 September until 15 October 2020. This phase entails workshops for stakeholders comprising the media, civil society, financial institutions, law enforcement and representatives from the presidency. It is imperative that the intended broad stakeholder engagement occurs, informing the incorporation of regional and international data protection standards and multi stakeholder input is obtained to ensure adherence to national legislation and responsiveness to national concerns.

Should the drafting process effectively include a wide range of stakeholders in the legislative process, this would represent adherence to the principle of "participation".

Accountability: Whilst not framed as a principle, the bill explicitly provides for an accountability provision under which:

> Controllers and, where applicable, processors, must take all appropriate measures to comply with the provisions set out in this Act and be able to demonstrate that the data processing under their control complies with them.[110]

109 Council of Europe. (2020, 24 September). Online Drafting and Consultation Workshops on Data Protection. *Global Action on Cybercrime Extended*.

110 Data Protection Bill, 2020., s 19.

Coupled with the presence of various fines and penalties under the bill, and the establishment of a data protection supervisory authority, the bill would ensure that controllers and processors are held accountable for failing to fulfil their obligations towards data subjects in terms of the bill and therefore satisfies the "accountability" principle of the human rights-based approach.

Non-discrimination and equality: Section 2(2) of the bill provides that the act would, as a law of general application, aim to protect everyone's rights in terms of personal data, irrespective of their nationality and residence. It is noteworthy that the bill provides that non-citizens and non-residents are afforded protection of their personal data where they are residing in Namibia:

> This Act applies to the processing of personal data undertaken within the territory of Namibia as well as to the processing of personal data undertaken outside the territory of Namibia where such processing relates to individuals' resident within the jurisdiction of Namibia.

Furthermore, under the bill, "all data subjects have the right to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of section 25, in exercising his or her rights under this Act."[111] As the human rights-based approach requires that everyone is entitled to exercise their rights free from discrimination of any kind, the bill's protection of non-citizens and non-residents affirms adherence to the principle of "non-discrimination and equality".

Empowerment: In this regard, it is a positive indicator that not only does the bill explicitly provide data subjects with various traditional data protection and privacy rights, but it also bestows

111 Ibid., s 12.

upon data subjects the right to obtain assistance from a supervisory authority,[112] and the right to obtain representation[113] by a not-for-profit body, organisation or association which has been properly constituted under Namibian law, to:

- Lodge a complaint on behalf of the data subject, with the data protection supervisory authority.
- Pursue an effective judicial remedy on behalf of the data subject, against a legally binding decision of the data protection supervisory authority.
- Pursue an effective judicial remedy on behalf of the data subject, against a data controller or processor.

Moreover, the bill also provides for a right to compensation under section 14, and a right of recourse to a judicial authority under section 30. Considering the foregoing, it is conclusive that the bill satisfies the human rights-based approach principle of “empowerment”.

Legality: The preamble of the bill highlights that it aims to protect the fundamental rights and freedoms of individuals, and in particular, their right to privacy which is protected by Article 13 of the Namibian Constitution. The bill is also in alignment with the rights and rationales set out in various international instruments that Namibia is a party to (International Covenant on Civil and Political Rights, African Charter on Human and Peoples Rights, the AUCC, etc). Furthermore, the analysis undertaken above has highlighted that the bill is extensive in its substantive rights and obligations and is predominantly in line with the legal rights set out in other data protection and privacy instruments. Accordingly, the bill may be deemed to be in line with the principle of “legality”.

112 Ibid., s 12.

113 Ibid., s 13.

In concluding the analysis of how a human rights-based approach to personal data protection has been applied in Namibia's policy and regulation, it has been found that the bill meets all the principles of the approach. However, it is emphasised that without enactment, or a proper functioning data protection supervisory authority, the protection of the human rights of Namibian citizens will be limited to Namibia's existing legal framework.

## Analysis against AfDec Principle 8

The African Declaration on Internet Rights and Freedoms (AfDec) is a pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. The declaration is intended to elaborate on the principles which are necessary to uphold human and individual rights on the Internet, and to cultivate an internet environment that can best meet Africa's social and economic development needs and goals.

Principle 8 (Privacy and Personal Data Protection) is one of 13 principles within the Declaration. The principle states that:

> Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law (as specified in Article 3 of the Declaration) and are necessary and proportionate in pursuance of a legitimate aim.

Considering Principle 8, one can extrapolate the following rights:

- Everyone has the right to privacy online.
- Everyone has the right to the protection of personal data concerning him or her.
- Everyone has the right to communicate anonymously on the internet.
- Everyone has the right to use appropriate technology to ensure secure, private and anonymous communication.

Furthermore, a core principle relating to any restriction of the above rights is apparent in that the above rights may only be limited by a law which pursues a legitimate aim as expressly listed under international human rights law (the AfDec states that grounds as such include the rights or reputations of others, the protection of national security, or of public order, public health or morals)[114] and are necessary and proportionate in pursuance of one of these legitimate aims.

In considering how the bill aligns with the requirements of Principle 8, the following observations have been made:

- Whilst the bill does not explicitly mention “privacy online”, the preamble of the bill indicates that it broadly intends to “protect the fundamental rights and freedoms of individuals, and in particular, their right to privacy with respect to the processing of such information” and can be interpreted to refer to all forms of processing, both online, and offline. The bill furthermore explicitly recognises a right to the protection of personal data which is only allowed to be limited in a very narrow set of circumstances. In particular, the bill sets out stringent requirements to be met where a public exemption

114 https://africaninternetrights.org

for the processing of personal data contrary to the provisions of the bill is sought.

- The bill does not provide for an explicit right to communicate anonymously online, or a right to use appropriate technology to ensure secure, private and anonymous communication. However, the bill does set out specific instances where public exemptions to the application of the bill may apply, thereby limiting the circumstances in which one's communications may be intercepted, surveyed or otherwise processed. Section 15 of the bill lists various public grounds for exception which include:
  - National security defence
  - Public safety
  - Important economic and financial interests of the state
  - The impartiality and independence of the judiciary of Namibia
  - The prevention, investigation and prosecution of criminal offences and the execution of criminal penalties
  - Other essential objectives of general public interest and the protection of the data subject or the rights and fundamental freedoms of others, notably the freedom of expression.

Further, all exceptions must be provided for by law, and must pursue a legitimate purpose, respect fundamental rights and freedoms and must be necessary and proportionate in respect of the grounds of exception. Of significance is the presence of various checks and balances on the use of exceptions under the bill contained within sections 15(3)-(6). These checks and balances include:

- The use of exceptions and restrictions shall be subject to objective and adequate safeguards in order to be considered lawful and to guard against their arbitrary application.[115]
- No blanket or unnecessary broad exceptions shall be defined in a law.[116]
- Any restriction shall be documented by the controller and be made available to the data protection supervisory authority on request.[117]
- Processing activities carried out for national security and defence purposes shall be subject to independent and effective review and supervision.[118]

When considering the bill's public exemptions alongside the AfDec's legitimate aims as expressly listed under international human rights law, it is apparent that the bill's exemptions include all of these legitimate aims under international human rights law. The bill's grounds for exemption may, however, be viewed as extending beyond the AfDec's listed legitimate aims. Those going beyond the AfDec's legitimate aims include: "important economic and financial interests of the State"; "the impartiality and independence of the judiciary of Namibia"; and the "prevention, investigation and prosecution of criminal offences and the execution of criminal penalties". However, because "the protection of public order" as provided for in the AfDec may likewise be interpreted broadly, these additional grounds may also be viewed as falling thereunder.

115 Data Protection Bill, 2020, s 15(3).

116 Ibid., s 15(4).

117 Ibid., s 15(5).

118 Ibid., s 15(6).

When considered alongside the various rights afforded to data subjects under the bill, it may be concluded that the bill meets all of the requirements of AfDec Principle 8, albeit indirectly insofar as the right to communicate anonymously online is concerned.

## Analysis against the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa

The Declaration of Principles on Freedom of Expression and Access to Information in Africa[119] ("the Declaration") is a soft-law instrument developed by the African Commission on Human and Peoples' Rights (ACHPR). The Declaration was revised and adopted by the ACHPR at its 65th Ordinary Session in 2019, replacing its 2002 iteration. The Declaration consists of 43 principles, including principles on access to the internet, internet intermediaries, privacy protections, and communication surveillance. The Declaration, at its essence, interprets Article 9 of the African Charter on Human and Peoples' Rights[120] – the right to receive information and free expression.

The relevant principles of the Declaration are as follows:

- Principle 40: Privacy and the protection of personal information
- Principle 41: Privacy and communication surveillance
- Principle 42: Legal framework for the protection of personal information.

Principle 40 outlines a fundamental right to privacy, including the confidentiality of one's communications and the protection of one's personal information, as well as a right to communicate

119 https://www.achpr.org/public/Document/file/English/Declaration of Principles on Freedom of Expression_ENG_2019.pdf

120 https://www.achpr.org/legalinstruments/detail?id=49

anonymously on the internet (including the use of pseudonyms) and to secure the confidentiality of one's communications and personal information from access by third parties through the use of digital technologies.

Principle 41 places limitations on state surveillance by placing a prohibition on the "indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications." States are also limited to only "engaging in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim." Where surveillance is predicated on a law, such law must provide adequate safeguards for the right to privacy including various factors provided for under Principle 41 (3)(a)-(f).

Principle 42 provides for basic principles that should govern the processing of personal data, as well as the basic data subjects rights that should be afforded to member state citizens. In particular, Principle 42 includes the following data protection and privacy features:

- Requirements that the processing of personal data be:
  - With the consent of the individual concerned
  - Conducted in a lawful and fair manner
  - In accordance with the purpose for which it was collected, and adequate, relevant and not excessive
  - Accurate and updated, and where incomplete, erased or rectified
  - Transparent and disclose the personal information held
  - Confidential and kept secure at all times.

- Other requirements include that oversight mechanisms be introduced through an independent entity that includes human rights and privacy experts.
- The right to:
  - Be informed in detail about the processing
  - Access personal information that has been or is being processed
  - Object to the processing
  - Rectify, complete or erase personal information that is inaccurate, incomplete or prohibited from collection, use, disclosure or storage
  - Exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it
  - Seek legal recourse to effective remedies.
- Obligations on parties who process personal data to notify persons in the event of a data breach (unauthorised access).

When considering the privacy-related requirements of the Declaration insofar as the protection of personal data is concerned, it has been found that the bill meets all of the requirements set out in Principle 42 (principles, rights and obligations), save for the unique requirement that the independent entity responsible for oversight (Namibia's future Supervisory Authority) include human rights and privacy experts.

In regard to the Declaration's requirements providing for a right to communicate anonymously online, it is reiterated that whilst the bill does not explicitly provide for such a right, the bill does, however, cater for the right to privacy online by protecting privacy

by default, and setting out specific instances where public exemptions to the application of the bill may apply, thereby limiting the circumstances in which one's communications may be intercepted, surveyed or otherwise processed.

Concerning state surveillance, it is emphasised that the bill provides for a narrow band of exemptions in section 15(1)(a)-(g) where state surveillance or the interception of communications would be permitted. Section 15 (2) also provides for equal adequate safeguards to those found in Principle 41 (3)(a)-(f), where a public exception to compliance with the bill is relied upon (for example, to conduct state surveillance for national security purposes).

Insofar as state surveillance and the privacy of communication online are concerned, it has been found that whilst the bill does not cater for such rights explicitly, the substantive and procedural aspects of the bill do indirectly provide protection against state surveillance and the interception of private communications online.

## Existence of other laws dealing with privacy and data protection online

There are a number of statutes which have an impact on privacy rights and personal data protection in Namibia:

### The Communications Act, 2009

This act[121] has drawn criticism as it allows the state broad powers to intercept communications without a warrant. The legislation therefore raises a number of concerns that it infringes

121 Communications Act 8 of 2009. https://laws.parliament.na/annotated-laws-regulations/law-regulation.php?id=136

the right to privacy as provided in Article 13 of the constitution[122]. The act provides that the intelligence agencies may surveil electronic communications and the only safeguard provided is Article 121(3) which provides that the state may not arbitrarily gain access to these communications.

Article 70 states that the director-general of the Communications Regulatory Authority of Namibia (CRAN) may designate a staff member from the National Central Intelligence Agency to serve as the head of interception centres. While the act provides, in Article 32, that the parliamentary committee on security has oversight over the agency's activities to prevent abuse, it is reported that the committee is not operational.[123]

## The Electronic Transactions Act, 2019

While the act[124] was passed in 2016, it has not been implemented and will only come into effect on the date gazetted. It is not certain when this may be expected. The act's objectives include the promotion and regulation of electronic commerce and the promotion of consumer protection in electronic commerce. However, it is difficult to envisage that these objectives could be properly realised without a broader personal data protection framework. The absence of dedicated data protection legislation may therefore undermine the objectives of consumer protection and the regulation of electronic commerce. An ideal regulatory framework would comprise robust data protection and ecommerce legislation to enhance the right to privacy and consumer protection while advancing and regulating the digital economy.

122 Privacy International. (2015). *The Right to Privacy in Namibia.* https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf

123 Ibid.

124 Electronic Transactions Act 4 of 2019. https://laws.parliament.na/annotated-laws-regulations/law-regulation.php?id=518&cid=19

Since 2005, Namibia has issued biometric identity cards for citizens and permanent residents and in January 2018, the government introduced biometric passports.[125] It is notable that these developments took place in the absence of a data protection framework. Medical aid schemes also utilise fingerprint technology to combat fraud and concerns were raised as the technology used was developed by South African countries. However, Namibians' sensitive personal data is vulnerable in the absence of a personal data protection framework. Namibia implemented the use of biometrics in voter registration[126] in 2013 and the potential for similar usage in the banking sector also represents a risk as Namibians do not enjoy legal recourse without the enactment of data protection legislation.[127]

Surveillance legislation has been an ongoing area of concern as evidenced by the UN's appeal to Namibia128 in April 2016, to reform its surveillance legislation and boost privacy protections.

An important component of this is the right to be anonymous online versus the presence of "real name" policies.

## Data protection practices in internet country code top level domain name registration

Privacy and data protection concerns have arisen for domain name registrations, particularly with the introduction of the

125 Mayhew, S. (2018, 8 January). Namibia makes the switch to biometric passports. *Biometric Update.com.* https://www.biometricupdate.com/201801/namibia-makes-the-switch-to-biometric-passports

126 Vrankujl, A. (2013, 20 December). Namibia unveils biometric machine for voter registration. *Biometric Update.com.* https://www.biometricupdate.com/201312/namibia-unveils-biometric-machine-for-voter-registration

127 Privacy International. (2015). Op. cit.

128 Privacy International. (2016, 31 March). UN calls on Namibia, New Zealand, Rwanda, South Africa, and Sweden to Reform Surveillance. Will the Governments Act? https://privacyinternational.org/news-analysis/661/un-calls-namibia-new-zealand-rwanda-south-africa-and-sweden-reform-surveillance

WHOIS protocol which allows a user to search for the owner of a domain name and their contact information.[129] The Internet Corporation for Assigned Names and Numbers (ICANN) is committed to "implementing measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information," subject to applicable laws.[130]

ICANN states that a discussion around the transfer of personal data inevitably impacts the operation of the WHOIS protocol.[131] This is especially true where a domain name registrant is in a different country to a domain name register, in order for the WHOIS protocol to resolve an enquiry, personal data such as a name and contact information would have to be transferred out of the registrants' country.[132] Cross-border personal data transfer regulations can however limit the type of information a WHOIS enquiry can return.

In 2015 ICANN adopted a Procedure of Handling WHOIS Conflicts with Privacy Law (which was revised in 2017).[133] This procedure requires a registrar that is subject to the ICANN registrar accreditation agreement to notify ICANN when that registrar is informed of any investigation or dispute arising out of the transfer of personal information following a WHOIS request.[134] The procedure further confirms that registrars are expected to comply with local laws by working alongside the relevant national government agencies.[135]

129 https://whois.icann.org/en/about-whois

130 https://whois.icann.org/en/primer

131 https://whois.icann.org/en/privacy

132 Ibid.

133 ICANN. (2017, 18 April) ICANN Procedure For Handling WHOIS Conflicts with Privacy Law. https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law

134 Ibid., Step 1.

135 Ibid., Step 1.4.

In Namibia, the absence of a data protection law can be interpreted to mean that there is no legal barrier to the disclosure of the name and contact information of a Namibian registrant. In its current form the Namibian Data Protection Bill provisions the regulation of cross border data transfers to international organisations and countries.[136] Under the bill, a WHOIS query from an international organisation such as ICANN would only be possible where "appropriate levels of protection are guaranteed".[137].

## Key stakeholders

The Ministry of Information and Communication Technology (MICT) is the primary government institution responsible for promoting the use and effective regulation of ICT services in Namibia.[138] While the ministry does not give express acknowledgement to all internet-related human rights, a stated strategic objective is to "enhance unhindered access to information for an informed nation."[139]

The Parliamentary Standing Committee on Information, Communication, Technology and Innovation acts as an oversight body to ensure that the MICT, among other ministries, is achieving its mandate. Additionally, the committee advises parliament on new legislation and policies that should be adopted to further ICT development in Namibia.[140]

The following organisations play a prominent role in data protection and privacy rights advocacy:

136 Data Protection Bill, 2020., s 41(1).

137 Ibid.

138 https://mict.gov.na

139 https://mict.gov.na/strategic-plan

140 https://www.parliament.na/index.php/committee-on-information-and-communication-technology-na

- Internet Society (ISOC): Since 2017, this non-profit organisation has been active[141] in Namibia. The organisation works to promote internet policy development with the aim to benefit society. ISOC Namibia also serves as a forum which represents many stakeholders active in the Namibian ecosystem.
- The Media Institute of Southern Africa (MISA) Namibia Chapter: MISA is an umbrella organisation which comprises national chapters in various SADC states. This civil society group focuses on advocacy regarding media freedom, freedom of expression and access to information as a means of advancing democracy in the SADC region.
- Namibia Media Trust: The Namibia Media Trust (NMT) is a civil society institution and non-profit organisation. It is a leading advocacy group which promotes media freedom and related issues and is concerned with regulation of the media (print, broadcast and online) in line with international best practices. In 2018, the NMT made submissions on the proposed Review and Amendment of Information and Communication Technologies (ICT) Policies and the Communications Act (the ICT review) which was conducted by the ITU and other parties as commissioned by the MICT. In its submissions on the ICT Review,[142] NMT commented on a number of pressing concerns, including media laws and policy which are beyond the scope of this study. However, it is significant that the NMT addressed data protection and privacy rights issues in the submissions.

  The NMT appealed to the government to secure people's personal data protection rights with regard to the internet. The NMT is of the view that the increased internet usage in the

141 https://isocnamibia.org

142 Namibia Media Trust. (2018). *Submissions on the ICT Policies and Communications Act Review.* https://www.nmt.africa/uploads/5be58699f3d58/NMTSubmission-2018ICTReview.pdf

daily lives of Namibians demands that the ICT review must include positive policy statements regarding personal data protection in any new ICT policy and legislation. The trust opined that this is also essential for economic development as European companies (which are important sources of direct foreign investment in Namibia) must uphold their clients' data protection rights in all transactions with Namibian companies under the General Data Protection Regulation.

The NMT requested that those responsible for the ICT review acknowledge the provisions of both the African Internet Rights Declaration and the AU Convention and incorporate key aspects of their personal data protection provisions in creating a Namibian Personal Data Protection Policy and subsequent legislation as part of the policy review. It was suggested that the Personal Data Protection Policy must be aligned with international best practices, including the African Internet Rights Declaration and the AU Internet Declaration. NMT added that it is vital that any policy and legislation will uphold the personal data protection rights of Namibians and also of those transacting with Namibians. The submissions also stated that in relation to ICT, the rights to freedom of expression and access to information are sacrosanct.

- NamIGF: Namibia has a national Internet Governance Forum (NamIGF) that seeks to raise awareness for internet governance issues as well as influence the public policy making process concerning internet regulation.

The following bodies are the key institutions involved in the development and future implementation of the new Data Protection Bill:

- Council of Europe and Commonwealth Secretariat

- The Ministry of Justice
- Parliamentary Standing Committee on ICT and Innovation
- Ministry of Information and Communication Technology
- Ministry of Education, Arts and Culture.

Considering Namibia has not yet passed the Data Protection Bill into law, there is no data protection authority.

## Perspectives and lessons from interview respondents

Namibian interview respondents' profiles were as follows:

- First respondent: Data protection expert and private sector stakeholder.
- Second respondent: Research associate and public policy advocate.
- Third respondent: Government official.
- Fourth respondent: Data protection expert and academic.
- Fifth respondent: Journalist, researcher and civil society advocate.

## Need for data protection law in Namibia

State surveillance: The second respondent noted that the lack of a data protection law in Namibia presents an unregulated state surveillance environment. According to this respondent, the average Namibian consumer is largely unaware of the implications of state surveillance on privacy, the extent to which personal information is accessed by state organs or the conditions of access. This concern is heightened considering that both major telecoms operators in Namibia are state owned. The second respondent's ongoing

research suggests widespread state surveillance in Namibia. Data protection is needed to prevent intrusive state surveillance. The second respondent finally pointed to the intent of the Namibian government to implement part 6 of the Communications Act that extends the interception powers of the state as the case for the data protection law to be effected with urgency.

Potential social media offences: Respondents signalled their observations of increased calls from the government to regulate social media abuse as indicative of the intent to introduce potential social media offences. The government's concerns, in the second and fifth respondents' opinion, related to public (online) criticism of the government and in particular, government officials. Prosecutions would rely on access to the contact information of the critics and data protection regulation is needed to ensure that personal information is disclosed under legitimate and authorised circumstances.

## Barriers to data protection law in Namibia

Adequate stakeholder engagement: The data protection expert and first respondent voiced concerns over the adequacy of stakeholder engagement and participation in the current drafting process of the new Data Protection Bill. These concerns largely stem from the logistical difficulties of holding meaningful stakeholder engagement sessions during the COVID-19 pandemic. Stakeholder consultations underway are poorly attended and the first respondent expressed concern for the detail of the written submissions that have been requested.

Delays in operationalisation: Respondents expressed concerns that, if promulgated, the data protection legislation may not be operationalised in the short term, pointing to other recently

enacted legislation that is not fully operational, such as the Whistleblower Protection and Witness Protections Acts of 2017 that have not been implemented despite a clear need for such legislation, and Article 144 of the constitution that binds to a number of international human rights instruments that endorse access to information as a fundamental human right. These include, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the African Charter on Human and Peoples' Rights (ACHPR). Respondents pointed to the Access to Information Bill, recently tabled in parliament following years of lobbying.

## Data protection implementation challenges

The fourth respondent indicated that the costs of establishing a DPA and the professional skills and experience in data protection regulation for a dedicated executive function may prove prohibitive in Namibia. The fourth respondent proposed that rather than establishing a new independent data protection authority, the mandate to investigate data protection violations and oversee the implementation of data protection law in Namibia should rest with the ombudsman.[143] A proposal to expand the mandate of the communication regulator, CRAN, to include data protection investigations, presents a conflict of interest as well as jurisdictional challenges. CRAN's current mandate includes assisting law enforcement to process information requests under the Communications Act through SIM registrations: should CRAN's mandate be expanded to include data protection, the question arises as to whether CRAN will be conflicted when assisting law enforcement while simultaneously ensuring the protection of personal information and the right to privacy. The fourth respondent indicated a flawed argument in a recommendation

143 Interview with fourth respondent, 2 October 2020.

that expanding CRAN's mandate to include data protection would be financially prudent. Following a Supreme Court ruling,[144] CRAN is no longer allowed to utilise regulatory levies in a manner not directly associated with defraying the expenses incurred by CRAN as the Communication Regulator. The effect is that costs incurred in regulating the protection of personal information cannot be expensed to CRAN's communications regulatory levies. Lastly, the respondent cautioned that expanding CRAN's mandate to include data protection presents a significant concentration of regulatory powers under one body.

The fourth respondent recommended the office of the ombudsman as ideally suited to receive an expanded mandate to protect personal information and the right to privacy. The ombudsman's current mandate is general public protection and broadly includes the promotion and protection of human rights. The ombudsman does not have any jurisdictional concerns or conflicts of interest when regulating personal information and privacy. The fourth respondent emphasised that the ombudsman is the only office that has the power to conduct investigations into abuse of power by law enforcement and the central intelligence services and that expanding the mandate to cover matters of interception and information requests following the introduction of a data protection law and the impending implementation of part 6 of the Communications Act is a natural fit.

Expanding the mandate of the office of the ombudsman would also empower it to conduct investigations into the telecoms operators themselves with considerably more independence that CRAN would have as there are no areas of conflict.

144 https://namiblii.org/na/judgment/supreme-court/2018/18

## Concluding observations and recommendations

Namibia recognises the right to privacy as a fundamental human right under Article 13 of the Namibian constitution. Accordingly, Namibians have a right to privacy in their homes and communications. This report suggests that the Namibian Data Protection Bill, 2020, is a positive step towards realising data protection rights for Namibians and conferring obligations to safeguard the personal data of Namibian citizens. The proposed establishment of a supervisory authority and specific identification of powers to receive and investigate complaints is welcomed as a positive step to the realisation of rights of privacy and privacy online.

From the analysis above, there is a notable and commendable effort in the Data Protection Bill to harmonise with several instruments. There is, however, the potential for further alignment and indeed closer inspection of the text of the bill against recommendations in the regional and sub-regional instruments to improve its coverage of data protection rights.

From a human rights perspective, the drafting and consultation process underway must include a wide range of stakeholders for adherence to the human rights-based approach principle of “participation” and Namibia must ensure that multistakeholder inputs are incorporated.

Further, in the context of the human rights-based approach to data protection, it would be crucial that the oversight function for the Data Protection Bill (supervisory authority) is adequately empowered to assess the bounds of state surveillance. A proposal to expand the communication regulator, CRAN’s mandate to include data protection investigations would present a conflict of interest as well as jurisdictional challenges. Accordingly, if Namibia

cannot establish a separate authority, the country may consider appointing the ombudsman as the supervisory authority.

A narrow band of exemptions is provided in the bill where state surveillance or the interception of communications would be permitted. Adequate safeguards are still required where these are relied upon (for example, to conduct state surveillance for national security purposes). The application of both the substantive and procedural aspects of the bill must balance powers of state surveillance and the interception of communications against rights to privacy and data protection.

A notable gap in the bill is that whilst it provides for sanctions and penalties, in its current draft form it does not list any such penalties, despite providing a placeholder for penalties. For effective enforcement and to deter violators, the bill must provide for penalties.

Ultimately, however, Namibia's data protection law must be passed, must be operationalised, and must be effectively governed to offer the assurance of privacy redress for Namibian citizens.

# Nigeria

Fola Odufuwa

## Executive summary

The practice of privacy and data protection is nascent in Nigeria. Although there is currently no comprehensive law on personal data protection, such protection has evolved over the past decade from passing references in general, sectoral or thematic legislation which were hardly enforceable until January 2019 when the National Information Technology Development Agency (NITDA) issued the country's first, single-document National Data Protection Regulations (NDPR). This watershed regulatory move came about under strong influence from continental regulations such as the African Union Convention on Cyber Security and Data Protection (2014), often referred to as the Malabo Convention, and international best practices particularly the operationalisation of the General Data Protection Regulation (GDPR) by the European Union in 2018.

The lack of specific regulatory coverage for data protection over the years has meant that individuals have little or no protection against the abuse of personal data by data processors. The move to create an all-encompassing data protection law is to correct chaotic data protection practices in the country. Arising from these realities and the groundswell of public opinion pointing out key deficiencies in the NDPR, the presidency through the National Identity Management Commission (NIMC) published a draft Data Protection Bill (draft bill) in August 2020 to establish an independent Data Protection Commission that will impartially regulate the processing of personal data, oversee data processors and controllers, and generally enforce the new legislation when passed into law. The draft bill, while not perfect, contains vital provisions that are likely to improve data privacy and security in the country and restrain harmful data practices or abuse of data by data controllers and processors.

The draft bill is being developed according to the human rights-based approach and conforms to international data protection regulations including the Malabo Convention, the ECOWAS Supplementary Act on Personal Data Protection of 2010, AU/ ISOC Personal Data Protection Guidelines for Africa and the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa. The main outcome of this study is that the Nigerian government needs to continue its drive towards a free society by sustaining its regional and international commitments on privacy and data protection and strengthening the legal and regulatory framework relating to these and other fundamental rights and freedoms. The state also needs to harmonise the views of stakeholders, private sector actors and development partners in completing the drafting of the proposed data protection legislation, take further action to raise public awareness on data privacy and security

from a human rights perspective and undertake to put an end to privacy rights and data protection infringements and violations.

## Methodology

On 18 September 2020 the Association for Progressive Communications (APC) engaged Fola Odufuwa (this researcher) to provide research expertise in assessing the state of privacy and data protection in Nigeria. The main objective of the study is to provide an in-depth rights-based analysis of the status of privacy and data protection of the country with a view to fostering a rights-based approach in furtherance of the African Declaration on Internet Rights and Freedoms (AfDec).

In compliance with the terms of reference and the research template, the researcher:

- Retrieved and reviewed relevant materials on the subject of privacy and personal data protection in Nigeria, such as legislation, regulations, scholarly reports, research journals and informed commentary. This activity also entailed reviewing pertinent publicly available materials from recent research carried out on behalf of United Nations and Africa Union Commission on the subject.
- Analysed materials retrieved in the task above to draw out the main themes and issues as would be consistent with the research template. He also identified any applications of the human rights-based approach to the development of existing data protection regulation and proposed legislation.
- Arising from the results of the first two tasks, he sought out the expert views of four knowledgeable in-country stakeholders who provided clarity on observed gaps in

regulation, legislation and the data protection environment. These individuals are:

  - Mary Uduma (chairperson, Nigeria Internet Governance Forum)
  - Gbenga Sesan (Paradigm Initiative)
  - Bidemi Olumide (Taxaide Technologies)
  - Olu Teniola (president, Association of Telecommunications Operators in Nigeria).
- Drafted the research report for the review of the APC team based on all the research activities described above.

This Nigeria country report contains the findings and recommendations at the conclusion of the consultation.

## Country context

As mentioned, the practice of privacy and data protection is nascent in Nigeria. Alhough there is currently no comprehensive law on personal data protection, data protection has evolved over the past decade from passing references in general, sectoral or thematic legislation which were hardly enforceable until January 2019 when the NITDA issued the country's first data protection regulations. NITDA is empowered by law to regulate information technology practices, electronic governance and the use of electronic data interchanges.[1]

This watershed regulatory move came about under strong influences from continental regulations such as the African Union Convention on Cyber Security and Data Protection (2014), often referred to as the Malabo Convention, and international best

1 NITDA. (2007). National Information Technology Development Agency Act 2007 Act No. 28.

practices particularly the operationalisation of the GDPR by the European Union in 2018. The fear of the country being locked out of commercial transactions with the European Union was also a driver of the data protection regulation. The framework gives practical force to constitutional privacy rights of citizens as the national government seeks to eliminate the processing of personal data of Nigerian citizens by "unauthorised persons without any lawful basis."

The need for consolidated data protection regulation has generally been widely acknowledged. For instance, one research report identified chaotic data protection practices in the country as at 2018 including wrong uses of collected information; lack of consent or even enquiry by data subjects regarding the use of their data; lack of transparency by state agencies; exposure of minors and children to privacy risks; and the absence of personal data protection rights and the ability to enforce those rights.[2]

The lack of specific regulatory coverage for data protection over the years has meant that individuals have little or no protection against the abuse of personal data by data processors.

Probably arising from these realities and the groundswell of public opinion pointing out key deficiencies in NITDA's 2019 regulations, the presidency, through the National Identity Management Commission (NIMC), published a draft bill[3] in August 2020 to establish an independent Data Protection Commission that will be responsible for the protection and regulation of personal data in the country. The core institutions driving data protection regulation in the country are the Federal Ministry of Communications and the Digital Economy (FMCDE),

2 Izuogu, C. E. (2018). *Personal Data Protection in Nigeria.* World Wide Web Foundation. https://webfoundation.org/docs/2017/12/Personal-Data-Protection-in-Nigeria.pdf

3 The first iteration of this bill is traced back in the literature to its initial presentation at the National Assembly in 2015. https://im-migration.gov.ng/draft-data-protection-bill-2020

NITDA, NCC, NIMC, Central Bank of Nigeria (CBN), and the Federal Ministry of Justice. The draft bill is said to be “working its way” back to parliament though it is unknown if, when and in what form it will eventually be passed.

## Constitutional underpinning

Privacy rights and data protection are enshrined in the Nigerian constitution. Section 37 states that “the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.”[4] However, while privacy and data protection are perfunctorily provided for in the constitution, prior to 2019 there was no regulatory mechanism by which citizens could practically claim or enforce these rights outside of the judicial system especially when they involve electronic data. While case law is said to be rife with privacy enforcement action and claims relating to physical spaces as homes, offices or personal freedoms, until recently there is negligible judicial activity when it relates to data privacy rights or personal data protection.[5] One successful enforcement of telephone privacy at the appellate court is said to have involved Etisalat, a mobile network operator in the country, taken to court by a private individual for the invasion of his data privacy through unsolicited SMS messages that were sent to his mobile by third parties in violation of Section 37.[6] The Federal Appeal Court upheld the judgement of the lower court in awarding damages of 8 million Nigerian Naira (USD 21,052) against the mobile network.[7]

4 https://wipolex.wipo.int/en/text/179202

5 Babalola, O. (2019). Emirates Telecommunications: Data Protection and Privacy Challenges in Nigeria (Legal Issues). Lecture delivered at the Nigerian School of Internet Governance, Lagos, Nigeria, 9 July. https://www.marketscreener.com/quote/stock/EMIRATES-TELECOMMUNICATIO-9059303/news/Emirates-Telecommunications-Data-Protection-And-Privacy-Challenges-In-Nigeria-Legal-Issues-30129496

6 Ibid.

7 Exchange rate of NGN 380 to USD 1.00.

## Existence of other laws dealing with privacy and data protection online

There are sectoral-specific privacy and/or data protection provisions in a number of recent legislations (Table 1). However, these provisions were neither adequate nor effective in ensuring widespread compliance and none imposed sanctions in the event of a breach of privacy or data protection rights.

**Table 1.**

**Sector-specific regulations governing privacy and data protection**

| Legislation or regulation | Regulator | Date | Purpose |
|---|---|---|---|
| Nigeria Data Protection Regulation8 | National Information Technology Development Agency | 2019 | Framework for digital rights, privacy and data protection |
| Federal Competition and Consumer Protection Act9 | Federal Competition and Consumer Protection Commission | 2019 | Regulations governing fair trade, competitive practices and for consumer rights including privacy and data protection |
| Credit Reporting Act | Central Bank | 2017 | Framework for credit reporting and regulation of credit bureaux |
| Consumer Protection Framework10 | Central Bank | 2016 | To ensure that consumers of financial services are protected and treated fairly by banks and financial institutions |
| Cybercrimes (Prohibition, Prevention, Etc) Act11 | National Security Advisor | 2015 | Framework dealing with cybercrimes, data protection, IP and privacy rights |
| National Health Act12 | Federal Ministry of Health | 2014 | Provides privacy rights, data protection and obligations for healthcare users and healthcare personnel |

8 https://ictpolicyafrica.org/api/documents/download?_id=5eb9686c7c7814001bc4ca8b

9 https://placng.org/i/wp-content/uploads/2019/12/Federal-Competition-and-Consumer-Protection-Act-2018.pdf

10 http://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20(final).pdf

11 http://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

12 http://nigeriahealthwatch.com/wp-content/uploads/bsk-pdf-manager/2018/07/01_-Official-Gazette-of-the-National-Health-Act-FGN.pdf

| | | | |
|---|---|---|---|
| Registration of Telephone Subscribers Regulations13 | Nigerian Communications Commission | 2011 | Regulatory framework for the registration of mobile subscribers |
| Freedom of Information Act14 | Attorney General | 2011 | Access to public records, privacy and data protection |
| National Identity Management Commission Act | National Identity Management Commission | 2007 | Framework for national digital identity systems |
| Child Rights Act | | 2004 | Guarantees privacy rights of children and minors |

## Regional and international commitments on privacy and personal data protection

Nigeria signed the communique adopting the African Union Convention on Cyber Security and Personal Data Protection at the 23rd Ordinary Session held in Malabo, Equatorial Guinea in June 2014. The Malabo Convention encourages African governments to legislate cybersecurity, protect the electronic data of their citizens and promote electronic interchanges on the continent. Though Nigeria is yet to ratify the Convention as at 18 June 2020[15] and the convention does not have the force of law either within the country or on the continent, the national government has nevertheless been taking steps towards privacy and data protection prior to and since the adoption of the Convention.[16]

In 2019 the government published the country's first-ever overarching data protection framework: Nigeria Data Protection

13 https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file

14 http://www.cbn.gov.ng/FOI/Freedom%20Of%20Information%20Act.pdf

15 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

16 Though not directly relevant to this data protection report, Nigeria is one of seven African countries to sign and ratify the Budapest Convention on Cybercrime, which provides guidelines for the establishment of effective rights-respecting national criminal justice systems. See: Akinola, K. (2018, 26 April). Nigeria looks beyond border in cybercrime push. *Technology Times*. https://technology-times.ng/nigeria-looks-beyond-border-in-cybercrime-push; Turianskyi, Y. (2020). *Africa and Europe: Cyber Governance Lessons. South African Institute of International Affairs*. https://www.africaportal.org/publications/africa-and-europe-cyber-governance-lessons

Regulation (NDPR). This is a flagship regulation of the Nigerian government as it comes under the pillar of development regulation, the first of eight adopted when President Muhammadu Buhari launched the National Digital Economy Policy and Strategy (NDEPS 2020-2030) in November 2019. Since 2010, a form of the data protection bill has been making its way through parliament but the latest version gained momentum early in 2020 when the government set up a working group to reform legislation relating to the digital economy. Both the NDPR and the proposed draft bill conform to Article 8 of the Malabo Convention which encourages the strengthening of "fundamental rights and public freedoms, particularly the protection of personal data, and [the punishment of] any violation of privacy without prejudice to the principle of free flow of personal data."[17] Though the Nigerian government has a poor reputation for upholding basic human rights and freedoms of its citizens in practice even when enshrined in law, there are hardly any known instances of direct detractions by the government from the data protection principles of the Malabo Convention.

Nigeria is also a signatory to the Supplementary Act on Personal Data Protection within ECOWAS adopted by the 15 member states of the Economic Community of West African States in 2010. The act, which was the first and only binding international data protection law in Africa,[18] creates a requirement for West African states to establish a legal framework for privacy and the protection of personal data. However, Nigeria is the sole remaining member state yet to establish national data protection legislation.[19]

17 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

18 Shyllon, O. (2017). *The Right to Privacy and the Protection of Personal Information in Africa: Challenges and Prospects.* Centre for Human Rights, University of Pretoria. https://aanoip.org/wp-content/uploads/2018/07/Privacy-and-Data-Protection-IB-Dec-2017.pdf

19 http://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf

## Existence of a comprehensive data protection law

Data protection in Nigeria is presently governed by the Nigeria Data Protection Regulation (NDPR) of 2019, established by the NITDA. This set of regulations covers and controls the use of data by private corporations, public sector ministries, departments and agencies and non-profit organisations, imposing obligations, penalties and sanctions on them for any privacy and data protection violations. It appears to have evolved from the NITDA's Draft National Guidelines on Data Protection of 2013 which deals with the processing of personal data but which was not implemented. In 2017 the agency published the draft regulations and solicited comments from stakeholders and the general public.[20] Though NITDA is empowered by law to make regulations on privacy and data regulations, NDPR is not an act of parliament so it does not have the full weight of the law. While NDPR establishes NITDA as a National Data Processing Officer, there is intense debate among legal practitioners whether NITDA has the statutory power to make itself an independent data protection authority for the country.

In August 2020, the national government published a draft Data Protection Bill which seeks to correct these twin issues (plus other NDPR deficiencies) and sought input from stakeholders and the general public.[21] The effort at regulatory reform is being driven on behalf of the Presidency by the Legal and Regulatory Reform Working Group of the Digital Identity Ecosystem Project which consists of representatives of the Ministry of Justice, FMCDE, NIMC, NITDA, NCC, National Population Commission, NIS, Office

20 These older iterations of the regulation were advisory in nature as they had no enforcement provisions. See: Izuogo, C. (2018, 21 October).Whiter the NITDA data protection guidelines 2017? *African Academic Network on Internet Policy.* http://aanoip.org/whiter-the-nitda-data-protection-guidelines-2017

21 OneTrust DataGuidance. (2020, 20 August). Nigeria: NITDA publishes draft Data Protection Bill 2020 for public comments. http://www.dataguidance.com/news/nigeria-nitda-publishes-draft-data-protection-bill-2020-public-comments

of the Secretary to the Federal Government and the Independent National Electoral Commission (INEC). The Working Group is tasked with upgrading the regulatory framework for identity management in the country.[22]

Prior to NDPR, data protection was not institutionalised and there was no specific authority with responsibility for the regulation and administration of privacy and data protection in the country. Sector-specific regulatory actions bordering on privacy and data protection were carried out by the Central Bank, NITDA and the Nigerian Communications Commission, agencies of government which took an early lead in the promotion of digital rights and in ensuring that their respective licensees are privacy-respecting and data-protection compliant. According to one research source, the banking industry, telecommunications, and oil and gas are the economic sectors with the most progressive data protection practices.[23]

In spite of the absence of data protection legislation, public and private sector organisations continue to collect personal data including biometrics from citizens and residents. National databases featuring biometrics include the SIM Registration (NCC), National Identity Number (NIMC), Voters Card (INEC), Bank Verification Number (CBN), Tax Identification Number (FIRS), Passport Information (NIS), to name a few. NIMC is currently implementing a government mandate to consolidate these national databases. Civil society groups continue to mount a strong opposition to the inadequate data privacy and data protection environment and bodies including Paradigm Initiative, Digital Rights Lawyers Initiative, among others,

22 Nasiru, J. (2020, 14 September). FG: Data protection law will help us gain trust of Nigerians. *The Cable.* http://www.thecable.ng/fg-data-protection-law-will-help-us-gain-trust-of-nigerians

23 ICSAN Lagos Chapter. (2020, 17 June). Nigerian Data Protection Regulation (“NDPR”) 2019: Compliance and Handling of Data Breaches. https://www.youtube.com/watch?v=7y0Cj7t6tXI

have taken ministries, departments and agencies including NITDA and major private players such as Facebook to court to challenge, in one instance, the legality of the NDPR or specific sections of existing laws and regulations in the light of known violations of privacy rights.

The draft Data Protection Bill was presented for public input in August 2020 and is said to be undergoing an internal review by the responsible working group to improve vague words or inelegant phrases and to further enhance the principles and best practices of data protection upon which it is developed. CSOs are relatively confident that the revised draft will significantly improve on and correct the deficiencies of the NDPR and further build on human rights gains, though this can only be found to be so (or not) when the new draft is eventually unveiled.

## Key features of the comprehensive data protection law

### Main features of NDPR and draft Data Protection Bill

The Nigeria Data Protection Regulation 2019 is a subsidiary legislation and has enforcement limitations by default. Though the NITDA adopted a less-bureaucratic regulatory framework and involved stakeholders and the general public in bringing the document together, the weaknesses inherent in NDPR are driving the quest to adopt a new Data Protection Bill which will establish the Data Protection Commission to impartially regulate the processing of personal data, oversee data processors and controllers, and generally enforce the new legislation when passed into law. The draft bill, while not perfect, contains vital provisions that are likely to improve data privacy and security in the country and restrain harmful data practices or abuse of data by data controllers and processors.

## *Principles*

The NDPR is largely modelled after GDPR and was developed to assist organisations in Nigeria to ultimately comply with the European data protection framework.[24] Although there are 62 similarities between the two documents, there are 76 differences, according to one research study.[25] The NDPR is based on six principles which underpin how personal data should be handled (Table 2).

**Table 2.**

**Governing principles of the NDPR[26]**

| | Principle | NDPR provision |
|---|---|---|
| **1** | Lawfulness and legitimacy | Art. 2.1 (1a) Personal data collected and processed must be legitimate and for lawful purpose. |
| **2** | Specific purpose | Art. 3.1 (7c) Controller to inform Subject of purpose of collection. |
| **3** | Accuracy | Art. 2.1 (b) processed PD shall be adequate and accurate |
| **4** | Storage and security | Art. 2.1 (c) PD shall be stored for the period only for the period they are reasonably required to so do.<br>Art. 2.1 (d); 2.6 Onus of Security lies on the Controller |
| **5** | Confidentiality, integrity and availability | Art. 3 enumerates the rights of a data subject. The principles of information security mangement which includes CIA are all covered. |
| **6** | Compliance and enforcement | Art. 4.1 (4) DPCO are licensed to aid Compliance. Enforcement would be done by NITDA upon default by Controllers and Administrators. |

The draft bill adopts the first five principles in Table 2 above as the legal basis for the processing of personal data but adds a couple more: processing – personal data must be processed

24 Ibid.

25 OneTrust DataGuidance. (2010, 14 April). Comparing privacy laws: GDPR v. Nigeria Data Protection Regulation. https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-nigerian-data-protection-regulation

26 Daniel, O. (2019). NDPR: Overview and Business Implications. Presentation by NITDA Desk Officer – NDPR at Taxtech Awareness Seminar, Lagos, Nigeria, September. http://taxtech.com.ng/download/NDPR-Overview-and-Business-Implications-by-Olufemi-Daniel-Desk-Officer-NDPR.pdf

in a manner that ensures "appropriate security of the personal data, including protection against unauthorised or unlawful processing;"[27] and the principle of identification – "personal data must be kept in a form that permits identification of data subjects for no longer than is necessary."[28] The draft bill omits the licensing of data protection compliance organisations as a compliance and enforcement principle or mechanism and does not provide for the continued administration of the NDPR.

### *Key definitions*

The NDPR is designed to safeguard the data rights of natural persons of Nigerian descent, whether resident in the country or not, create a trusted environment for safe electronic exchanges of personal data and generally lift the country's human rights rating and overall global competitiveness. The regulation defines six stakeholders in the data protection ecosystem as follows:

**Table 3.**

**Key definitions of NDPR and draft Data Protection Bill**

| Definition | NDPR | Draft Bill |
|---|---|---|
| **Data subject** | Any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity | Identified or identifiable living natural person to whom personal data relates |
| **Data controller** | An entity that determines the purposes for and the manner in which personal data is processed | Natural or legal person or body which has decision-making power concerning the purposes and means of data processing |
| **Data processor** | Not defined but NITDA references "person or organisation who processes data" | Natural or legal person or body which processes personal data on behalf of the data controller |

27 Section 3(a)(g) of the draft Data Protection Bill.

28 Section 3(a)(h) of the draft Data Protection Bill.

| | | |
|---|---|---|
| **Data processing officer** | Employee of a large data controller | Not defined |
| **Data protection compliance organisation (DPCO)** | Organisation licensed by NITDA to carry out certain mandatory data protection services | Not defined |
| **Oversight** | National Information Technology Development Agency (NITDA) | Independent Data Protection Commission |

### *Data subject rights*

The rights of data subjects are comprehensively outlined in sections 2.1, 2.2, 2.3, 2.4 and 3.1 of the NDPR. The regulation specifies that personal data cannot be obtained except when the purpose for which the data is being collected is made known to the data subject.[29] Data subjects must give definitive consent and data processors are restricted from requesting consent for the "propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts."[30] Subjects are also to be assured of their privacy rights and the full security of their personal data. They can object to the processing of their personal data, withdraw consent from data processors at any time or request the complete erasure of personal data.[31] Data subjects are also to be informed whenever there is a change in the purpose for which personal data is being processed.

The draft bill also lays out synonymous data subject rights as the NDPR.[32] These include the right to be notified of data breaches affecting the subjects, right of access to personal data, right to rectification and erasure, right to be forgotten and the right to

29 NDPR Section 2.3.

30 NDPR Section 2.4.

31 NDPR Section 3.1.

32 Part V, Sections 17 to 25 of the draft Data Protection Bill 2020.

judicial remedy, among others. However, the proposed legislation further introduces the right to have data processing suspended and the right in respect of automated processing.

### *Conditions for lawful processing*

The NDPR and the draft bill both set out five similar conditions, at least one of which has to be met, before lawful processing of personal data can occur. These are: specific consent of data subject, contractual obligation involving data subject, legal obligation of a data controller, vital interest of data subject and public interest.

### *Relevant exemptions in the public interest*

Both the NDPR and the draft bill specify only one exception from the direct consent of a data subject – whenever data processing is necessary for "archiving, scientific research, historical research or statistical purposes for public interest." However, the regulation does not provide a definition or interpretation of scientific or historical research and it is possible that this clause may be misused.

### *Breach notification requirements*

The NDPR does not specifically provide for data breach notification. However, the NITDA has the power to set up an administrative redress panel to investigate allegations of any data breach. The draft bill, on the other hand, specifies that data subjects have to be informed within 48 hours of the Data Protection Commission being notified of any breach of their personal data.[33]

33 Section 17 (3) of the draft Data Protection Bill.

### *Cross-border data transfers*

Under the NDPR, transfer of personal information to another country can occur if the NITDA has approved the country as having an adequate level of data protection.[34] In such a case, data controllers must show proof of consent, transmit an overview of their data encryption method and conduct the data transfer under the supervision of the country's attorney general. Exceptions include the voluntary consent of the data subject to the proposed transfer, contractual obligation, public interest, legal claims or vital interest of the data subject.[35] The draft bill also contains similar provisions that regulate the trans-border interchange of personal data but with the bottleneck of having to carry out any transfer under the supervision of the attorney general eliminated.

### *Other relevant features*

The NDPR also contains a grey area: the matter of data localisation. Section 2.11 of the regulation recognises the need for, and does allow, cross-border data exchanges under certain conditions. However, this appears to be at variance with the agency's guidelines for Nigerian Content Development in Information and Communication Technology (ICT) of 2019,[36] which stipulate that electronic data must be hosted on local servers within the country. Sections 11.1.4 and 12.1.4 of the guidelines specifically direct telecommunications operators and networking service companies to "host all subscriber and consumer data within the country in line with existing legislation." Furthermore, Section 13.1.2 mandates data

34 NDPR Section 2.11.

35 NDPR Section 2.12.

36 http://nitda.gov.ng/regulations

management players to “host all sovereign data locally within the country and shall not for any reason host any sovereign data outside the country without an express approval from NITDA.”

### *Enforcement*

In December 2019, the agency issued non-compliance notices to 100 companies in aviation, betting and financial technology for failing to submit data audit reports which were due by 25 October 2019.[37] The regulator also began investigating alleged cases of data breaches involving a number of organisations including the Lagos State Inland Revenue Service,[38] Truecaller,[39] and Nigeria Immigration Service.[40] Altogether, the NITDA’s actions in enforcing the NDPR have alerted private and public sector organisations to the stringent penalties, expensive costs and reputational damage which would be brought about by non-compliance with the regulations. Due to the COVID-19 pandemic, enforcement has been slower and the agency has twice moved the deadline for the submission of data audit protection reports by data processing organisations from 15 March to 30 June.[41]

## Data protection authority (DPA)

Since NDPR took off in March 2019, NITDA as the responsible authority for data protection in Nigeria has been quite busy implementing data protection regulations in the country. It has

37 Communications Week. (2019, 13 December). NITDA to Issue Notices of Data Protection Non-Compliance to 100 Firms. *Communications Week*. http://www.nigeriacommunicationsweek.com.ng/nitda-issues-100-firms-data-protection-non-compliance-notice/

38 Olalekan, F. (2019, 28 December). LIRS under investigation after dumping taxpayers’ data online. *Nairametrics*. https://nairametrics.com/2019/12/28/lirs-under-investigation-after-dumping-taxpayers-data-online

39 Paul, E. (2019, 25 September). NITDA investigating alleged privacy breach by Truecaller. *Techpoint.africa.* https://techpoint.africa/2019/09/25/nitda-truecaller-privacy-breach

40 Okedara, S. (2019, 28 June). Nigeria Immigration Service and the Burden of Data Protection. *Global Freedom of Expression.* https://globalfreedomofexpression.columbia.edu/updates/2019/06/nigerian-immigration-service-and-the-burden-of-data-protection/#:~:text=On%20Friday%20July%2012%2C%202019,NITDA%20came%20from%20various%20fronts

41 Andersen Tax. (2020, 12 May). NITDA Further Extends Deadline for Filing of Data Protection Audit Report to 30th June 2020. https://andersentax.ng/nitda-further-extends-deadline-for-filing-of-data-protection-audit-report-to-30th-june-2020

licensed 72 data protection compliance organisations (DPCOs) to monitor, audit, conduct training and implement data protection compliance for data controllers in the country. As at September 2020, the country now has a national database of statutory audit reports filed by 635 entities[42] from near zero compliance. Within the first year, the NITDA has issued 230 compliance and enforcement notices and investigated 15 data breaches. A web portal was launched for the filing of audit reports and reporting of breaches by members of the public and a data breach investigation team was set up in conjunction with the inspector general of police.[43]

However, despite initial regulatory successes, the NDPR did not create an independent data protection authority and NITDA's role as a national data protection officer was not defined in the regulations. To further institutionalise the privacy rights and data protection regulatory space, the draft Data Protection Bill stipulates the creation of a new, independent data protection commission as the national authority responsible for protecting personal data and regulating the processing of personal information by data controllers and data processors. This commission will promote public awareness of data rights. It will also have powers to investigate breaches of data rights and take enforcement actions in line with the new law. On the downside, civil society advocates have pointed out that the composition of the governing board of the commission is heavily skewed in favour of representatives of government in the ratio 12 of 16,[44] a structure which may prevent the full impartiality of the new regulator.

42 NITDA. (2020). *Nigeria Data Protection Regulation Performance Report 2019-2020.*

43 Ibid.

44 Paradigm Initiative & NetRights Coalition. (2020). *Comments on Nigeria Draft Data Protection Bill 2020.* https://cpj.org/wp-content/uploads/2020/09/PIN-Memo-on-draft-DPB.docx.pdf

NITDA's role and involvement as the current regulator of data protection has been the subject of a number of court cases instituted by various civil society groups including Laws and Rights Awareness Initiative, Digital Rights Lawyers Initiative and Paradigm Initiative, among others. These cases are ongoing and relate mainly to breach incidents involving ministries, departments and agencies, e.g. NIMC and Lagos Inland Revenue Service, or private sector players including TikTok, Facebook and Truecaller with NITDA joined in as a co-defendant. The consultant is not aware of a legal challenge against the legality of the regulation.

## Organisations and associations involved in advocacy related to data protection

Civil society groups are the biggest advocates for privacy and data protection in Nigeria. In September 2020, The NetRights Coalition, which has over 100 civil society organisations and individuals including Paradigm Initiative, Digital Rights Lawyers Initiative, Media Rights Agenda, Committee to Protect Journalists, Premium Times Centre for Investigative Journalism, Knowledge House Africa and SafeOnlineNG, published the views and position of civil society on the draft Data Protection Bill.[45] The key issues raised with the proposed bill include:

- The need to secure the independence of the Data Protection Commission (DPC). In the proposed bill, the commission is dominated by representatives of government with no further oversight or accountability provided. Rights groups are advocating for a multi-stakeholder approach to the establishment of DPC with sufficient representation of private sector actors and civil society in addition to government.

45 Ibid.

- The need to specifically protect journalists and news agencies in fulfilling their duties. The NetRights Coalition also believes that numerous clauses in the bill (e.g. 4(2)(e), 3(1)(h), 20, 23, 25, 30, 35 and others) may be exploited by unscrupulous government officials to censor the content of journalists, restrict their ability to report freely, particularly when individuals are involved and retaliate against individual journalists or the media organisations that they work for.

The NetRights Coalition presented these matters to the working group through a position paper and at a validation workshop held in Abuja on 14 September 2020. Conversations with key informants during this consultation suggest that the government is taking the views of civil society seriously, though the final form of the draft bill that would be presented to the National Assembly is yet to be finalised. Civil society and members of the public would also have the opportunity to participate in public hearings when parliament commences considering the draft bill.

Public organisations that impact on data protection in some form and that are often the focus of civil advocacy groups when it comes to privacy and data rights infringements are the Central Bank, Nigeria Identity Management Commission, Nigerian Financial Intelligence Unit (surveillance), Economic and Financial Crimes Commission (cybercrimes and enforcement), Corporate Affairs Commission, National Population Commission, National Health Insurance Service, Nigeria Immigration Service, Nigeria Police Force and the Federal Inland Revenue Service, to list a few.

## Data protection practices in internet country code top level domain name (ccTLD) registration

The Nigeria Internet Registration Association (NIRA) is the not-for-profit registrar and administrator of the country code top level domain (ccTLD). Established by the presidency in 2006, NIRA develops policies and rules governing the operations of sub-level domain registries and promotes the use of the domain and the internet, among other functions. It runs the registry-registrar-registrant (3R) model in operating and managing the top-level domains. With respect to data protection, NIRA is said to have implemented GDPR-compliant privacy and data protection policies in 2019. However, a cursory search of NIRA's publicly available WHOIS database returns results that include unredacted personal data including cell phone records, email and physical address of contacts and hosts for sub-level domains.[46] While it may be possible that data subjects in this case gave consent for their personal data to be utilised or presented in this way, it is also possible that this is not the case. If proven, then the practice of publicly revealing personal data of .ng domain contacts may be a likely breach of the Nigeria Data Protection Regulation 2019. NIRA's privacy policy[47] does ensure that registration information is provided only on a voluntary basis and the policy does not require NIRA to redact personal data nor provide for any recourse in the case of a data breach.

## Analysis in line with AfDec and other relevant instruments

Nigerian laws generally conform to best practices and international conventions of human rights to a large degree. For instance, both the Nigerian Data Protection Regulation and

46 https://whois.nic.net.ng/whois.jsp

47 http://www.nira.org.ng/images/Policies/Nira_Privacy_Policy.pdf

the draft bill comply with Article 8 of the African Declaration on Internet Rights and Freedoms[48] (Table 4). The article stipulates that:

- Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her.
- Everyone has the right to communicate anonymously on the internet, and to use appropriate technology to ensure secure, private and anonymous communication.
- The right to privacy on the internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim.

**Table 4.**

**Objectives of NDPR and the draft Data Protection Bill**

| NDPR (Section 1.1) | Draft Data Protection Bill (Part 1, Section 1) |
|---|---|
| The regulation was developed to "safeguard the rights of natural persons to data privacy; foster safe conduct for transactions involving the exchange of Personal Data; prevent manipulation of Personal Data; and ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice." | Bill seeks to "establish and provide an efficient regulatory framework for the protection of personal data, regulate the processing of information relating to data subjects, and to safeguard their fundamental rights and freedoms as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999." |

The regulation and the draft bill also conform to the Malabo Convention[49] which mandates the commitment and respect of AU member states to fundamental freedoms and human rights

48 https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf

49 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

and the African Charter on Human and Peoples' Rights. The convention outlines six data protection principles (Article 13) to be adopted in formulating national legislations. These principles relate to consent and legitimacy; lawful and fair processing; purpose, relevance and retention of data; accuracy of data over its lifespan; transparency of processing, and confidentiality and security of personal data. The existing and proposed data protection regulatory documents are based on similar principles as the Malabo Convention with minor variations.

Furthermore, the regulation and the draft bill largely follow the framework described in the ECOWAS Supplementary Act on Personal Data Protection of 2010.[50] The act mandates member states of the economic community to "establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage and use of personal data without prejudice to the general interest of the State" (Article 2). The draft bill, unlike the regulation, further establishes an independent data protection regulator in line with Article 14 of the ECOWAS Act.

With respect to the AU/ISOC Personal Data Protection Guidelines for Africa[51] which recommend a multistakeholder model in the development of national data protection regulations and legislations, both the regulation and the draft bill received input from stakeholders, civil society groups and members of the Nigerian public. The two data protection documents are also built on the same principles as the AU/ISOC guidelines except for anonymity, pseudonymity and data minimisation which are neither specified nor provided for in the regulation and draft bill.

50 https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf

51 Internet Society & Commission of the African Union. (2018). *Personal Data Protection Guidelines for Africa*. https://www.internet-society.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

The regulation and the draft bill also conform to the privacy and protection of personal information provisions outlined in Sections 97, 99 and 100 of the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa.[52] However, neither the regulation nor the draft bill grant the "right to communicate anonymously or use pseudonyms on the internet" to data subjects in the country contrary to Section 98 of the declaration. The revised declaration was issued in draft form on 30 April 2019 by the Special Rapporteur on Freedom of Expression and Access to Information in Africa pursuant to Resolution 350 (ACHPR/ Res.350 (EXT.OS/XX) 2016) of the African Commission on Human and Peoples' Rights, and given how recent it is, it is unknown whether Nigeria has ratified the document.

In reviewing data protection literature relevant to Nigeria, the main recommendation to the state on its regional and international commitments on privacy and data protection from a variety of domestic and international bodies relates to reforming and strengthening the legal and regulatory framework. Nigeria is deeply engaged with the Universal Periodic Review (UPR) processes in further compliance with its regional and international commitments on privacy and data protection. A review of the third cycle was carried out in 2018 and a review of the subsequent UPR report[53] shows the country accepting over 280 recommendations including the "adoption of legislation that regulates the functioning of Nigeria's security agencies by limiting their powers, establishing oversight mechanisms consistent with international human rights standards and safeguarding the right to privacy" (UPR III. 148.33). The state also agrees to "take the necessary steps for the full implementation of the

52 https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf

53 United Nations Human Rights Council. (2018). UPR of Nigeria (3rd Cycle – 31st session): Thematic list of recommendations.

legislation related to the protection of human rights" (UPR III. 148.15) and "strengthen the implementation of its international obligations and cooperation with human rights protection mechanisms, in particular by reporting to all treaty bodies" (UPR III 148.20). Evidence of steps taken towards implementing UPR recommendations includes the reform of the national privacy and data protection regulatory landscape through the adoption of NDPR and the proposed legislation on data protection.

Additionally, both the NDPR and the draft bill are direct responses being taken by the country to update national data protection regulation and laws in line with the General Data Protection Regulation (GDPR). Since the operationalisation of GDPR, data protection has become a "hot topic" with policy makers, private sector actors, civil society groups and the general public and the establishment of NDPR in 2019 has further heightened awareness of privacy data rights across the spectrum of society.

As highlighted in this report, the national government is presently planning to replace Nigeria's Data Protection Regulation of 2019 with new legislation that addresses deficiencies identified in NDPR in order to improve the practice of privacy and data protection in the country. The main weakness of NDPR lies in limitations within the statute that established it. One, Section 6 of the NITDA Act makes the agency the regulator of electronic governance and electronic data exchanges. Following on from this, NDPR was developed to focus almost exclusively on data protection of electronic exchanges with almost no regulatory coverage for non-electronic data. Though this is yet to be judicially tested, if proven, the lack of coverage for physical data collection systems would seem to be a major omission in a society where many organisations continue to store private data on paper. While neither the NITDA Act nor NDPR have been tested in the courts regarding

NITDA's ability to regulate non-electronic data, there is a school of thought that the regulator was not established to regulate non-electronic data[54] and cannot therefore provide data protection regulations for paper-based filing systems.

Secondly, there is also an argument as to NITDA's statutory ability to make itself the country's data protection authority. Presently, there is no legislation in place that backs NDPR regulations. Altogether, Nigeria continues to face significant hurdles in its quest to build a rights-respecting society. The first is incorporating the country's commitments to international regulations, conventions, laws and norms especially as relates to human rights into national laws. This process has been slower than envisaged. The second is in ensuring the proper implementation of the laws as there is often a wide gulf between what the law says and what state actors do in practice.

## Analysis of the status of a human rights-based approach to personal data protection in the country

Nigeria has been cooperating with the international human rights system of the United Nations, African Union and other international bodies to protect and promote human rights in the country. As noted in the previous section, Nigeria has participated in three universal peer review cycles so far and is preparing for the fourth cycle due in 2021. Actions in the promotion of human rights undertaken by the national government include the ongoing development of the National Action Plan and Guiding Principles on Business and Human Rights, implementation of gender equality reforms through the establishment of the Committee on the Convention on the

54 Scott, B., & Eke, S. (2020). *NITDA's Power to Regulate Non-Electronic Data.* http://www.spaajibade.com/resources/nitdas-power-to-regulate-non-electronic-data-bisola-scott-and-sandra-eke/

Elimination of All Forms of Discrimination against Women in 2017; consistent cooperation with the International Criminal Court and respect for the rule of law and human rights.[55] According to the UN report, the challenges to the upholding of human rights in Nigeria can be attributed to the plurality of ethnicities, disparate legal systems, corruption, weak internal security and enforcement, and cultural practices and mindsets.[56]

In evaluating the country's adherence to a human rights-based approach, we apply this approach to the two regulations on personal data protection – NDPR and the draft bill:

## Participation

The evolution of NDPR and the draft bill have involved the active participation of public and private sector, development organisations, not-for-profit groups and civil society and members of the public. Though NDPR does not directly grant data subjects the right to fully participate in decisions that affect the enjoyment of their rights, the draft bill does. Section 6 (1) of the draft bill stipulates that "every data subject has the right to be informed about the processing of his personal data". The draft bill also grants data subjects the right to request confirmation as to whether their personal data has been processed and to receive such confirmation in a transparent manner.[57] Section 19(1)(a) grants data subjects the "right not to be subject to a decision significantly affecting him based solely on an automated processing of data without

55 United Nations Human Rights Council. (2018). National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21, Nigeria.

56 Ibid.

57 Section 18 (1) (a) of the draft Data Protection Bill 2020.

having his view taken into consideration". Data subjects can object to the processing or profiling of their personal data[58] and demand a cessation of the processing of personal data.[59]

## Accountability

Much more than the NDPR, the draft bill holds every stakeholder layer in the data processing ecosystem accountable for failing to fulfil their obligations towards data subjects, except in both regulations, the regulator itself. For instance, while NDPR holds data processors accountable for data breaches for which they are penalised data subjects whose rights are violated have no recourse to any action or claim over their breached personal data. Neither NITDA nor the Data Protection Commission is held accountable in any respect under NDPR or the draft bill respectively.

## Non-discrimination and Equality

Though the NDPR is built on principles of equality and non-discrimination, it is the draft bill that specifically prohibits all types of discrimination. Section 26 (7) of the bill stipulates that "A person shall not process sensitive data in respect of race or ethnic origin unless the processing of the sensitive data is (a) necessary for the identification and elimination of discriminatory practices, and (b) carried out with appropriate safeguards for the rights and freedoms of the data subject."

## Empowerment

The regulatory documents, in varying degrees, entitle participants in the personal data ecosystem to exercise their

58 Section 22 (1) of the draft Data Protection Bill 2020.

59 Section 24 (1) of the draft Data Protection Bill 2020.

rights including making claims, in the case of the draft bill, against the Data Protection Commission. Where rights cannot be exercised within the ambit of the regulation, the Nigerian and international judicial systems to which Nigeria subscribes have proven to be a point of recourse for the aggrieved, following a rise in human right wins in recent years. A case in point is the 10 July 2020 judgement of the ECOWAS Court of Justice which ordered the repeal or amendment of Section 24 of the Cybercrime Act of 2015 for violating Article 9(2) of the African Charter on Human and People Rights and Article 19(3) of the International Covenant on Civil and Political Rights.[60] The case was brought by Laws and Rights Awareness Initiatives seeking certain orders to hold the government accountable for freedom of expression violations involving journalists and bloggers. If the Cybercrime Act is brought in line with human rights norms and conventions as ordered by the ECOWAS Court, freedom of expression would be further guaranteed which would in turn benefit data protection in the country.

## Legality

The government's approach to the development of the NDPR and draft bill have been derived from existing legislation and in line with the legal rights of citizens and residents of the country. The weaknesses in both documents have been identified and stakeholder inputs particularly with respect to the draft bill is currently being collated towards improving the draft and bringing it more in line with international best practices. The national government has been demonstrating political will in improving the regulatory framework for data rights for its citizens.

60 http://prod.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_16_20.pdf

## Concluding observations and recommendations

Nigeria has taken good steps towards modernising the privacy and data protection framework and raising the country's compliance with international conventions, regulations and norms relating to human rights and fundamental freedoms. The National Data Protection Regulation of 2019 has catalysed the shift in this direction and the plan to establish a comprehensive legislation, the Data Protection Bill of 2020, presently in draft form, represents important milestones for the country. Nevertheless, good work still needs to be done by the government, public sector, private organisations, development partners and civil society advocacy groups to complete the foundational process for sound privacy and data protection practices in the country.

To achieve this, the researcher makes the following recommendations.

Government:

- Collate the views of stakeholders, private sector actors and development partners in completing the drafting of the proposed data protection legislation.
- Take further action to raise public awareness on data privacy and security from a human rights' perspective.
- Undertake to put an end to privacy rights and data protection infringements and violations.
- In the interim, provide adequate funding to NITDA and other key sectoral regulators including NIMC, NCC and CBN towards improving the privacy and data protection environment.

- Revise portions of existing law that are either in conflict with international conventions on privacy and data protection or that are open to abuse by state officials including Section 24 of the Cybercrime Act, among others.

Civil society:

- Work with the government and the national assembly to ensure that the new data protection law complies with international rights and privacy regulations when promulgated.
- Work with international organisations to create oversight arrangements for the new Data Protection Commission.
- Continue the work of advocacy to build a rich database of case law precedents that can be used to shape rights policies.

Development partners:

- Continue to put pressure on the Nigerian government to ensure that national legislation complies with international regulations.
- Assist the public sector to develop capacity for the rule of law through training programmes, overseas study tours to benchmark countries, etc.
- Work with responsible ministers of government to eliminate rights violations.
- Organise capacity-building programmes for local journalists and news media.

# South Africa

Gabriella Razzano

## Executive summary

The Protection of Personal Information Act, 2013 (POPIA) is set to be in force in South Africa midway through 2021. The inevitability of this broad data protection framework means that there are urgent questions on implementation priorities that need to be identified, rather than allowing those priorities to be determined by economic and contextual factors that may skew approaches to reactive strategies. Instead, an approach that forwards sound access to information and privacy practices that are contextually appropriate, and designed based on evidence, should be pursued.

This research was pursued to examine three broad research questions:

- What is the current data protection landscape in South Africa?
- What influences are impacting the data protection landscape?
- (Given the answers to questions one and two) What are the priority policy areas for the different stakeholders to create positive influences on South Africa's data protection landscape moving forward?

Through these questions, it was demonstrated that an historical and contextual analysis with a human rights-focus (an approach seldom pursued in relation to South Africa data protection) unpacked two key realities:

- The important role of the public sector as a data processor.
- The role of POPIA as a form of data subject empowerment in respect of both access to information and privacy.

There has been a central paradox witnessed: political influences in the country have often undermined the political passage of data protection, whilst there has simultaneously been a political prioritisation of data collection and datafication for economic ends, without acknowledgement of the Information Regulator of South Africa (IRSA) as a central realising institution for that end.

The delays in ensuring the full, and capacitated, effectiveness of the IRSA have significantly undermined POPIA's generally sound provisions. It is impeding empowerment in relation to data subject privacy rights, but also their access to information rights that have been struggling for realisation since the passage of the Promotion of Access to Information Act (PAIA) in 2000. Given the context, and the challenges, improving the capacity

– and political enabling environment – for the role of the IRSA should be prioritised.

In addition, the accessibility of recourse in relation to data protection and access to information for the public must bear in mind both the realities of the IRSA, but also the challenges which stem from trying to pursue individualised forms of recourse for data subjects in the context of low levels of digital literacy, and contexts that mean citizens are not readily able to champion their own rights easily. Alternative strategies for placing the data subject centrally in considering appropriate remedies, and stakeholder actions, should be pursued as a matter of urgency.

The research thus provides recommendations for the private sectors, public sector, public interest lawyers and civil society, and IRSA ahead of POPIA's full effectiveness.

## Introduction

The Protection of Personal Information Act (POPIA) was first assented into law on 19 November 2013. Envisioned as the key statutory effort to implement personal data protections (as an aspect of privacy protection), it created the office of the Information Regulator of South Africa (IRSA) for its enforcement. Advocate Pansy Tlakula was appointed as the chairperson of the IRSA in December 2017. And while some of the sections of POPIA came into effect on commencement in April 2014, only in June of 2020 were the bulk of the sections made effective – but in reality they will only be enforceable as of 1 July 2021.[1] The IRSA has oversight not just of POPIA, but of the access to information law, Promotion of Access to Information Act

1 Razzano, G., Van der Spuy, A., & Rens, A. (2020, 24 June). Waiting for POPIA. *Research ICT Africa*. https://researchictafrica.net/2020/06/24/waiting-for-popia/

(PAIA) as well. This relationship is important practically, but also academically – as there is significant opportunity for the IRSA to learn from the lessons that have emerged in the attempted enforcement of PAIA up to this point. In fact, the enforcement of PAIA held an important lesson for the establishment of the IRSA itself, demonstrating that "a statutory rights regime is likely to be ineffective unless adequate, accessible and cost-effective mechanisms are provided to right-holders to allow them to enforce their rights."[2] A human rights-based approach importantly centres the protection, promotion and fulfilment of the rights of privacy (and access to information) into the analysis of South Africa's data protection landscape, which is being examined at a vitally important part of the POPIA's historical trajectory.

## Country context

A STEP method is a useful analytical tool for examining context, which examines an environment across social, technological, economic and political axes (in a business intervention, it usually considers environmental impact contexts as well).[3] While useful, given its business-projection focus, it is largely ahistorical. In order to consider South Africa's data protection landscape, a historical outline of the passage of POPIA will be provided first, before consideration of the immediate STEP contexts.

## History

In South Africa, data protection was a part of the immediate discussions on legislative reform after independence.[4] In 1994, a

2 Currie, I., & Allan, K. (2007). Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa. *South African Journal on Human Rights*, *23*, 563-579.

3 Szigeti, H., et al. (2011). STEEP Analysis as a Tool for Building Technology Roadmaps. Paper presented at eChallenges e-2011, Florence, Italy, October. https://www.researchgate.net/publication/301295850_STEEP_analysis_as_a_tool_for_building_technology_roadmaps

4 Currie, I., & Allan, K. (2007). Op. cit.

"Task Group on Open Democracy" was appointed by the deputy president at the time, Thabo Mbeki, to explore open democratic priorities; and within their suite of eventual proposals, data protection was an important component of their envisioned "Open Democracy Bill".[5] The privacy component of the bill:

> [A]imed at strengthening the rights of the individual in relation to personal information by providing an expedited procedure for obtaining access to information about the requester (i.e., it was made easier to obtain your own information than other information); a right to seek the correction of personal information; regulation preventing the improper use of personal information. Unlike the access to information and government-in-the-sunshine parts of the Open Democracy Bill, this aspect of the legislation applied also to information held by private bodies.

This cross-over into public and private sector contrasted to the public law-focused obligations seen in other sections (except for the access to information provisions, which also sought to – in certain conditions – create obligations on the private sector). In relation to enforcement, the original bill didn't envision an IRSA, but an "Open Democracy Commission" that would deal with the promotional aspect of the bill, and an "Information Court", a form of superior court, for specific information recourse.[6]

However, when the bill went to cabinet, it was significantly gutted, with the most significant change perhaps being the abolition of the Open Democracy Commission and Information Courts – moving oversight (rather than full enforcement) powers to the existing South African Human Rights Commission (SAHRC), with

5 Ibid.

6 Ibid.

recourse functions being shifted to existing courts.[7] As critics of the move noted: “In many ways, open democracy legislation is only as effective as its enforcement provisions.”[8]

The bill then went before parliament, who decided to split it up into different parts. The Joint Committee on the Open Democracy Bill recommended the Minister of Justice and Constitutional Development consider data protection legislation separately; a question which he then referred for consideration to the South African Law Reform Commission (SALRC). This resulted in their paper, “‘Privacy and Data Protection” Discussion Paper 109 (October 2005), with its main recommendations being that:

- Privacy and information regulation be by a general protection law, *with or without sector-specific statutes*, which would then be supplemented by sectoral codes.
- It should cover both automatic and manual processing, and protect both private and juristic (a business or similar that has legal personality) persons.
- The eight core information protection principles posed were, namely: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation (with special information protection).
- They recommended provision for an *independent information protection regulator* with oversight of both POPIA and PAIA.
- It also suggested notification prior to any processing by entities (which in the modern data environment would have

7 White, J. (1998). Open Democracy: Has the Window of Opportunity Closed. *South African Journal on Human Rights*, *14*(1), 65.

8 Tilton, D., & Calland, R. (2002). *In Pursuit of an Open Democracy: A South African Campaign Case Study.* https://www.humanright-sinitiative.org/programs/ai/rti/international/laws_papers/southafrica/Calland%20&%20Tilton%20-%20In%20pursuit%20of%20open%20democracy.pdf

been a significant challenge given the frequency and subtlety of modern data processing).[9]

In considering the enforcement, an IRSA-like structure would primarily exercise its remedial function through conciliation and mediation, with a very proactive role. Chiefly, the report envisioned a regulator to take a flexible approach. This shift from the notion of a "commission" to a "regulator" seemed a more realistic nod to the both public sector and private sector focus on data protection provisions.

Yet the privacy issues identified by the Open Democracy Task Team in 1994, and confirmed by the final report of the SALRC in 2009, remained largely unaddressed in law outside of some sectoral protections – until the passing of the POPIA in 2013. This is the context in which the subsequent delays in the full effectiveness of the POPIA addressed in the introduction, must be understood. By May 2020 (and in many public fora prior), chairperson Tlakula was directly lamenting in parliament the lack of support by the Department of Justice and Constitutional Development (DOJCD) in reinforcing her call to bring into effect the remaining sections of the law.[10] By June 2020, POPIA had had a 26-year path. And it is with that historical passage, the current STEP environment should be outlined.

## Social

A key social reality of South Africa's data protection environment, is the mechanics of its existing digital divide. While typically the digital divide is used to refer only to difference of who is

9 South African Law Reform Commission. (2005). Privacy and Data Protection Discussion Paper. https://www.justice.gov.za/salrc/dpapers/dp109.pdf

10 Parliamentary Monitoring Group. (2020). COVID-19 Impact on Judiciary; OCJ & Information Regulator 2020/21 APPs; with Deputy Minister of Justice. Justice and Correction Services Committee, Parliamentary Monitoring Group, 12 May. https://pmg.org.za/committee-meeting/30196/

online and who is not, there is an additional difference in *how* people experience online once there that is worth reflecting on.[11] Research about access to the internet in Africa suggests that many African countries sit well below the 20% internet penetration threshold believed to be necessary for a country to capitalise on digital dividends.[12] Even in South Africa, only around 50% of the population are online (facilitated especially by broadband).[13]

These truths about digital inequality do not, however, consider the full spectrum of experienced inequality. Research in Southern Africa has shown, for instance, that additional barriers to equality in the experience of access is that the unaffordability of data, which is very consequential for lower-income groups usage, also means that "most people are using services passively, not in the high-speed, always-on environment where studies of causality in relation to penetration and economic growth have been done."[14] This passivity, which is also connected to digital literacy, means that lower-income individuals accessing the internet merely become a market for global digital commerce, rather than the beneficiaries of digital dividends. And while that may be an economic qualifier, the social reality for South African is that a) data and devices are expensive and inhibit access to the internet, and b) in an online environment, marginal use puts South African citizens at even higher risk of experiencing privacy harms. People that infrequently use ICTs often only do so when compelled to engage in order to access services: "As people who have been

11 Gangadharan, S. P. (2015). The downside of digital inclusion: expectations and experiences of privacy and surveillance among marginal internet users. *New Media and Society*, *19*(4), 597-625. https://journals.sagepub.com/toc/nms/19/4

12 Digital dividends is a term used to the broader positive developments, which derive directly from using digital technologies, such as job creation, or economic growth and easier access to global markets.

13 See in particular Table 3, which provides both supply and demand side data comparisons across the region, in Gillwald, A., & Mothobi, O. (2019). *After Access 2018: A demand-side view of mobile Internet from 10 African countries*. Research ICT Africa. https://researchictafrica.net/2019_after-access_africa-comparative-report/

14 Ibid.

'watched by default', low-income populations in particular may be attuned to trading their details for welfare benefits."[15]

## Technology (and data)

Personal data protection is clearly referring to data in the sense of information. It is nevertheless worthwhile considering data in the sense of purchasable data for internet access, to build on the social contextual discussions above.

In South Africa, a major barrier to people coming online is the cost of data.[16] Data services and products are still unaffordable to almost half of the South African population, and the infrastructure is both urban centred and insufficient – with South Africa ranking 80 out of 189 countries in terms of broadband speed.[17]

This has largely been understood as a regulatory and market problem. So much so that the Competition Commission initiated an inquiry into the data services market in August 2017, releasing its broad findings and recommendations in 2019.[18] The Competition Commission was so incensed by the lack of competition in the South African data services market, that it included in its recommendations "immediate relief on data pricing", with Vodacom and MTN being ordered to immediately reach a settlement with the Commission to reduce costs.[19] Yet, recent research has demonstrated that despite some immediate reductions to data costs, the cost of data is still largely prohibitive

15 Srinivasan, J., et al. (2018). The Poverty of Privacy: Understanding Privacy Trade-Offs from Identity Infrastructure Users in India. *International Journal of Communication*, *12*, 1231.

16 Gillwald, A., Mothobi, O., & Rademan, B. (2018). *The State of ICT in South Africa*. Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

17 Ibid.

18 Competition Commission. (2019). Data Services Market Inquiry Report. http://www.compcom.co.za/newsletter/data-market-inquiry

19 Ibid.

(given poor regulation and imperfect markets) – and it has not been sufficient to alter the reality of the disconnected.[20]

## Economics

Understanding the central economic driver underpinning personal data flows is important for contextualising South Africa's data protection response. Data (and personal data) is central to facilitating the digital economy, as driven by the fourth industrial revolution (4IR).

The collection and processing of massive amounts of personal data has become an increasingly contentious issue, because the computing analysis of this "big data" allows researchers and private or public sector organisations alike to infer people's movements, activities and behaviour presenting ethical, political and practical implications for the way people are treated and seen.[21] Yet, these developments are also central activities within the emerging economic activities of all countries. Emerging technologies of 4IR like artificial intelligence (AI), blockchain, cloud computing, drones, and the internet of things (IoT) produce, store and analyse an unprecedented amount of data. This has implications for how data (and personal data) move, especially when considered within the context of dispersed global value chains: cloud computing has quickly risen to prominence, disrupting traditional models related to data storage and distribution, with repercussions in various areas such as law, business and society.[22] The connection of devices to the internet,

20 Chinembiri, T. (2020, 25 June). Despite Reduction in Mobile Data Tariffs, Data Is Still Expensive in South Africa. *Research ICT Africa*. https://researchictafrica.net/publication/despite-reduction-in-mobile-data-tariffs-data-is-still-expensive-in-south-africa/

21 Taylor, L., & Meissner, F. (2020). A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk. *Antipode, 52*(1), 270–90. https://doi.org/10.1111/anti.12583

22 Keshvardoost, S., Renukappa, S., & Suresh, S. (2018). Developments of Policies Related to Smart Cities: A Critical Review. Paper presented at the IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), Zurich, Switzerland. https://doi.org/10.1109/UCC-Companion.2018.00083

and systems such as the IoT, AI, machine learning and other emerging technologies, have a direct implication in terms of data storing, processing and management, considering that data can be now produced, stored, and analysed by machines without human interventions.

The global dynamics of this digital economy are also incredibly important for understanding the South African context. The digital economy is dominated across digital services by a handful of American firms (Google, Amazon, Facebook, Apple, Microsoft – collectively known as GAFAM) and Chinese firms (Baidu, retail Alibaba, platform Tencent and Xiaomi – BATX).[23] This massive dominance of both market, and data, leads to the extraction of value from African consumers.[24] And from a social media and content distribution perspective, this tendency continues: with the social media market dominated in term of users by companies like Facebook (and Instagram), YouTube, Twitter and TikTok. It is this massive dominance of the digital market by only a few companies (and countries) that results in the digital colonialism cited by many authors, and results in the extraction of data and value to other jurisdictions. This has been identified as a significant inhibitor to digital economic progress on the continent.[25] These forces were confirmed by an industrial think tank working with the South Africa Department of Trade and Industry, who additionally noted that a central dynamic of data in this digital economy was acknowledging the need for "a clearly defined set of policies on data ownership, data quality, data categorisation and anonymity."[26] This recommendation is

23 Thieulin, B. (2019). *Towards a European Digital Sovereignty Policy*. Economic, Social and Environmental Council. https://www.lecese.fr/en/publications/towards-european-digital-sovereignty-policy

24 Ibid.

25 Van der Spuy, A. (2020, 23 March). Colonising Ourselves? An Introduction to Data Colonialism. *Research ICT Africa*. https://researchictafrica.net/2020/03/23/colonising-ourselves-an-introduction-to-data-colonialism

26 Barnes, J., Black, A., & Roberts, S. (2019). *Towards a Digital Industrial Policy for South Africa: A Review of the Issues*. Industrial Development Think Tank. http://www.thedtic.gov.za/wp-content/uploads/DPIP.pdf

notably well after the signing into law of the POPIA, and is an acknowledgment of the political and policy support still needed to make the existing legal framework effective.

## Politics

Law is a dialectical phenomenon – it is both influenced by extraneous superstructures, influences the base, and is influenced by the base.[27] The role of politics in this spiral is particularly interesting, and is again worthwhile preceding with historical developments for context. South Africa's apartheid history is of course well-documented. Like the liberation movements of many African countries, independence led to the election of a nationalist political party: in South Africa, the African National Congress has remained in power since the first democratic elections in 1994.[28] This central nationalism has resulted in economic orthodoxy over redistribution, but with state-centrism as a focus across spheres of policy.[29] This is an important consideration when looking at the regulatory and legislative interventions that have subsequently been both proposed and implemented.

While these may seem like meta structural influences of not much relevance to data protection, the political aspects of data governance in the country are incredibly important for considering the role it might, and should, play moving forward. Interestingly, in the executive summary of SALRC's 2009 report, it conceptualised the challenge of data protection in 2009 as being based on "[the] *growth of centralised government* and the rise

27 Casalino, V. (2018). Karl Marx's Dialetics and the Marxist Criticism of Law. *Revista Direito e Práxis, 9*(4), 2267–92. https://doi.org/10.1590/2179-8966/2018/29868

28 Mkandawire, T. (2009). From the National Question to the Social Question: Project Muse. *Transformation: Critical Perspectives on Southern Africa*, *69*, 130-60. https://doi.org/10.1353/trn.0.0029

29 Ibid.

of massive credit and insurance industries" [emphasis added].[30] Certainly, state-centrism is important as it has translated into data practice as well. In South Africa, biometric data collection was almost always a part of traditional social grant verification, with biometric fingerprinting being used by colonial and apartheid administrations.[31] These data patterns of collection, centralisation and control are an important reality for imagining how data practices led by government may continue.

To turn to the political priorities of importance to data governance more directly, South Africa has not been unaffected by the World Economic Forum's persistent discourse on the 4IR.[32] So influential has that international discourse and focus been, that in 2019 President Cyril Ramaphosa appointed a 4IR Presidential Commission, as a national overarching advisory mechanism on digital transformation.[33] Yet in formulating strategies for the 4IR, South Africa has had to acknowledge both its contextual, and policy, inadequacies. Lagging infrastructure, a lack of digital skills, as well as continuing traditional separation in our industrial sectors are all potential inhibitors acknowledged by the Department of Trade and Industry.[34] Understanding and prioritisation of the digital and data within economic imperative actually synergises with the SALRC report, which contextualised data collection and exchange within trade understandings.[35]

30 South African Law Reform Commission. (2005). Op. cit.

31 Donovan, K. (2015). The Biometric Imaginary: Bureaucratic Technopolitics in Post-Apartheid Welfare. *Journal of Southern African Studies*, *41*, 4.

32 Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.

33 Phakathi, B. (2019, 17 February). Ramaphosa Appoints Body to Make SA a Contender in the Digital Revolution Space. *Business Live*. https://www.businesslive.co.za/bd/national/2019-02-07-ramaphosa-appoints-body-to-make-sa-a-contender-in-digital-revolution-space

34 Department of Trade & Industry. (2018). *The Digital Industrial Revolution*. http://www.thedtic.gov.za/wp-content/uploads/fitp.pdf

35 South African Law Reform Commission. (2005). Op. cit.

And yet, there seems to be a divergence in understanding the role of the IRSA within this new political impetus. South Africa's main overarching policy frame is its National Development Plan (NDP) 2030.[36] While the plan does not overemphasise digital elements of development, it certainly does associate them to being central tools for development. Yet in their own (and most recent) strategic plan, the IRSA states: "The Regulator does not contribute directly towards any of the outcomes in the National Development Plan."[37] But, as we have seen, sound data governance frameworks underpin digital economic development, and will be central to fostering trust for good digital economic growth. Even some of the NDP plans have specific reference to datafication and data collection – particularly in relation to health data.[38] The failure to connect sound data practice, and an expanded role for the IRSA, within direct, stated political priorities for state data collection plans is a disconnect worth flagging.

This may be a result of the discrete political influences in the country that have often undermined the political passage of data protection, resulting in this paradox of political prioritisation of data collection and datafication for economic ends, not being met head on with the prioritisation of the IRSA as a central realising institution. In trying to understand, for instance, the delays in the passage of the POPIA, it is worth noting that in one of the first cabinet meetings on the original draft Open Democracy Bill, a lead minister, Kader Asmal, noted:

> On the one hand, people must not feel powerless at the hands of those who temporarily or permanently control

36 National Planning Commission. (2012). *National Development Plan 2030: Our Future - Make It Work*. https://www.gov.za/documents/national-development-plan-2030-our-future-make-it-work

37 Information Regulator of South Africa. (2020). *Strategic Plan for 2020/21 to 2024/25*. https://justice.gov.za/inforeg/docs/InfoRegSA-2020-2025-StrategicPlan.pdf

38 National Planning Commission. (2012). Op. cit.

their destinies. On the other, the duly elected democratic government must not be rendered powerless in carrying out its mandate. Lord Acton, as we all know, said that power corrupts. It is necessary to adapt Acton and to point out that powerlessness is equally corrupting, for individuals and for the state. The former leads to individual frustration and helplessness. The latter causes governmental drift leading to chaos – with the state unable to perform the functions expected of it.[39]

Resistance to prioritising open democracy, when the issues of privacy and access were understood together, could be understood as resistance to a perceived risk that conservative interpretations of the Bill of Rights could be used to seek to constrain progressive policy.[40] Yet, the practices of mass data collection seemed to continue, without a concomitant creation of responsibilities for both private and public sector data processing actors.

And the creation of an empowered and capacitated IRSA was consistently demeaned politically. When a contact tracing initiative was proposed by national government in response to the COVID-19 crisis in March 2020 with expanded powers for the Director-General of Health to collect mobile phone data (and only after some resistance from civil society at the lack of accountability measures), regulations were passed that gave oversight to an independent judge, with no mention of a role for the IRSA.[41] While the IRSA was not yet fully empowered, the chairperson had issued a guidance note very quickly on COVID-19 data practices, noting in an appearance before parliament that:

39 Tilton, D., & Calland, R. (2002). Op. cit.

40 Ibid.

41 Gillwald, A., et al. (2020, 27 April). Mobile Phone Data Is Useful in Coronavirus Battle. But Are People Protected Enough? *The Conversation*. http://theconversation.com/mobile-phone-data-is-useful-in-coronavirus-battle-but-are-people-protected-enough-136404. Interview with John Giles, October 5, 2020.

> [The Office of the Information Regulator] was not consulted when the regulations were drawn up, not even on the sections on data, de-identification and the security of information, etc. There was no reference to POPIA in the regulation. Immediately after the regulations were passed, the IR had been the first to issue a press statement on the importance of access to information and had implored the government to be pro-active in providing information.[42]

And although the IRSA has frequently raised issues of insufficient funding for their upcoming mandate, the parliamentary committee that oversees it has not always been empathetic, with the chairperson having to note in the latest budgetary discussion:

> The Chairperson stated that South Africa was wrong to think that things could be done incrementally in order for things to work. One could not do things using an incremental approach. The way the issue was being handled was concerning ... With a budget of R28 million (USD 1.79 million), the IR was going to face the same challenges that the Public Protector was facing. The IR would spend a lot of time in court as once all the sections were operational, it would have to fight very strong interests. Things would not immediately be solved once everything had been delegated to the Regulator. There was a need for the security cluster, and the relevant departments, to address the matter. 18 employees, or even 27 employees, could not deal with things as if it was just an administrative issue. It was a highly problematic matter.[43]

42 Parliamentary Monitoring Group. (2020). Op. cit. These are meeting minutes, not verbatim statements.

43 Ibid.

So while the centrality of data is understood as a political priority for purposes of development, and with a corresponding importance for a state-centred development agenda from the South African government, this is not met with an impetus for ensuring sound data governance and practices – a political reality that has long marred the historical progression of South Africa's data protection framework as realised through POPIA.

## Constitutional underpinning

South Africa's constitution protects the right to privacy in section 14:

> Everyone has the right to privacy, which includes the right not to have –
>
> a. their person or home searched;
>
> b. their property searched;
>
> c. their possessions seized; or
>
> d. the privacy of their communications infringed.[44]

The direct reference to communications privacy has been expanded to include informational protection; and is a relatively direct constitutional reference to information privacy that many regional constitutions do not share (often privacy is merely captured as a form of property right). South Africa's constitutional regime is based on "no fault"; in other words, once a breach is established, there is not a requirement to demonstrate fault.[45] The essential structure of the constitutional provision is to outline the methods by which privacy might be infringed i.e. through search, seizure, or communications

44 Constitution of the Republic of South Africa, 1996, s 14.

45 McQuoid-Mason, D. (2014). *'Privacy', in Constitutional Law of South Africa: Commentary*, 2nd ed. Juta.

interference, rather to centre on what is the remit of “private” (this remit has emerged through case law).

Traditional United States scholarship on privacy described it as the “right to be let alone”, but that was fundamentally envisioned within the context of space and property.[46] The understanding of privacy within the information, data and communication contexts, is in fact far more modern – yet South Africa has both constitutional and common law jurisprudence on privacy that are worthwhile reflecting on to understand the modern remit of privacy.

Privacy jurisprudence in South Africa began emerging in the 1950s.[47] But central constitutional principles began to impact on its conceptualisation; in *Bernstein*[48] the notion of privacy began to be understood along a continuum, with Judge Ackermann noting:

> A very high level of protection is given to the individual’s intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual’s activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.

While this seems to confirm a very individualistic foundation for privacy rights reminiscent of the American jurisprudence, it is also

46 Warren, S., & Brandeis, L. (1980). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

47 Burchell, J. (2009, March). The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law, 13*(1). https://www.ejcl.org/131/art131-2.pdf

48 Bernstein and Others v Bester NO and Others [1996] ZACC 2. This notion was confirmed in later cases.

emergent from its common law roots in *dignitas* and derivation from the concept of human dignity (a notion which has been confirmed by the case law).[49] The right to privacy was also later explained by the Constitutional Court as the "right of a person to live his or her life as he or she pleases", which bears similarities to the classic Warren and Brandeis definition of the "right to be let alone".[50]

The private law roots of privacy are interesting and may be influential in future interpretation.[51] Our Bill of Rights has horizontal application, and applies to juristic persons to the extent applicable – taking into account the nature of the right and the nature of the duty imposed.[52] These kinds of attributes are important, as less sophisticated rights regimes often struggle with the private dimensions of enforcing privacy in domestic contexts, particularly in the context of emergent technologies.[53]

Specific ideas on informational privacy were considered for instance in *Mistry*.[54] The court here acknowledged that the constitutional right to privacy does not directly reference informational privacy, but assumed it to be included in this matter.[55] The Constitutional Court provided some general guidelines on data protection as consisting of queries like:

- Whether the information was gathered in an intrusive manner.
- Whether information related to intimate aspects of the subjects personal life.

49 Burchell, J. (2009, March). Op. cit.

50 NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (7) BCLR 751 (CC), para 33.

51 See a modern example of expanding privacy rights in private law for application in the realm of social media in H v W [2013] ZAGPJHC 1.

52 Constitution of the Republic of South Africa, 1996, s 8 (2)-(4).

53 Kurbalija, J. (2016). *An Introduction to Internet Governance*. Diplo Foundation. https://www.diplomacy.edu/sites/default/files/AnIntroductiontoIG_7th edition.pdf

54 Mistry v Interim National Medical and Dental Council and Others [1998] ZACC 10.

55 Ibid., para 47.

- Whether it was used for a purpose other than for what it was provided.
- Whether it was communicated or disseminated to the press or public from whom the data subject "could reasonably" expect such information to be withheld from.[56]

This was obviously contextualising data protection in an "interference" context, but some of the elements of course bear similarity to broader processing limitations. Taking these ideas, and comparing them to traditional notions on privacy, the idea of prevention of "interference" and "invasion" exists more readily than notions of exerting control as over ones data as a form of empowerment and agency. The Open Democracy Bill, and SALRC recommendations, moved the context far more significantly in that direction.

Later readings began to centre that more directly, with Neethling in 2005 defining privacy as:

> An individual condition of life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the *person concerned has himself determined to be excluded from the knowledge of outsiders* and in respect of which he has the will that they be kept private [emphasis added].[57]

Thus, the idea the right to privacy entailing an individual's right to control his personal information free from unwanted intrusions begun to centre more clearly – though of course elements of this

56 Ibid., para 51.

57 Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1). *THRHR*, *79*(51).

can be read into the Mistry judgement guidelines, too.[58] Authors have noted that Neethling's definition leads to two ways in which the processing of a data subject's personal data can be infringed, namely by a) unlawfully processing true and correct personal data about an individual; or b) processing false and misleading data about an individual, with the former meaning a data subject's privacy is infringed and the latter infringing a person's individual identity.[59] POPIA has been enacted to:

> Regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives *effect to the right to privacy* subject to justifiable limitations that are aimed at protecting *other rights and important interest* [emphasis added].[60]

It will be interesting to consider over time how the elements of the infringements to personal identity associate with the right to privacy, given it is not a "natural" aspect of the constitutional right, and yet is included (practically and necessarily) within the scope of the POPIA – this has become merged through the categorisations of data subject rights, in particular.[61] Over time, privacy and control have become important partners, but are a result of developing ideas of constitutional protections over time.

## Broader legislative environment

### PAIA

The POPIA impacts a variety of laws, but is also being enacted within a particular legislative environment. Importantly, access to

58 Ibid.

59 Ibid.

60 Protection of Personal Information Act 2013, Preamble.

61 This is especially true as this component would link to ideas (and challenges) around rights to erasure.

information (as mentioned) is governed by the PAIA. Enacted in 2000, this act creates a process for the request of information from both public entities, as well as private entities when required for the exercise or protection of any other right. POPIA has reallocated oversight and enforcement of PAIA from the South African Human Rights Commission (SAHRC) to the IRSA. This "handing over" of powers has, however, not yet occurred – and has been delayed as part of the broader deferral of legal effectiveness POPIA.[62] So POPIA essentially impacts PAIA through:

- The removal of the obligation to submit PAIA manuals to the SAHRC.
- The full transition of current PAIA functions of the SAHRC to the IRSA (as well as the expansion of the powers in performing those functions provided to the IRSA).
- The development of an alternative review mechanism to a court application for challenging PAIA decisions.[63]

To a degree, there are components of data and information protection within PAIA itself. While there is a right to request access to information, PAIA provides a mandatory grounds of refusal against a request of information if it would involve "the unreasonable disclosure of personal information of a third party".[64] Yet (and while POPIA has amended slightly the definition of personal information) the sections provided certain caveats to the refusal ground, for instance not including information if consent has been given, or if it is in the public domain. There has also been a tendency in PAIA case law to interpret these refusal grounds quite restrictively.

62 Razzano, G., Van der Spuy, A., & Rens, A. (2020). Op. cit.

63 Protection of Personal Information Act 2013, Schedule: Laws Amended by section 110.

64 Promotion of Access to Information Act, s 34 and 64.

## Statutory personal information protection/data privacy

The National Health Act, 2003[65] is an example of specific, statutory data protection for a sectoral information type. The act considers this within the concept of confidentiality, and provides that all information concerning a user (including information relating to his or her health status, treatment or stay in a health establishment) is confidential. No person may disclose any such information unless: a) the user consents to that disclosure in writing; b) a court order or any law (like PAIA or section 15 of the act itself) requires that disclosure; or c) non-disclosure of the information represents a serious threat to public health.

Another sectoral example of information protection relates to confidentially of information related to HIV-status, which is provided for children in the Children's Act, 2005. The Health Professionals Council of South Africa has issued guidelines to similar effect, though this would obviously be qualified as per the National Health Act, 2003 which provides the public health exclusion.

There are also statutes that deal with the methods of interference, rather than the substantive nature of the information itself. The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 permits the interception of communications of any person by authorised state officials, subject to prescribed conditions. While communications interference statutes may not be uncommon, several of the sections of the law have been declared unconstitutional given the broad powers the law provides.[66] The court – when considering the challenge to the law – considered

65 National Health Act, 2003, s 14.

66 Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others [2019] ZAGPPHC 384. The declaration of unconstitutionality is currently before the CC for confirmation.

that it lacks provision for post-surveillance notification, it fails to prescribe an appointment mechanism and terms for the designated judge (who oversees notices for interception) which ensure the designated judge's independence, it fails to adequately provide for a system with appropriate safeguards to deal with the fact that the orders in question are granted *ex parte*, fails to prescribe data processing practices for the enforcement authorities that would allow for oversight of the processes, and fails to consider the specific cases of both lawyers and journalists (and their forms of privilege) which should mean specific protections from surveillance.[67] In addition, it declared practices of mass/bulk surveillance by the national communications centre to be unconstitutional, as there is no statutory authorisation available for the activity.

The Electronic Transactions and Communications Act, 2002 was one of the earliest legislative interventions to try and engage on data protection, although chiefly within an e-commerce context (the early rumblings of digital economic activities in the country). The act is largely recognised as a failure, not least of all in its inability to ensure in any way its commitment to "universal" internet access in the country. The National Integrated ICT Policy White paper, 2016 proposed a swathe of amendments to the law, many of which are in the process of being legislated.[68]

## Privilege

Privilege is a form of specific data protection worth noting. While confidentiality arises from agreement (either tacit or express), privilege is a form of ethical protection for communications that arise between persons who have a special duty of fidelity and

67 Ibid.

68 Gillwald, A., Mothobi, O., & Rademan, B. (2018). Op. cit.

secrecy toward each other.[69] In South Africa, there is significant common law consideration of privilege, particularly as it relates to legal professional privilege.[70]

## Bills of relevance

The reemergence of the Protection of State Information Bill (dubbed “the Secrecy Bill”) is noteworthy in considering the data protection landscape. First introduced in 2010, the Secrecy Bill was immediately met with significant civil society pushback. Coalescing around resistance to the bill, and specifically the heavily state-security influenced prohibitions on access of state information even if simply “sensitive” or “commercial”, a civil society movement called the Right2Know Campaign was developed and it is still active today. While the bill went through many changes in parliament, it was passed in 2011, but it has been referred back to parliament by President Ramaphosa for a *second* time (having first been referred back by former President Zuma in 2013). Civil society has called on the president to expand the grounds for review, as many problems still remain.[71] In the context of data protection, at its simplest there has always been an a concerted effort by arms of government to expand on categories of “confidential information” to prevent legitimate access, even though confidentiality is not a form of automatic exclusion from the ambit of PAIA.[72] It is interesting to note the political energy placed historical into state information protection, in spite of significant “foot dragging” in relation to personal data protection.

69 Wagner, K., & Brett, C. (2016, 29 August). I Heard It through the Grapevine: The Difference between Legal Professional Privilege and Confidentiality. *De Rebus*. http://www.derebus.org.za/heard-grapevine-difference-legal-professional-privilege-confidentiality

70 South African Airways Soc v BDFM Publishers (Pty) Ltd and Others [2016] 1 ALL SA 860 (GJ).

71 Media Monitoring Africa et al. (2020, 9 July). OP-ED: Secrecy Bill Is Still Fundamentally Flawed and Needs to Be Reconsidered. *Daily Maverick*. https://www.dailymaverick.co.za/article/2020-07-09-secrecy-bill-is-still-fundamentally-flawed-and-needs-to-be-reconsidered/

72 Razzano, G. (2015, 8 June). State Security, Classification and Information Trumps: The State’s Awkward PAIA Conundrum. *Daily Maverick*. https://www.dailymaverick.co.za/opinionista/2015-06-09-state-security-classification-and-information-trumps-the-states-awkward-paia-conundrum

This is not the only bill in the South African landscape, which shows an inability to properly consider the constitutional foundations of both data access and data privacy alongside each other: the draft Films and Publications Amendment Regulations are just as problematic (and even more worryingly have been drafted in an attempt to realise the Films and Publications Amendment Act, 2019 which received significant pushback from civil society – though that pushback was largely ignored).[73] The regulations introduce a cumbersome process for the classification of online distributed content in South Africa alongside significant reporting requirements, but also provide the Film and Publications Board with broad discretionary powers for registration.[74]

Both of these bills demonstrate a tendency toward broad desires for centralised, and highly controlled data practices by the South African government (alongside some misunderstandings of the realities of the digital data environment), with an undermining of personal data mechanisms that would place more control in the hands of data subjects themselves.

## Domain name regulation

Though largely regulatory issues, a brief consideration of the domain name regulation frame is of relevance to considering the digital human rights environment. All domain names in South Africa are regulated and managed by the .za Domain Name Authority (.ZADNA), which is an entity created by statute (their functions include domain disputes). It was established under the Electronic Communications and Transactions Act, 2002 as non-profit company. The ZA Central Registry (ZACR)

73 The Draft Films and Publications Amendment Regulations. 2020. Published for comment.

74 Business Tech. (2020, 5 August). Massive Problems with New Proposed Internet Rules for South Africa. *Business Tech.* https://businesstech.co.za/news/internet/422966/massive-problems-with-new-proposed-internet-rules-for-south-africa

– as the entity managing various .za second level domains, such as co.za, net.za, org.za and web.za – recently celebrated topping 1,000,000 domain name registrations, with the majority of these domain names being under .co.za.[75] To a register a domain, an applicant must submit at least two independent and operational name server hosts alongside personal contact details.[76] In practice, applicants can use a privacy service to shield their details from the public.[77]

The .ZADNA is also set for amendment through the National Integrated ICT Policy White Paper, 2016 – and will be absorbed into a central economic regulator, which may assist in some of the fund distribution challenges it has seen.[78]

It is worth reflecting on the practical impact such an authority can have in relation to data and information management, which was demonstrated during COVID-19. During the crisis, the Minister of Communications and Digital Technologies directed that all .za websites have a landing page with a visible link to the South African Resource Portal on COVID-19.[79] This was an interesting form of state intervention to try and counter misinformation, though was also partnered with other far more restrictive measures like the criminalisation of the spread of COVID-19 related misinformation.[80]

75 https://www.registry.net.za

76 Le Roux, C. (2017). *'South Africa', in Domains & Domain Names*. Law Business Research.

77 Ibid. It is worth noting that once POPIA is fully operational, the registrars will of course need to be POPIA compliant and are not totally excluded from its processing provisions. However, their statutory obligation to make certain personal information public will exclusions from certain provisions, such as section 15 which states that there is no further processing limitation on information derived from public records.

78 Gillwald, A., Mothobi, O., & Rademan, B. (2018). Op. cit.

79 Giles, J. (2020, 28 March). za landing pages should link back to www.sacoronavirus.co.za. *Michalsons*. https://www.michalsons.com/blog/za-landing-pages-should-link-back-to-www-sacoronavirus-co-za/42571

80 Hodgson, T., Farise, K., & Mavedzenge, J. (2020, 5 April). Southern Africa Has Cracked down on Fake News, but May Have Gone Too Far. *The Mail & Guardian*. https://mg.co.za/analysis/2020-04-05-southern-africa-has-cracked-down-on-fake-news-but-may-have-gone-too-far

## Regional and international commitment to privacy and data protection

Privacy is a fundamental right guaranteed in almost all declarations of rights. In the classical human rights enunciation of the Universal Declaration of Human Rights (1948), Article 12 (though not binding) states that:

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

Similarly, the International Covenant on Civil and Political Rights (1966), to which South Africa is party, guarantees the right to privacy in Article 17, as follows:

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

These are clearly consistent with South Africa's own constitutional enunciations; South Africa's enunciation which states that "[e]veryone has the right to privacy, which *includes*" envisions a potentially broader role for privacy. Notably, the ICCPR includes a protection against *unlawful* interference, thus emphasising the importance of legal frameworks for contextualising domestic rights of privacy.

In the region, personal privacy was not prioritised previously as a rights area given its association with individualised, rather

than communal, rights.[81] For instance, the African Charter on Human and Peoples' Rights (1981) provides for a number of rights under the Universal Declaration of Human Rights (UDHR, 1948) but does not mention the right to privacy. This omission is believed to have emanated from the perceived nature of the right by the framers of the African Charter, as promoting individualism contrary to the communalism that typifies African societies. Nevertheless, the right to access, update and correct personal information, which has its origins in the right to privacy, is protected in the Declaration of Principles on Freedom of Expression in Africa, 2002. Principle IV (3) of the declaration states that "everyone has the right to access and update or otherwise correct their personal information, whether it is held by public or by private bodies", thus providing data subject rights.

More directly concerned with data governance frameworks, is the highly influential European Union General Data Protection Regulations, 2016 (GDPR). The limitations posed by the GDPR on cross-border transfer on countries without similar protections has been cited as a significant contribution to the renewed impetus in the passage of data protection frameworks since its inception. Framed within a human rights context, the GDPR pays significant attention to the establishment of an independent data protection act.

Of course, there is in addition the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014. While it provides data protection guidelines, the instrument is not binding as an inadequate number of countries have ratified it, with South Africa not even yet signing it. In many senses, the lack of domestic traction for the document arising with it not aligning with government priorities

81 Boshe, P. (2017). *Data Protection Legal Reform in Africa*. Passau University.

domestically – which centre in many African countries largely on control frames – it was originally "pushed through" as an attempt to comply with European data protection imperatives from a strong economic incentives perspective.[82] The earliest instruments on data protection were always strongly embedded in economic imperatives – exemplified for instance in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 (the first binding instrument on data protection), and the Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 1981 (these guidelines were importantly referenced in the drafting of the SALRC's recommendations on our domestic data protection frames). Though South Africa was not party to that convention, it is *signatory to* (though has not ratified) the Council of Europe Convention on Cybercrime (Budapest Convention), 2001 – which deals with broader cybercrime issues, but also prohibits unlawful data interference, whilst also obliging criminal offences for different forms of data interference and alteration.

In terms of specific legislative guidance, the SADC drafted a Model Law on Data Protection, 2013. In addition to creating a frame for the transfer of personal data, the model law in the main also provides guidance on:

- The establishment of a domestic DPA
- Integrity and quality of data
- The provision of data subject rights
- General rules for the processing of data

82 Sutherland, E. (2020). Presentation at Conference on privacy and data protection in Africa, Centre for Human Rights, online, 12 October.

- Obligations on those who control and process data
- Recourse and sections
- Codes of conducts.

Outside of these more direct data protection frames, additional human rights instruments of relevance include the expanded Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019 (from the African Commission on Human and Peoples' Rights) importantly considers broader data governance issues, such as stating that data localisation laws are permissible only where justifiable and compatible with international human rights law.

Guideline documents of relevance include the African Union Commission and Internet Society's Personal Data Protection Guidelines for Africa, 2018 and the African Declaration on Internet Rights and Freedoms, 2016.

It is important to note how many of the African instruments of relevance to data protection are strongly framed within human rights frameworks.

## Key features of POPIA

### The implementing environment

The POPIA's future effectiveness date comes at a time of real urgency. Even without full enforcement powers, the IRSA has already had to engage on numerous high profile, mass data breaches that have threatened the South African trust environment. IRSA has engaged on the Facebook/Cambridge Analytica breach in 2018, as well as domestic breaches like that

at Aggregated Payment System Ltd, Liberty Holdings Ltd, and even the Experian breach said to have impacted the personal data of 24 million South Africans.[83]

It is worth thinking too about the first significant official action taken by the IRSA, to understand the realities that the POPIA is confronting. In April 2017, the IRSA were called as respondents in a case called *Black Sash*.[84] The court challenge related to a contract that had been given to a company Cash Paymaster Services (CPS), to help the South African Social Security Agency distribute grants (and collect biometric data of grant beneficiaries). The contract predated the POPIA, but when the challenge arose the IRSA were cited largely to assist in the construction of the relief. The case raised a significant data governance problem – even though the main challenge was trying to engage with grant distribution functions and the validity of the tender, it became clear that CPS had been using data they gathered (and potentially data supplied to them) to sell "over-the-top" products to beneficiaries, such as life policies, high interest loans and airtime. In the case IRSA raised the need to construct the relief to ensure that it expressly noted that the data subjects owned their own personal data; and beside demonstrating important proactivity by the IRSA, it also demonstrates that particular risks present in South Africa due to poorly constructed public-private partnerships.[85]

It is within this context, and the broader context articulated earlier, that we should examine the detailed construction of the POPIA itself.

83 See statements issued by the IRSA on such breaches: https://justice.gov.za/inforeg/media.html

84 Black Sash Trust v Minister of Social Development [2017] ZACC 8.

85 Razzano, G. (2017, 23 April). Sassa Grants: The Small Information Win Hiding in the Grant Crisis. *Daily Maverick*. https://www.dailymaverick.co.za/opinionista/2017-04-24-sassa-grants-the-small-information-win-hiding-in-the-grant-crisis

## Definitions

The POPIA centres its provisions in relation to three key stakeholders:

- A *data subject* is the person that personal information relates to or identifies.
- A *responsible party* is the party that decides to process personal information in a certain way.
- An *operator* is the person that processes personal information for somebody else. This person does not determine the purpose and the means for processing.

It provides a broad definition of personal information, considering it to be in essence information that identifies a living person is personal information. This can be for example: age, race, gender, education, medical, financial, criminal or employment history of a person. It includes not only contact information like an email address, telephone number or location information, but biometrics, correspondence and personal opinions. Importantly (and consistently with constitutional protection of privacy) juristic persons such as companies and NGOs can also have personal information, so the POPIA protects more than just living people (this extension to juristic entities contrasts with the GDPR).[86]

The POPIA also creates a subcategory of personal information called special personal information, which concerns especially sensitive information. This is the kind of information that someone can use to unfairly discriminate against a data subject.

86 Giles, J. (2020, 13 February). GDPR vs POPIA: Compare the GDPR with the POPI Act? *Michalsons*. https://www.michalsons.com/blog/gdpr-mean-popi-act/19959

Examples are race, ethnic origin, trade union membership, health, biometric information (such as fingerprints), and criminal behaviour. This requires more rigorous processing limits; you cannot process special personal information unless you are authorised to do so. There is a general authorisation that applies to all the types of special personal information, and there are further specific authorisations that relate to each type of special personal information.

Processing covers all the different ways that someone's personal information can be handled by a responsible party or operator. It includes opening a file, reading a document, or emailing information to someone. It could also be saving documents on a USB, transferring them from one computer to another, or even deleting or editing documents. Basically, processing covers all the different ways you handle someone's personal information.

## Exclusions

Sections 6 and 7 apply to exclusions of data from POPIA, namely:

- If processed in the course of a purely personal or household activity.
- That has been de-identified to the extent that it cannot be re-identified again.
- If processed by or on behalf of the state with regard to national security, defence or public safety, or the prevention, investigation or proof of offences; or for the purposes of the prosecution of offenders or the execution of sentences or security measures, *to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information.*

- For exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information.
- If processing is solely for the purposes of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.
- Processing by cabinet and its committees, the executive council of a province and a municipal council of a municipality.
- For purposes relating to the judicial functions of a court referred to in section 166 of the constitution.
- Under circumstances that have been exempted from the application of the conditions for lawful processing by the information regulator in certain circumstances.

## Processing requirements

A data subject's consent is not necessary in all circumstances to process their personal information (though authorisation is needed for special personal information), and the POPIA allows responsible parties to have different reasons why they are processing the personal information – such as a legitimate interest being established (there is a significant focus in EU GDPR related jurisprudence on "legitimate interest").[87] The POPIA centres itself more explicitly across eight conditions that

87 Protection of Personal Information Act, 2013, s 11. This approach to consent is directly supported by some of the discussions on consent contained in the African Union Commission and Internet Society's Personal Data Protection Guidelines for Africa, 2018.

responsible parties need to comply with for their processing to be lawful. The conditions[88] (in cursory form) are:

- Accountability: This means that the responsible party must take the lead in ensuring compliance with POPIA.
- Processing limitation: The responsible party must have a good reason for processing someone's information and try as far as reasonably possible to collect the personal information directly from the data subject.
- Purpose specification: The data subject must know about the purpose for which the responsible party is processing the personal information.
- Further processing limitation: The responsible party must ensure that if they process that personal information again, it must be for the original purpose that they informed the data subject about.
- Information quality: The responsible party must ensure that the personal Information they process is accurate and complete.
- Openness: The responsible party must be open towards data subjects regarding how they process personal information
- Security safeguards: The responsible party must provide appropriate and reasonable security measures against any risks that the personal information is exposed to.
- Data subject participation: The responsible party must communicate with the data subject about the processing and give the data subject to correct or update the personal information the responsible party is processing.

88 Protection of Personal Information Act, 2013, s 18-25.

Transfer is a form of processing. Personal information can only be transferred out of South Africa if the responsible party ensures certain conditions are met. The main one of these conditions is that the responsible party has the consent of the data subject to the transfer. The POPIA only allows for the transfer of personal information outside of South Africa to a country with substantially similar levels of data protection as POPIA.

## Data subject rights

Importantly, POPIA creates certain rights for the data subject to try and expand the control a data subject can exert over their own data. These rights include the data subject participation rights in sections 23 to 25, which the responsible party is obliged to ensure: such as the right to access personal data, correct it, or even destroy it if certain conditions are met. In addition, section 5 of POPIA outlines broader data subject rights, such as rights to object to different forms of processing, and to submit a complaint to the IRSA, or take civil claims on the basis of interference with their data.

These empowering sections are important from a public interest perspective. In addition, the rights that relate to infringements on personal identity (and the correction of it) contribute not just to expanding trust in the digital economy, but also ensuring data integrity for better data usage, and advancing important personal realms of human rights.

## Powers, duties and functions

The POPIA creates broad enforcement powers for the IRSA[89] (as noted too, expanding the remit to oversight of PAIA as well). In regard to these acts, the IRSA is obliged to educate, monitor and

89 Contained in detail in the Protection of Personal Information Act, 2013, section 40.

enforce compliance, consult and handle complaints, to facilitate cross-border cooperation, and other related general duties. In relation to systemic issues within both the data access and protection fields, the IRSA is able to investigate issues without complaints being lodged. IRSA can issue fines and other penalties for responsible parties failing to protect personal information. IRSA can attempt to resolve complaints through dispute resolution mechanisms, and has other "commission" powers such as issuing summons and holding public sittings, but is also obliged to establish an enforcement committee, which includes a judge.

The enforcement provisions are then given more detail in chapter 10, such as rights to apply to issue warrants, search and seizure powers and – through the enforcement committee – issue notices, which (if failed to comply with) can constitute a criminal offence. It is interesting that the GDPR, in contrast, does not created criminal offences.[90]

An important consideration for the future of enforcement is the power of the IRSA, outlined in section 99 to institute civil claims on behalf of a data subject (or, foreseeably, a group of data subjects). While the educational aspect of the IRSA's work will be important considering the digital literacy environment, so too might be the ability for the IRSA to directly support and empower data subjects in the public interest.[91]

## Codes of conduct

An important aspect of the POPIA (reminiscent of both the SALRC recommendations, and also the SADC Model Law of Data Protection, 2013) is chapter 7, which outlines the issuing of

90 Giles, J. (2020). Op. cit.

91 Interview with Varsha Sewlal, Executive: Legal, Policy, Research and Information Technology Analysis, 12 October 2020.

sectoral codes. Such codes are very important, as they provide sectors with specific agency to co-create codes of conduct along IRSA that can be responsive to their sectoral realities in terms of data processing. Although they can never be of a lower standard than the provisions of the POPIA, so flexibility in the regulatory framework allows the private sector greater participation; and in addition may help relieve the compliance burden. Essentially, codes create sector specific guides, and allow for the establishment of a sectoral adjudicator that can hear complaints related to the breach of the code from members of the public (this in turn can help relieve the preliminary burden on the IRSA for filtering significant amounts of complaints, and relates to administrative law principles on internal remedies already available in PAIA for access to information requests).[92]

The IRSA had already issued Guidelines on the Development of Codes of Conduct, with public comments on the draft having now closed.[93] In public hearings, certain private sector representatives raised concerned on the burdens posed by the guidelines, which may simply be met by the acknowledgement that there is no obligation to create codes for the sector, though (given the above) it would seem advisable.

## Breach notifications

An important positive obligation created by the POPIA, which strongly supports its role within the cybercrime and cybersecurity context, is contained in section 22, which obliges the responsible party to inform both the IRSA and the data subject concerned if they have reasonable grounds to believe a breach of personal data has occurred.

92 Ibid.

93 The guidelines are available for review here: https://justice.gov.za/inforeg/docs/InfoRegSA-Guidelines-Invite-20191205.pdf

The breach notice must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. It is worth noting here that the Cybercrimes Bill, 2017 may attenuate that provision by prescribing a 72-hour notification period in relevant breach cases.

## Data protection authority

The role of IRSA in concurrently overseeing both data access and data protection is not necessarily typical, though some other jurisdictions incorporate both mandates within their data protection authority (DPA) structure.[94] This dual function is important conceptually: both data access and data protection are partners in creating a trusted digital economy that centres on data with integrity, that flows and is processed in a manner that is lawful.

This dual function is also a recognition of the failures in implementation that have haunted the PAIA up to this point.[95] In spite of early recognition of the vital importance of a form of independent DPA for ensuring the advancement of data rights that were highlighted in both the Open Democracy Bill and the SALRC recommendations,[96] the limited powers of the SAHRC in the enforcement of the PAIA have often been directly attributed to the poor implementation (and low levels of compliance) with the law.[97] However, the postponement in handing over of functions

94 See for instance Canada, specifically s 3 of the Personal Information Protection and Electronic Documents Act, 2000. So too for Australia, see section 2 (A) (a) of the Privacy Act, 1988 and section 3 and 11 of the Freedom of Information Act, 1982. For Sri Lanka, see sections 3(1) and 5 (1) (a) of the Right to Information Act of 2016; the United Kingdom and Hungary as well.

95 Tilton, D., & Calland, R. (2002). Op. cit.

96 This essential component of has been highlighted on academic texts in relation to both access to information and data privacy.

97 Currie, I., & Allan, K. (2007). Op. cit.

from the SAHRC to the IRSA until next year presents an additional problem: this lacuna means that the SAHRC is now reducing its capacity to engage on PAIA compliance, with members of the public still having no recourse to the IRSA.[98]

Nevertheless, the establishment of the IRSA is well underway. As mentioned, since December 2017, the chairperson advocate has been Pansy Tlakula. The IRSA is in addition comprised of four other members: two part-time, and two full-time. The two full-time members are Advocate Lebogang Stroom-Nzama and Advocate Collen Weapond, and the current part-time member is Advocate Sizwe Snail ka Mtuze. However, the fourth part-time member vacancy is currently open (Professor Tana Pistorius vacated her position), and the appointment process is currently underway, with the justice committee just completing public hearings for the appointment.

Various executive and administrative positions have been filled, and the IRSA is currently finalising discussions with the National Treasury, which will see them expanding their current budget to allow for more hiring ahead of the 2021 deadline.[99] Budget constraints have marred implementation more broadly, and the IRSA has been using the policies of the DOJCD while establishing its own administrative capabilities.[100] However, this has impeded its capacitation by adding additional bureaucratic blocks to procurement and hiring, and also serves as a threat to its perceived independence.[101]

98 Interview with John Giles, managing attorney, Michalsons Attorneys, 5 October 2020.

99 Interview with Varsha Sewlal, Executive: Legal, Policy, Research and Information Technology Analysis, 12 October 2020.

100 Parliamentary Monitoring Group. (2020). Op. cit.

101 Ibid.; Currie, I., & Allan, K. (2007). Op. cit.

In terms of strategy, the IRSA recently presented its Strategic Plan 2020/21-2024/25 before parliament.[102] This is the second strategic plan since its creation, with the original Strategic Plan for 2017-2020 having been outlined through these strategic goals:[103]

| Strategic outcome-orientated goal | Strategic objective |
|---|---|
| South Africans that are aware and understand their rights in regard to personal information and access to information. | Develop and implement awareness and educational programmes aimed at promoting the protection of personal information and access to information. |
| A conducive legislative, policy and technological environment that promotes the protection of personal information and access to information. | Monitor and research the processing of personal information and computer technology to ensure the promotion and the protection of personal information and access to information.<br><br>Monitor and enforce compliance by private and public bodies to ensure that existing and proposed legislation and policy promotes the protection of personal information and access to information. |
| A conducive regulatory environment that allows for the protection of personal information and access to information. | Make regulations, guidelines, codes of conduct and notices. |
| Informed stakeholders and cooperative relationships to ensure the protection of personal information and access to information. | Undertake engagements with relevant stakeholders concerned with the protection of personal information and access to information. |
| Protection of personal information and access to information through resolving complaints. | Conduct prompt investigations and complaints and ensure resolution of disputes related to the violation of the protection of personal information and access to information. |
| Alignment of national legislation with international best practice through research. | Conduct comparative legal research relating to the protection of personal information and access to information. |
| Optimally functional independent information regulator. | Create a high performing information regulator to deliver on its mandate. |

102 Parliamentary Monitoring Group. (2020). Op. cit.

103 The full document is available for review at: http://www.justice.gov.za/inforeg/docs/InfoRegSA-2018-2019-APP.pdf

The breadth of the strategic objectives of the first plan are of course noteworthy. In its second strategic plan, perhaps given the role of the new executive staff, the plan talks less of goals and objectives, and moves toward "measurement" languages, highlighting instead "Impacts, Outcomes and Outputs". In looking at those, they are summarised as:[104]

| Impact statement: Promotion and protection of personal information and the promotion of access to information | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Outcome** | **Outcome Indicator** | **Baseline 2019/20** | **Performance targets over the medium term period** | | | | |
| | | | **2020 /21** | **2021 /22** | **2022 /23** | **2023 /24** | **2024 /25** |
| Personal information promoted, protected and respected | Number of complaints received | 271 | 300 | 400 | 500 | 600 | 700 |
| | Percentage of stakeholders who are aware of the existence of the Regulator | Nil | Nil | Nil | 5% of sampled population | 10% of sampled population | 10% of sampled population |
| Access to information promoted | Percentage improvement in the compliance with section 32 of PAIA | Not yet determined | Nil | Nil | 10% | 15% | 25% |

There are a few noteworthy aspects of the strategic plan measures. The first is that a baseline has already been established for POPIA complaints, because the IRSA is already receiving frequent complaints from by members of the public, and their agents, in spite of not yet having full enforcement powers.[105] It is also noteworthy that the impact on access to

104 Parliamentary Monitoring Group. (2020). Op. cit.

105 Interview with Varsha Sewlal, 12 October 2020. Op.cit.

information has been limited and relates only to promotion, and not protection and respect. This may relate to the fact that full obligations will only transfer later, but there is a continuing emphasis on data protection that raises flags on the focus on access to information – in spite of its massive significance to the advancement of human rights.

Outside of this practical implementation, the IRSA has already begun to establish itself within the region (an important consideration in the long term for intra-regional co-operation, the need for which will only expand in the emergence of the African Continental Free Trade Area). Besides regular public engagements on regional platforms such as the opening the Conference on Privacy and Data Protection in Africa, online (12-15 October 2020), and the Roundtable of African Data Protection Authorities, Johannesburg (18 June 2019), the IRSA importantly hosted the 11th International Conference of Information Commissioners, Johannesburg (10-13 March 2019) (this will be an important network of commissioners for the IRSA to remain engaged with in future).

## Other key stakeholders

As mentioned previously, there are other stakeholders that will be important in helping the IRSA fulfil its functions. The SAHRC will be an important partner not just because the IRSA will need to complete the “taking over” of the SAHRC’s PAIA mandate, but also because of the lessons the SAHRC will be able to share in its experiences trying to facilitate public access to information (and enforcement). As the central national institution for promoting constitutional democracy and human rights in South Africa, they will have a continued role to play in the fulfilment of the right to access information and right to privacy in partnership with the IRSA.

Also associated with the legacy of the PAIA in the POPIA's history, it is worth noting that South Africa's Public Protector (PP) has specific powers to investigate at his or her own initiative, or on the basis of a complaint, issues relating to the administration or operation of the PAIA (bearing in mind of course the PP's broader mandate to investigate public maladministration and misconduct).[106] In their first strategic plan, the IRSA had already acknowledged the need to collaborate with the PP for generating accurate public complaint statistics in relation to the PAIA.[107]

Given the centrality of data protection to the pursuit of a good digital economy, there will also be an important role to play for associated regulators, such as the National Consumer Commission (not a full regulatory authority) and the Competition Commission. The Competition Commission has in fact just released a report for public comment called "Competition in the Digital Economy", which centres data privacy and sovereignty as key consumer concerns.[108]

## Data protection advocacy

South Africa has a robust civil society movement on the advancement of access to information, which (as seen in the history) has driven important progress on PAIA and POPIA since independence.[109] The strong civil society voice demonstrated in campaigns against the Secrecy Bill, or in for instance the former Open Democracy Advice Centre's over decade long POPIA advocacy (unfortunately that organisation was forced

106 Public Protector Act, 1996, section 6(4)(d).

107 The full document is available for review: https://www.justice.gov.za/inforeg/docs/InfoRegSA-2018-2019-APP.pdf

108 Public call for comments: http://www.compcom.co.za/wp-content/uploads/2020/09/Competition-in-the-digital-economy_7-September-2020.pdf

109 Tilton, D., & Calland, R. (2002). Op. cit.

to close given insufficient funding in recent years),[110] were all strongly associated to human rights agendas. There are also other advocacy groups still active in the South African region who engage on data protection, such as Media Monitoring Africa, the Right2Know Campaign, and others who perform research and advocacy functions.

Human rights as a normative priority have extended to advocacy related not just to data privacy and access, but also to data pricing and accessibility. Research ICT Africa tracks mobile pricing data across the continent, but also leverages that data for policy-based advocacy on reducing digital inequalities.[111] The #DataMustFall movement arose organically as public frustration has increased at exclusionary data pricing,[112] and appears to have been influential in the Competition Commission's approaches in the Data Services Market Enquiry discussed earlier.

Yet there should be a concern that broader advocacy in relation to access to information and privacy may not be resulting in strongly targeted civil society engagement on data protection, in particular. At public hearings hosted by the IRSA, private sector interests have been strongly represented by the legal sector in particular, who are engaging keenly given the compliance ramifications of the law.[113]

110 Parliamentary Monitoring Group. (2011, 14 February). Protection of Personal Information Bill: Input by South African Human Rights Commission Proposed Relocation of Certain Powers. *Justice and Correctional Services Committee*. https://pmg.org.za/committee-meeting/12553/

111 See examples of their research and policy publication: https://researchictafrica.net/research/research-papers-and-publications/

112 Shapshak, T. (2016, 21 September). #DataMustFall Highlights South Africa's Costly Wireless Broadband Problems. *Forbes*. https://www.forbes.com/sites/tobyshapshak/2016/09/21/datamustfall-highlights-south-africas-costly-wireless-broadband-problems/ - 5f6292463a55

113 Interview with John Giles, 5 October 2020. Op. cit.

## Participation and accessibility

A fundamental issue of importance for human rights is participation. Certainly, since the establishment of the IRSA, significant attempts have been made by the IRSA in practice to facilitate participation. Consultation is central to the IRSA's obligations, as seen in section 40 of POPIA. Public consultations were held in each province to facilitate comments on the first swathe of proposed regulations in 2017.[114]

And an extension of this participation, is the accountability of the IRSA to parliament who can help act as representatives of the public on certain issues. Yet, given particularly the digital divide that marks the South African landscape, the centralisation of the office in Johannesburg (with no capacity yet for provincial offices) severely limits the ability of citizens to participate directly in IRSA events.[115]

Participation should extend to accessibility – which is an issue of innate concern in the South African landscape. Years of implementation challenges in relation to PAIA have highlighted the limitations of recourse in relation to the law being facilitated by courts, given costs, delays, and other direct accessibility challenges.[116] The creation of the IRSA is a direct response to this challenge for both POPIA and PAIA, yet the current

114 A schedule of these hearings is available at: https://justice.gov.za/inforeg/docs/InfoRegSA-Regulations-Invite-20171108.pdf

115 Interview with Varsha Sewlal, 12 October 2020. Op. cit.

116 Peekhaus, W. (2014). South Africa's Promotion of Access to Information Act: An Analysis of Relevant Jurisprudence. *Journal of Information Policy, 4*, 570-96. https://doi.org/10.5325/jinfopoli.4.2014.0570

budgetary constraints limit the direct accessibility to this recourse given the single issues. As the chairperson herself noted presenting to parliament:

> The number of data breaches in the public and private sectors, the unlawful and unauthorised use of personal information of individuals, cyber-crime and identity theft were increasing at an alarming rate. Until the remaining sections of POPIA were brought into effect, the Regulator was unable to enforce compliance and victims were deprived of an appropriate remedy. It was for that reason that the Regulator had written to the Minister of Justice and Correctional Services to request him to bring the remaining sections of POPIA into effect during the 2020/21 financial year.[117]

The IRSA is currently trying to procure an online complaints filing system to help manage this, though obviously low levels of internet penetration in rural areas, in particular, and high data costs threaten its full effectiveness.[118]

Accessibility will continue to be a realistic challenge to both non-discrimination and equality, restricting equality realities along the rural/urban divide, gender, and income as a direct expression of the digital inequalities addressed in our examinations on context.

## Accountability

Accountability is, of course, directly referenced within POPIA as a lawful processing ground. However, the reality of accountability requires investigations outside of the straight wording of the law.

117 Tisné, M. (2020). *The Data Delusion: Protecting Individual Data Isn't Enough When The Harm Is Collective*. Stanford Cyber Policy Center. https://cyber.fsi.stanford.edu/publication/data-delusion

118 Interview with Varsha Sewlal, 12 October 2020. Op. cit.

The positive obligations of responsible parties to facilitate these lawful processing grounds form a direct kind of accountability – and vitally extends to both public and private sector bodies. Yet, the POPIA expressly excludes from its remit cabinet, or processing by a public body involving national security and law enforcement functions.[119] While the national security and law enforcement exclusions are at least attenuated by the inclusion of the phrase "*to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information*", it is hard to understand why the blanket exclusion for cabinet exists (though it is reminiscent of the similar blanket exclusion in PAIA, as well).

This links to a chief emerging concern in the South African context: both the capacity, and political will, for ensuring data protection compliance within the public sector itself.[120] Public sector accountability is of primary importance, given the public sectors role in data collection *en masse* given its social development functions. Broadly POPIA recognises this role, which was again raised as a consideration within the SALRC recommendations.

The codes present an alternative form of accountability, which expands the role of the private sector in supporting sound data practices.

The existence of "alternative" remedies within the POPIA will help support accountability, and especially their broad supportive powers given to the IRSA such as seen in their ability to *mero motu* investigate and assess, but also in their ability to support civil claims on behalf of data subjects.

119 Protection of Personal Information Act, 2013, s 6.

120 This is the subject of a case study that I will soon be publishing in partnership with the London School of Economics, and confirmed by: Interview with John Giles, 5 October 2020. Op. cit.

## Legality

Certainly POPIA is broadly consistent with both regional and international best practice on data protections in its drafted form. Yet the political inability to provide the IRSA with both budgetary support, and even delays in the effectiveness of its provisions, have severely undermined the practical reality of this "consistency". For instance, the African Union Commission and Internet Society's Personal Data Protection Guidelines for Africa, 2018, recommend that states establish an independent DPA to ensure their national privacy and personal data protection laws are being observed. The DPA should have a clear mandate, powers and resources to be able to:

- Monitor compliance with, and enforce, applicable law on privacy and data protection.
- Engage with other stakeholders (such as governments, data controllers, civil society) to develop regulatory guidance, trust frameworks, and enabling measures such as stakeholder education.
- Inform people and data controllers about their rights and obligations.

While the legislated powers, duties and obligations of the IRSA are consistent with instruments such as these, this report has already noted how the actual implementation is being challenged by both political apathy, and budgetary limitation.

This political apathy has historical precedent, with a prioritisation of data collection by the state before data protection. This will remain a threat to the data protection environment, and concomitantly also undermines the IRSA's capacity to constrain, and guide, the private sector in its fulfilment of the POPIA.

## Empowerment

Empowerment of citizens will remain a foreseeable challenge in the South African data protection environment. The IRSA already considers one of its most significant challenges being to expand the understanding of both privacy rights, and privacy risks, to the public at large.[121] In addition, marginalised users may be passive in digital environments, or simply not incentivised to exert their privacy rights. Education alone will not change cultures on exerting rights in the South African context.

The African Declaration on Internet Rights and Freedoms, 2016 highlights that privacy and data protection also require that:

> The collection, retention, use and disclosure of personal data or information must comply with a transparent privacy policy which allows people to find out what data or information is collected about them, to correct inaccurate information, and to protect such data or information from disclosure that they have not authorised.

This highlights the fundamental importance of the POPIA's creation of data subject rights. These rights facilitate access but emphasise to the individual capacity of a data subject to exert some control over their own data reality. It both protects personal privacy, and moves forward beyond the rights of personal identity as necessary collaborative partners.

Yet this individualised empowerment may not serve marginal communities in the whole, and many forms of data harms will in fact be collective.[122] Certainly African human rights discourse

121 Interview with Varsha Sewlal, 12 October 2020. Op. cit.

122 Tisne, M. (2020). Op. cit.

has always strongly focused on collective rights (let us not forget it is this communal nature that at one time inhibited acknowledgements of privacy), and the important question will become how collectivist understandings of law – facilitated by class actions or even collective forms of protection like data trusts – will emerge as important human rights articulations of *ubuntu* that can make empowerment a firmer reality.

## Conclusion and recommendations

There is seldom historical and contextual analysis with a human rights focus to inform the analysis of South Africa's data protection landscape. Understood largely as an economic imperative, significant focus is placed in the public discourse on private sector compliance. This undermines two essential realities of the context:

- The role of the public sector as a data processor
- The role of POPIA as a form of data subject empowerment in respect of both access to information *and* privacy.

The delays in ensuring the full, and capacitated, effectiveness of the IRSA have significantly undermined the law's generally sound provisions. It is impeding empowerment in relation to data subject privacy rights, but also their access to information rights that have been struggling for realisation since the passing of the PAIA in 2000.

Certainly the law will not be enough, and the existing digital economy reality in the country will require coordination of the enabling policies on issues of ICT and digital industrial policy to align with data protection imperatives. This again reiterates the need for an active IRSA, that can help ensure human rights based debates are included within these typically "economic-only" discussions.

Human rights should remain the central, informing normative parameters for data protection and data access, and within this frame the empowerment of the public (and data subjects) is both highlighted, but also attenuated by an African discourse that requires us to more readily feature both the collective harms, and protections, that the future of privacy protection in South Africa should consider.

Recommendations for the private sector:

- The private sector should collaborate responsively in relation to the development of codes of conduct to both enhance accountability and give recognition to important sectoral considerations.
- The private sector should prioritise equally their privacy and access to information obligations.
- The private sector should start implementing lawful processing practices immediately given the POPIA will be fully effective midway through 2021.

Recommendations for the IRSA:

- In the short term, the IRSA should focus on procuring and implementing an effective online complaints lodging system to facilitate public recourse.
- Other accessibility priorities should be explored, such as WhatsApp channels, and provincial roadshows.
- Public education should focus on explaining the realities of privacy rights, including mechanisms for empowering the public to improve their own data protection.
- In the medium term, the IRSA should begin designing procedures to facilitate effective support for data subject claimants in relation to civil claims.

- Data processor outreach must include both private and public sector educational campaigns.
- Outreach should include coordination and cooperation (regionally and domestically) with regulatory authorities of relevance to ensure human rights priorities can be forwarded.

Recommendations for public interest lawyers and civil society:

- Feasibility studies should be conducted into forms of data trusts and data stewardship models that might help realise collective privacy protection.
- Feasibility studies should be conducted into public interest litigation, including collective consideration of class action suits, to forward data privacy from a human rights perspective.
- The public interest imperatives in driving the full realisation of the protection, promotion and respecting of access to information must continue to be of central importance, largely through the forwarding of effective implementation of PAIA.

Recommendations for the public sector:

- The public sector must ensure internal compliance with the POPIA as a matter of urgency.
- The public sector should demonstrate political will both in prioritising data within the digital economy, but also for sound data protection practices as its necessary foundation, and to ensure public trust through the active promotion, protection and respecting privacy and access to information rights.

## Annexure A: Methodology

The selected methodology for this research was heavily influenced by its roots as practitioner-based participatory action research.[123] Given the desire to both leverage the lived experience of the author in this area of work, and also focus on identifying practical opportunities for existing practitioners in the area, it was clear that a qualitative method would be the most appropriate. This qualitative evidence was analysed through a human rights-based lens, which also incorporated political economy questions for the broader issues of context.

The primary research questions were:

- What is the current data protection landscape in South Africa?
- What influences are impacting the data protection landscape?
- (Given the answers to questions one and two) What are the priority policy areas for the different stakeholders to create positive influences on South Africa's data protection landscape moving forward?

To understand the preliminary considerations of context in relation to South Africa's data protection landscape, desktop research was done into the contextual background, and secondary source literature was supplemented by primary sources, such as:

- Parliamentary meeting transcripts
- Case law and statute
- Policy documentation.

123 Babbie, E., & Mouton, J. (2004). *The Practice of Social Research*. Oxford University Press.

Additional primary source material was generated through interviews. Since the research was largely pursued under participatory action research, these interviews were with in-country experts, which were conducted such as:

- Interview with Varsha Sewlal, Executive: Legal, Policy, Research and Information Technology Analysis, 12 October 2020
- Interview with John Giles, Managing Attorney, Michalsons Attorneys, 5 October 2020.

The interviews were conducted as semi-structured for two key reasons: firstly, to build trust and ease between interviewer and interviewee and improve the potential conversation flow, and secondly, to ensure the research did not through prescription block itself off from areas of inquiry that may not have been properly foreseen during the initial stages of research design. This is consistent with standard qualitative interview techniques:

> Design in qualitative interviewing is iterative. That means that each time you repeat the basic process of gathering information, analyzing it, winnowing it, and testing it, you come close to a clear and convincing model of the phenomenon you are studying. […] The continuous nature of qualitative interviewing means that the question is redesigned throughout the project.[124]

A scheduled formal interview with a representative of the SAHRC had to be cancelled given personal circumstances of the interviewee, but the researcher was nevertheless able to leverage previous conversations with the SAHRC in public fora, as well as outcomes from the SAHRC's "4IR and Human Rights: Challenges and Opportunities for National Human Rights Institutions" workshop held on 5 and 6 March 2020, for background context.

124 Ibid.

# Tanzania

Rebecca Ryakitimbo[1]

## Executive summary

Tanzania has, in the last five years, moved from a green-light to a red-light country where digital rights are concerned. The recent past has shown much progress towards legislating restrictions rather than legislating protections, hence the reason why to date the data protection and privacy bill has not progressed nor have its provisions been made public. Tanzania's data protection policy has been in the form of a bill since 2014 and has not progressed since. With the country deploying digital mechanisms for collection of data, including the registration of citizens via the National Identification Authority (NIDA), which allows telecoms to get hold of data such as biometrics, there is yet to be one specific piece of legislation that addresses data protection concerns.

1 This research was carried out with contributions from anonymous contributors representing renowned lawyers, policy and government experts. It documents the development of the data protection and privacy bill of Tanzania in efforts to foster a rights-based policy development process.

Although the Constitution of Tanzania (under Article 16) guarantees the right to privacy it also provides some contradictions in relation to the presence of other laws to which this right shall not be applied. The constitution further explains that rights and freedoms provided for do not render unlawful any law or any act done according to such law to ensure that the rights and freedoms of others are protected. Hence the constitution alone cannot be the one piece of law that ensures privacy, although it does guarantee it.

Despite the lack of a comprehensive data protection and privacy law, Tanzania has certain pieces of legislation that impact data protection and privacy both negatively and positively, such as the Electronics and Postal Communication Act (EPOCA) regulations, the Cybercrime Act 2015 as well as the Registration and Identification of Persons Act, among others. The presence of such laws does not in any way fill the need for data protection and privacy laws.

Laws in Tanzania are yet to guarantee the right to communicate anonymously on the internet and the use of appropriate technology such as VPNs, hence the country is a long way from realising Principle 8 of the African Declaration on Internet Rights and Freedoms (AfDec) and its applications. The presence of different mechanisms and agencies that require the collection of data from users puts rights holders at risk as long as there is no net to fall back on, in case of a breach or infringement of the “right to privacy”. To strengthen the privacy and data protection framework, Tanzania ought to legislate a comprehensive data protection and privacy policy, ratify the Malabo convention (which it has an obligation to do as a member of the African Union), adopt a multistakeholder approach for policy development, and harmonise existing laws to ensure data protection and privacy are ensured. In line with this, it is essential that mechanisms such

as the UPR and others are enforced and their recommendations taken into consideration and addressed with urgency.

To develop a compressive piece of legislation it is important that a human rights-based approach is employed to ensure participation, empowerment, and inclusivity of all people as this is the only way to ensure a people-centred policy. Localisation of bills should be a key priority to ensure such technical terms and provisions are clear and in a language spoken by the masses, i.e. Swahili. The same urgency used on legislating restrictions should apply to legislating protections such as the data protection and privacy policy.

## Methodology

The research employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews. Desk research on shadow reports, policy briefs, academic works, government documents and other literature was conducted.

These reviews help to build an understanding of the developments in the drafting of the data protection and privacy bill in the country. A legal and policy analysis was done to ensure that pieces of legislation and practices existing that touch on data protection and privacy were captured.

Such laws and policies include those that govern the protection of data and privacy in different sectors, including government agencies and public service agencies.

Key informant interviews were conducted through phone calls and one-on-one interviews with purposely-selected respondents. These included staff of government institutions, telecoms companies, rights holders, CSOs and lawyers.

## Tanzania country context

Tanzania is an East African country with a population of 55.9 million as of 2019.[2] Tanzania's National Strategy for Growth and Reduction of Poverty gives the highest priority to the eradication of poverty.

Tanzania has, since the inception of multipartyism in 1995, been under the rule of Chama Cha Mapinduzi (CCM) party, with fierce opposition growing in the last decade as more opposition parties emerge.[3] In 2015, President John Pombe Magufuli came into power, his regime has been instrumental in implementing a clampdown on corruption and improving public services towards the industrialisation of the economy. However, his government has faced criticism from human rights and international organisations as far as human rights are concerned. Sources have claimed that his regime has greatly undermined and stifled the voice and freedoms of citizens leading to political instability and violations of the rule of law.[4]

Over the past six years, the country has taken steps towards legislation and policies to regulate the digital space. The Cybercrime Act was enacted in 2015 and a number of laws, including the EPOCA regulations, have been regularly amended to encompass several issues. However, the data protection and privacy policy has been stagnant and there has been little or no progress on the issue.[5]

2 National Bureau of Statistics. (2020). *2019 Tanzania in Figures*. http://www.nbs.go.tz/nbs/takwimu/references/Tanzania_in_Figures_2019.pdf

3 https://www.nationsonline.org/oneworld/tanzania.htm

4 The World Bank. (2020, 13 October). The World Bank In Tanzania. https://www.worldbank.org/en/country/tanzania/overview

5 The Citizen. (2015, 5 April). Why proposed law on data privacy is too little, too late. *The Citizen.*

Most stakeholders have noted that the data protection and privacy bill seems to not be a priority to the country as we have seen other short-term bills that came to parliament and got passed in a short time while this particular bill has taken years to mature. Concerns include the burden of cost that comes with the bill since a data protection agency will need to be established which is a budget item that simply doesn't seem to be a priority at the moment. An independent body called the Tanzania Communication Regulatory Authority (TCRA) handles regulation in this sector. The authority was established under the TCRA Act no. 12 of 2003.[6] Institutions that have a hand in the development of data protection and privacy include parliament, the TCRA and the Ministry of Works, Transport and Communication.

## Constitutional underpinning

Article 16 of the Constitution of the United Republic of Tanzania recognises the right to privacy. It states that "every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications."[7]

According to *Tanzania Data Protection Overview* by Francis Kamuzora and Chris Green, there are limitations to this protection as cited in Article 30 of the constitution, which states that:

- The rights and freedoms provided are not to be exercised in a manner which infringes on the freedoms of other persons or public interest.
- The rights and freedoms provided for do not render unlawful any law or any act done pursuant to such law for the purpose

6 https://www.tcra.go.tz

7 http://www.parliament.go.tz/uploads/documents/publications/en/1475140028-The%20Constitution.pdf

> of ensuring that the rights and freedoms of other people or the interests of the public are not prejudiced, ensuring defense, public safety, public peace, public morality, etc., to name just a few.[8]

This leaves room for privacy to be violated under certain circumstances such as when a provision of another law allows. An example of this is the Electronic and Postal Communications (Investigation) Regulations of 2017 (the EPOCA Investigation Regulations), which empowers the state law enforcement organs to tap into private telecommunications for purposes of investigation, upon obtaining a warrant for that purpose.

## Existence of other laws dealing with privacy and data protection online

Despite the lack of comprehensive data protection and privacy law, there are certain pieces of legislation that impact data protection and privacy both negatively and positively.

- The EPOCA Online Regulations (2018 and 2020): This act prohibits disclosure by the TCRA of any information obtained by it in the course of its duties or exercise of its functions as well as any person from intercepting any communication at any place in the country except as provided under the EPOCA Investigation Regulations. Under regulation 5(1)(f) it requires content providers to "have in place mechanisms to identify sources of content". This obligation poses a threat to the right to anonymity and whistleblowing and may lead to self-censorship.[9]

8 Green, C., & Kumazora, F. (2019). *Tanzania Data Protection Overview*. DataGuidance. https://www.dataguidance.com/notes/tanzania-data-protection-overview

9 http://www.tcra.go.tz/regulatory/The%20Regulator%20Special%20Edition

- The Cybercrimes Act: The act makes it an offence to intercept personal communications and interfere with data by damaging, deleting, altering, obstructing and interrupting it. The Cybercrimes Act also prohibits operators and other service providers from monitoring activities or data being transmitted in their systems. However, it provides an exception for investigation purposes for the disclosure of information, which leaves room for undermining of rights under the pretence of investigations.[10]
- The Registration and Identifications of Persons Act (1986): While this particular act provides for specific protection of persons' identities, it gives the minister in charge broad powers to decide on exceptions for sharing such data. Provision IV of this act states that "the registrar and registration officer and any immigration officer performing functions under this act shall not produce for inspection or supply copy the photograph, of any person registered under this act or his fingerprints or disclose or supply a copy of particulars furnished under section 7 and 9 except and unless with the written permission of the minister."[11]
- EPOCA SIM Card Regulation: Under general provision part IV, section 20 the regulations states offences on misuse of information citing: "Any licensee, dealer or agent who misuses information of a customer for SIM Card registration commits an offence and upon conviction shall be liable to a fine of not less than five million Tanzanian shillings [USD 2,156.233] or imprisonment for a term not less than twelve months or both."[12]

10 http://www.parliament.go.tz/polis/uploads/bills/acts/1452061463-ActNo-14-2015-Book-11-20.pdf

11 http://www.parliament.go.tz/polis/uploads/bills/acts/1566541530-The%20Registration%20and%20Identification%20of%20Persons%20Act,%201986.pdf

12 http://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(SIM%20Card%20Registration)%20Regulations,%202020

## Regional and international commitments on privacy and personal data protection

### General Data Protection Regulation (GDPR)

Although focused on European citizens, the GDPR applies in jurisdictions outside the EU provided they handle personal data of EU citizens. It has set a pace on the need to ensure data protection and privacy across continents, where accounting of how and why subjects' data is processed; and upon request, providing subjects with copies of their data in a machine-readable format. Further, other rights that accrue to the data subject such as the right to erasure, data portability, consent, right to know, rectification, and right to be informed, have been prioritised.[13]

### African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)

The convention provides a guideline through its provisions on the legal framework for data protection and privacy. Furthermore it mandates the member states to set up data protection authorities that are independent and ensures that the laws developed across the continent are in harmony if they follow the convention. Article 13 of the convention states the basic principles to govern the processing of personal data such as consent and legitimacy, lawfulness and fairness, purpose, relevance and storage, accuracy, transparency, confidentiality, and security of data.[14]

13 CIPESA. (2018). *Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa*. https://www.cipesa.org/?wpfb_dl=272

14 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

## East African Community framework for cyber laws

The framework was drafted in 2008 and divided into frameworks I and II, of which the implementation is ongoing. It covers mostly cybersecurity concerns but also shows concern over data protection and privacy within the region.

In Article 2.5, the framework recognises the need for comprehensive data protection and privacy policy within the region. The framework here is used to describe those obligations placed upon those entities that process information about living individuals, generally referred to as “personal data”. The framework identifies minimum obligations which represent international best practice in the area:

- Compliance with certain “principles of good practice” in respect to their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security.
- To supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended.[15]

These treaties and/or regulations provide a framework which Tanzania can build on to develop data protection and privacy laws that are not only sufficient to address concerns but provide room for harmonisation across continents and countries. They provide the basic principles and underlying provisions for data portability, among others. Their relevance stems from the need for data rights accorded to citizens of other nations across the globe being reciprocated to Tanzanian citizens as well.

15 http://repository.eac.int/handle/11671/1815

## Data protection and privacy law in Tanzania

Tanzanian data protection and privacy law has been a bill for a number of years, although sources report that the ministry and relevant bodies are in the process of developing a more comprehensive policy that will soon come to light. As of June 2020 Tanzania had not yet ratified the Malabo Convention on data protection and privacy, according to the AU convention status report.[16] In varying degrees pieces of different legislation address some data protection and privacy concerns, however this is limited to specific privacy concerns.

Hence, the said pieces of legislation such as the EPOCA regulations and the Cyber Crime Act do not address concerns such as how data is collected, handled and maintained, making them overly broad to ensure rights. There are discussions about the draft bill, but the government has not yet publicly confirmed when it will be published for public review and opinion.

Bits and pieces of varying legislations implement data protection and privacy on a lower scale by touching on a few privacy concerns but do not specifically address all data protection and privacy concerns as we await the bill that will focus on that.

## Challenges to implementation of a data protection and privacy policy in Tanzania

Key challenges include:

- The lack of a comprehensive single piece of legislation: Without a single legislation focused only on data protection and privacy concerns, Tanzania cannot implement what does not exist. Hence the first and foremost building block to ensuring implementation is the development of a policy.

16 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

- The cost implications: While a policy development process is a government item based on government priorities at the time, the costs associated with such a process may be pending till the government makes it a priority. Costs, such as to establish a data protection agency with required personnel and resources, are often not high up on priority lists of governments.
- Lack of transparency on bill's status: Different sources state that the bill is underway but since it was first mentioned in 2013 there has been no information made public. The lack of transparency of the state of the bill leaves a lot to be desired, one cannot implement a policy that is not publicly available nor are stakeholders provided with the draft to help ensure it is people centred from the start of the development process. As the saying goes "nothing for us without us".
- Contradictory different pieces of legislation: The existing laws and policies that give access to data for specified reasons leave room for violations of the right to privacy in some instances. While the constitution guarantees "the right to privacy" it leaves room for other laws to override this in specified circumstances. The irony of this is when a data protection and privacy policy is developed there is a possibility of it being limited by provisions existing in other laws such as the Cybercrime Act.

Some of the key data protection issues in Tanzania include:

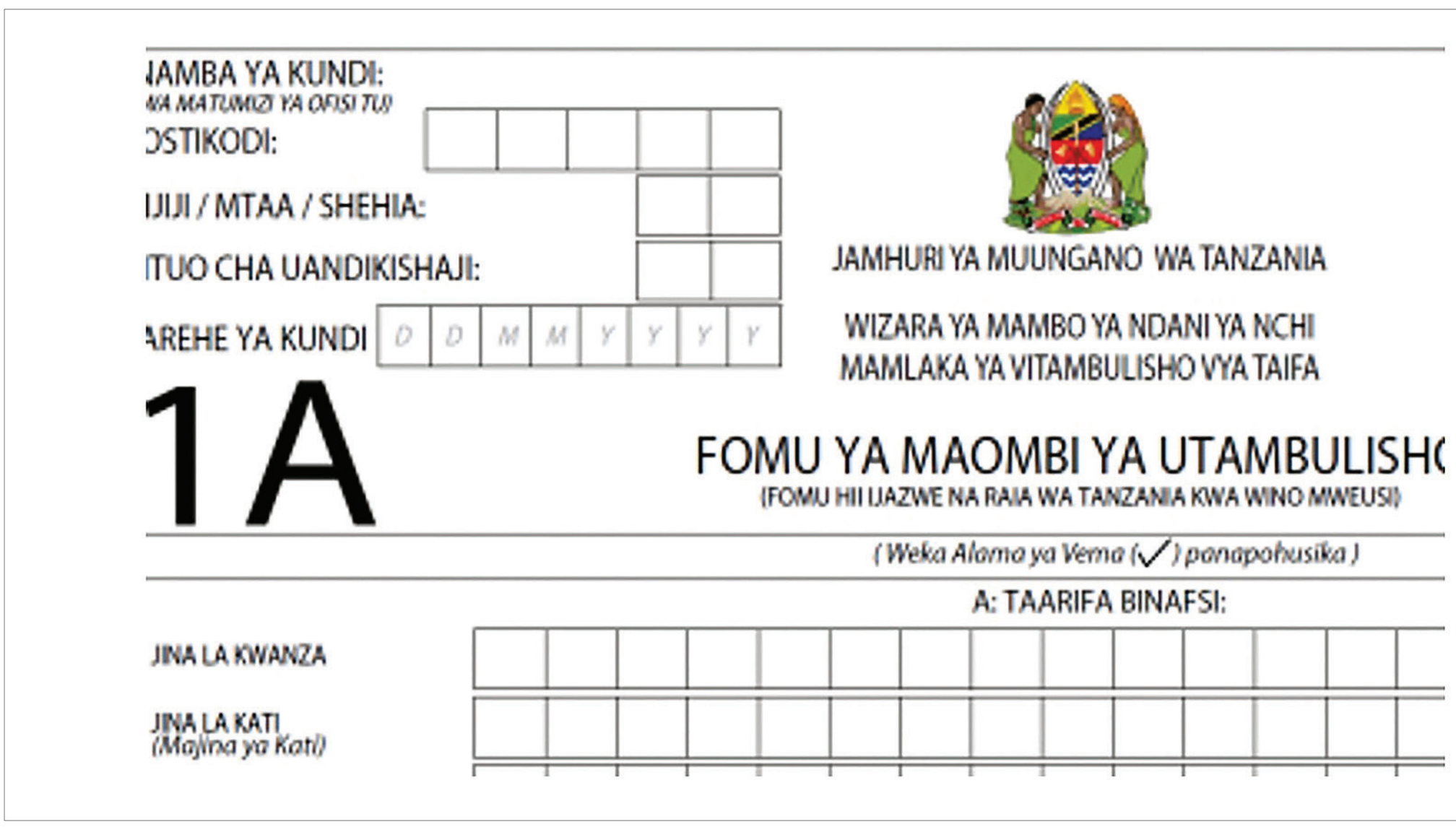
- Collection of biometric data by service providers: While providing a legal identity for each resident is progressive, not legislating protections ahead of such a task is not. Most registrars are exposed to the extremely personal data of users with little or no information given to the rights holders on how they can ensure their rights are respected. Most

users are aware that the government has made it mandatory to register SIM cards alongside their biometric data but are not aware of the specifics guiding this regulation and/or how their data is protected. Under the EPOCA SIM card regulations of 2020, biometric registration of SIM cards by all users (whether visitors, residents or citizens) is required. This registration of SIM cards requires an individual to submit his or her NIDA number or card to the telecoms provider. The service provider will then conduct online or electronic fingerprint verification of an individual with NIDA for biometric SIM card registration. After the search, the provider will keep the subscriber's records as per details electronically retrieved from NIDA, and then register the SIM card bearing the name of the individual.[17]

- The roll-out of the national identification system: The National Identification Authority (NIDA) was established by the National Identification Authority (Establishment) Instrument, 2008 with the mandate to register and issue identity cards to Tanzanian citizens and eligible residents who are non-citizens aged 18 years and above in accordance with the Registration and Identification of Persons Act (Act No.11 of 1986) Revised Edition 2012.[18] This requires the collection of personal information such as names, area of residence and date of birth as well as biometric data such as fingerprints to be enrolled in the system and provided for a national identification number commonly referred to as "NIDA number". The NIDA number is mandatory for one to register a SIM card or to open a bank account or gain access to public services.

17 http://www.tcra.go.tz/regulatory/The%20Regulator%20Special%20Edition

18 https://www.velmalaw.co.tz/wp-content/uploads/2017/03/LEGAL-RESIDENT-REGISTRATION-ADVERT-07032017-J4-EDITED.pdf




NIDA registration form.

IMAGE SOURCE: https://www.ajirasasa.com/2020/09/fomu-za-usajili-wa-kitambulisho-cha-taifa-nida-nida-registration-form.html

Currently, the Ministry of Transport, Works and Communications, and its subsidiaries such as the independent regulatory body TCRA, are working towards the draft that will hopefully be available for comments and review by the public and other stakeholders before being tabled to parliament in the near future.

## Data protection and privacy in Tanzania's existing laws

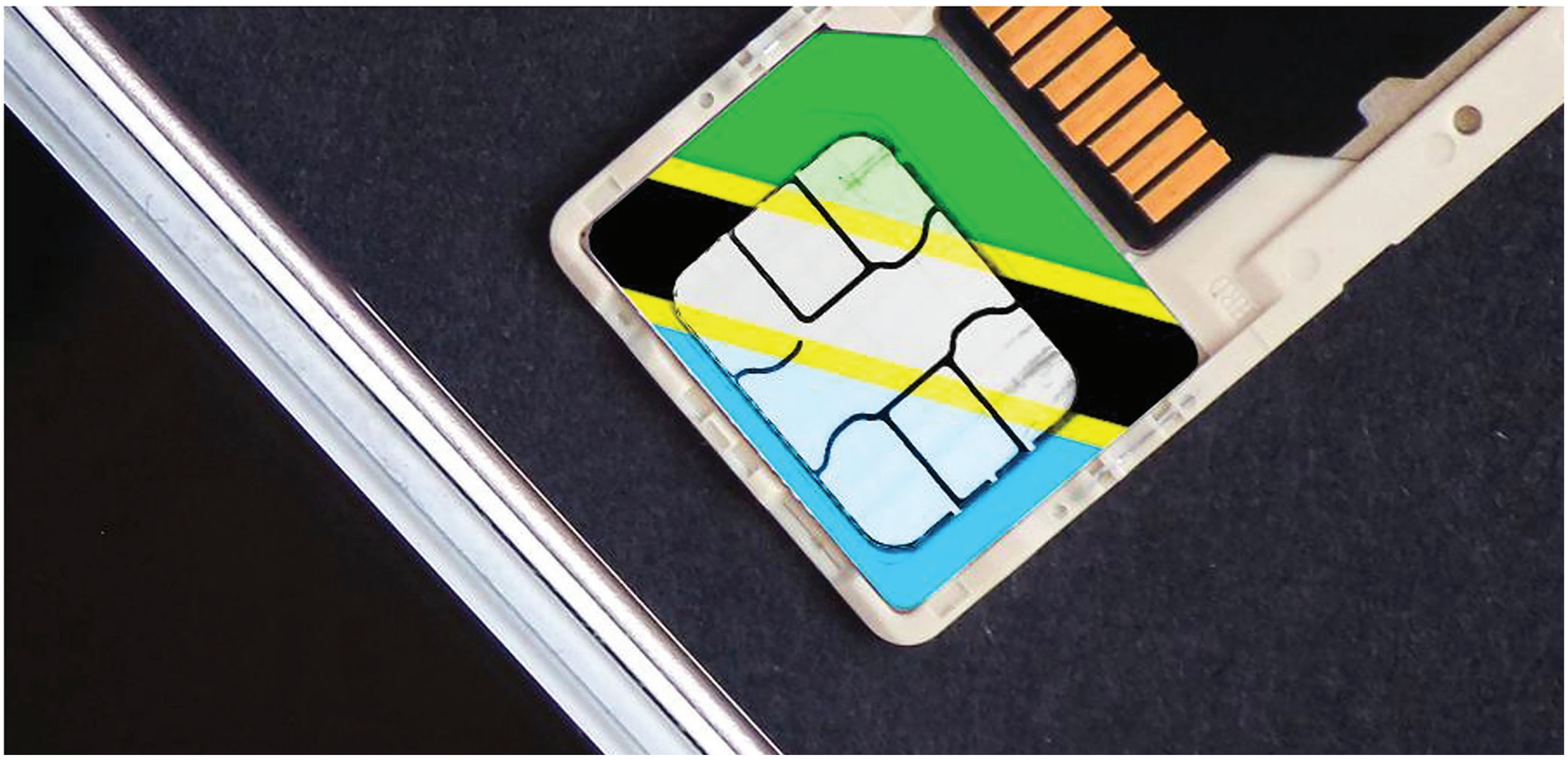
The following pieces of legislation, though not focused entirely on data protection and privacy, do address some specific privacy concerns and exemptions to access to data:

- EPOCA SIM card regulations
- EPOCA online regulations
- Cybercrime Act 2015
- Registration and Identification of Persons Act 1986.

From these acts and regulations some key definitions are provided that to some extent address data protection and privacy, although not entirely. Under the above laws the authority in charge of all that the laws, including data protection and privacy, relate to is referred to as the Tanzania communications regulatory authority established under the Tanzania Communications Regulatory Authority Act. This proves that a heavy burden rests on the shoulders of the TCRA, which seems to be tasked with many responsibilities from licensing to control of the digital landscape including data.

The laws further describe a “consumer” as any person who uses electronic communications or postal products or services. Generally tallying users under the “consumers” tag and not specifying them as data subjects, could once again be corrected if a specific law was in place to protect data and privacy. The EPOCA SIM card regulations also refer to “individual biometric SIM card registration category” as a category whereby biometric registration of SIM cards are to be used solely by a customer for personal use. Most rights holders fall in this category and are compelled to provide such data. During SIM card registration the “integrated circuit card identifier” is also collected. This integrated circuit card is a unique serial number that is printed and stored in the SIM card of a subscriber, and is an internationally standardised way of identifying a SIM card. As a result the tracking of individuals is made very easy even where a user or customer in this case changes their SIM card.

The laws describe “interception” in relation to a function of a computer, including acquiring, viewing, listening or recording any computer data communication through any other means of electronic, or other means, during transmission through the use of any technical device. Despite its good intention it leaves out



SIM card registration through use of the NIDA number known as NIN.

IMAGE SOURCE: https://furtherafrica.com/tag/national-identification-authority/
IMAGE SIGNIFICANCE: Sim card registration through use of NIDA number known as NIN

interception by other devices such as surveillance and/or mobile phones hence it only refers to interception via computers.

In particular, the Cybercrimes Act describes “computer data” as any representation of facts, concepts, information, or instructions, in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function. While it describes data within its context as a law, it does not define data from the perspective of its types such as personal and biometric data. In this case a “service provider” refers to a person or party that makes information system services available to third parties, hence telecoms providers fall under this category as those who provide telecommunication services.

Under the EPOCA online regulations “content” is referred to as information in the form of speech or other sound, data, text or images whether still or moving except where transmitted in

private communications. This definition partly guarantees data protection by stating that private communications should not be referred to as content for the public. Under the Cybercrime Act and EPOCA regulations, a “PIN” is an acronym for personal identification number; this is made mandatory for every SIM card holder to have in order to access service, partly a mechanism to ensure protection and privacy of consumers’ data.

Although there are varying terms described in each of these legislations that refer to data protection and privacy they are still very much tied to specific concerns of each legislation and not data protection and privacy overall.

There are some data subjects’ rights provided for under each of mentioned pieces of legislation within their scopes. For example, under the Cybercrime Act, the data subject has the right “through a take-down notification, to notify the service provider of any data or activity infringing their rights under Provision 45.” They also have the right to correct their information or data collected by a provider of services, i.e. change of SIM Card number, etc., although this is stated more as an obligation than a right in the respective legislations.

The above pieces of legislation do not specifically address conditions for the lawful processing of data but do impose mechanisms or provisions that identify when data should be collected for what purpose under each said piece of legislation.

- The Registration and Identification of Persons Act specifically states data to be collected for registration purposes.
- The SIM card regulation also states data to be collected and the procedures of how such data will be handled specifying the authorities that will keep copies of data.

Both laws provide for fines or penalties for unlawful processing of any such data/information collected for the purpose specified in each piece of legislation. However, this does not entirely address or qualify as conditions on processing but rather guidelines under each legislation on how their data is processed.

There are specific instances in which an individual can request to be exempted from providing their information as specified below:

- The Registration and Identification of Persons Act allows the provision of the “power to exempt” in a situation where the minister by order published in gazette may exempt any person/category of persons to comply. The provisions further give persons the right to ask for exemption where they claim that the act does not apply to them; however, the burden of proof lies with them.
- Section 6 of the SIM card regulations also provides exemption on data collection, such as, “A customer from Government institution or an authorized agent of the Government who requires an exemption of biometric SIM Card registration shall apply the following procedure:

  (a) A customer shall write a letter to the Authority to obtain approval for fingerprint exemption and shall provide details for such exception;

  (b) A customer shall be required to present his NIDA identity and the Authority approval to the service provider for SIM Card registration; and

  (c) The service provider shall register SIM Cards as per the approval of the Authority at customer centers, service providers’ shops, or agents’ shops only.”

## Institutions assigned with the responsibility to oversee rights to personal data protection

There are no specific institutions assigned with the responsibility to oversee rights to personal data protection in Tanzania. Instead, institutions abide by their mandates, which to some extent oversee some rights to personal data protection.

However, the Tanzania Communications Regulatory Authority (TCRA), a quasi-independent government body, was established with the responsibility of regulating the communications and broadcasting sectors in Tanzania. It was established under the Tanzania Communications Regulatory Act No.12 of 2003 to regulate electronic communications, postal services and management of the national frequency spectrum in the United Republic of Tanzania.[19]

Since Tanzania does not yet have a specific piece of legislation that mandates an establishment of a data protection authority, that duty currently in some ways falls under the authority of TCRA.

TCRA has the duty to protect the interests of consumers including enhancing public knowledge, awareness and understanding of the regulated sectors.

## Effectiveness and challenges of TCRA

Since its establishment TCRA has been instrumental in providing oversight in the communications sector. It serves as the body that oversees the implementation of policies, legislations and regulations that apply to its mandate. However, issues such as data protection and privacy fall on its lap only because there is no

19 https://www.tcra.go.tz/about-tcra/tcra-profile

specific legislation nor policy established for this purpose. So far, TCRA has 142 written regulations, 89 enforced policies, and over 17 years of experience. However, handling privacy and data protection is a challenge. The scope of data protection and privacy is broad and needs specific laws and a body to handle its issues specifically. With various legislations in place that have had a “here and there” touch of addressing data protection and privacy, TCRA finds itself as the middle man that has to be able to address each specific legislation’s approach towards data protection and enforce it.

## Organisations and associations involved in advocacy related to data protection

Over the years civil society human rights groups and activists have raised concerns regarding different privacy issues within Tanzania. Ranging from how telecoms service providers handle data and the privacy of consumers’ services to the protection of privacy of special groups within communities. Local, regional and international NGOs have also been instrumental in trying to put forth their concerns where data protection and privacy are concerned.

Some institutions that have made known their concerns over the years include:

- The Tanzania Human Rights Defenders Coalition (THDRC): An organisation that has submitted concerns through the universal periodic review (UPR) UN mechanism emphasising the protection of data and respect of privacy that specifically affect Tanzania. Locally it has condemned actions such as interception of phone calls that was rampant in the year preceding the election year by issuing statements and commenting on draft bills in parliament. THRDC has been instrumental in leading various organisations to form coalitions to give input within and outside Tanzania,

successfully presenting their recommendations to the government of Tanzania at the UN human rights council.[20]

- The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as well as Paradigm Initiative (PIN) have also played a critical role within the region to ensure privacy and data protection concerns are addressed. This includes the publication of policy briefs, legal analysis and country reports, joint submissions of open letters among others to insist on the need for data protection and privacy legal frameworks.

## Data protection and privacy in SIM card regulation and public health concerns

The EPOCA SIM Card Regulations 2020 provide an obligation to all service providers who can be referred to as data controllers to keep and secure the details of all who register their SIM cards. These service providers, dealers and whoever is involved in collecting or processing such data, upon any misuse of information of a customer for SIM card registration, are considered to commit an offence and upon conviction shall be liable to a fine or imprisonment or both. However, such protection of privacy is for the SIM card customers and the only data being protected is data of the person related to SIM card registration only.[21]

The privacy concerns of public health systems and health insurance are partly addressed, however the dimensions of privacy are only within the specific role of the legislation and all other privacy issues not directly linked to the core purpose of the relevant legislation are not addressed. For example, the

20 Olengurumwa, O. (2019, 28 July). Advice on the situation of privacy and communication security in Tanzania. *Tanzania Human Rights Defenders Coalition*. https://thrdc.or.tz/advice-on-the-situation-of-privacy-and-communication-security-in-tanzania

21 http://www.tcra.go.tz/regulatory/The%20Regulator%20Special%20Edition

HIV and AIDS (Prevention and Control) Act (2008)[22] addresses privacy issues but only for identified victims of HIV and AIDS. All these regulations only touch on a small section of data protection and privacy and hardly cover the entire area as a whole nor do they address clearly the principles of data protection and privacy, as would a data protection and privacy-focused policy if enacted.

With the introduction of the national identification number (NIN) being mandatory, the number and/or identification is used as a prerequisite for access to services from various agencies. These agencies are able to collect the data of consumers with insufficient guidelines on this. This includes local agents of telecoms that collect fingerprints and have access to records from NIDA; the same applies to banks, health insurance agencies that all have immense access to personal data. Despite the presence of specific regulations that address how such sectors handle data, the pieces in themselves are not sufficient to guarantee protection in totality.

## Data protection practices in .tz ccTLD registration

The Tanzania Network Information Centre Limited (tzNIC) was introduced in Tanzania on 16 November 2006 as a non-profit limited company with the sole purpose to "control, manage and operate" the .tz country code top-level domain (ccTLD). TzNIC members are composed solely of TCRA and the Tanzania Internet Service Providers Association (TISPA), an association of major ISPs operating in Tanzania. On 18 October 2018, the members of tzNIC passed a special resolution to liquidate tzNIC and agreed to

22 Lane, J., Cooper, P., Hagopian, A., Sabford, S., & Katz, A. (2015). *HIV/AIDS and Health Information Privacy Laws in Tanzania*. University of Washington. http://www.globalhealth.washington.edu/sites/default/files/ALB_Background_Paper-Health_Information_Confidentiality_in_Tanzania.pdf

"execute the process of transferring the tzNIC functions to TCRA", however, TzNIC still operates but now under TCRA.[23]

## "WHOIS" practice

TzNIC has a dedicated webpage that allows the public to make enquiries on the WHOIS server information regarding a specific domain name. However, there is a set of guidelines that are termed as "WHOIS data and services terms of use" that stipulate principles of the servers' operation.[24] A query on the TzNIC WHOIS server provides details on the date of registration, expiry, etc., however; data provided depends on the information available to TzNIC.

Most of the enquiries return limited information on the owner of the domain but give data about the registrar of that domain who is usually a domain registrant company, some providing the website address, phone number, and/or physical address of the registrar and not the owner of the domain. The terms and conditions for querying the server also require that one "may use this Data only for lawful purposes and that under no circumstances will you use this Data to disseminate data and/or support the transmission of mass unsolicited, commercial advertising or solicitations via email, telephone, or facsimile."

## Analysis in line with the African Declaration on Internet Rights and Freedoms (AfDec) and other relevant instruments

AfDec's privacy and personal data protection principle addresses key areas and its applicability to ensure rights are secured, this includes:

23 https://www.tznic.or.tz/index.php/en

24 https://www.tznic.or.tz/Whois_tou.pdf

- Everyone has the right to communicate anonymously on the internet: The different pieces of legislation in Tanzania that address privacy and data protection do not cater for a user to communicate anonymously. Provisions under the EPOCA SIM card regulation require personal information and biometrics for registration and use of a SIM card, hence without one's details one cannot access services. With the introduction of NIN numbers as prerequisite to usage of services such as health insurance and application for a passport. Telecoms providers are now furnished with information of users, removing the right to anonymity whether on the internet or any other communication mechanism since the NIN numbers carry a wealth of information including biometrics and other personal data. Also, the EPOCA online regulations necessitate cybercafés to make use of surveillance cameras, which doesn't allow anonymity.
- The right to use appropriate technology to ensure secure, private and anonymous communication: The current laws do not directly prohibit use of tools such as circumvention tools. However, they do so indirectly for example the cybercrime act's section on illegal interception mentions "circumvent the protection measures implemented to prevent access to the content of non-public transmission." This section makes the circumvention punishable by law.
- The right to privacy on the internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this declaration) and are necessary and proportionate in pursuance of a legitimate aim. Under the EPOCA investigation regulations, rule 4 states that communications may be intercepted for the purpose of the:
  - Preservation or protection of national security: This is a one-size-fits-all term and is subject to various

interpretations, hence a weapon that can be used in cases where the government wants to undermine freedoms.

- Preservation of public safety, economic well-being or interest of the country: This also is open to different interpretations as will be fit at that time.
- Preservation, investigation, or proof of criminal offences: This, although a legitimate course, is still too narrowly explained and vague for interpretation.
- Prosecution of offenders or the execution of criminal sentences or security measures.

It further states that lawful interception shall be done by the director general of the Tanzania Intelligence and Security Service (TISS) or the director of criminal investigations, under a warrant duly applied for and granted by the issuing authority (Inspector General of Police). Failure to comply with a warrant is an offence punishable by imprisonment for a term of not less than 12 months, or a fine of not less than TZS 5 million (USD 2,156.233) or both fine and imprisonment.

In addition, any person may intercept communications if he or she is:

- Party to the communications
- Has the consent of the person who is sending, the person to whom it is sent or a party to the communication
- Is authorised by law; or is *bona fide* intercepting communications for the purpose of or in connection with the provision, installation, maintenance or repair of the communications service.[25]

25 Green, C., & Kumazora, F. (2019). Op. cit.

Despite there not being a data protection and privacy policy, the proposed legislation has taken into account regional guidelines including:

- East African Community (EAC) Cyberlaws Framework of 2008: Although not specifically focused on data protection and privacy it does mention and emphasise the need for one.
- Southern African Development Community (SADC) Model Law on Cyberlaws of 2010: As Tanzania also belongs to the SADC regional body as a member and for the year 2020 has been the chairman of the regional body, the new policy in development will borrow from the SADC model law as well.[26]
- African Union (AU) Convention on Cyber Security and Personal Data Protection of 2014: The convention seeks to establish a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, and promotion of cybersecurity governance and combating cybercrime. Tanzania has yet to ratify the AU convention but sources indicate that once draft policy is ready for public opinions ratification will be next.

## Data protection in UPR

The previous Universal Periodic Review (UPR) national report of 2016 highlights that Tanzania had made some progress towards ensuring the protection of data and privacy. Section C part 17 of the National Report on Tanzania states the enacting of the Cybercrime Act 2015 as a response to the need for the country to legislate policies that address data protection. Although the Cybercrime Act of 2015 was enacted to criminalise offences related to computer systems and information communication

26 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

technologies and for investigation, collection and use of electronic evidence and related matters, it also provides the right to privacy.[27]

The UPR mid-term report from CSOs regarding compliance of the country in addressing data protection related recommendations reported that:

> The Cyber-Crimes Act of 2015 and the EPOCA Online Content Regulations of 2018, intended at ensuring the exercise of fundamental freedoms related to access to information, freedom of expression as well as protecting Tanzanian citizens, ensuring  media professionalism and to keep abreast with developments in the electronic industry.

But the report also noted, “However, these legislations still have some provisions that limit rights of the people and need to be amended as they were enacted without enough consultations.”[28]

In the previous UPR cycle CSOs submitted privacy and data protection related recommendations that have yet to be accepted and worked on. In 2016 Privacy International in partnership with CIPESA and THRDC submitted recommendations on the “right to privacy in Tanzania”. Among the things they recommended that have yet to be carried out by the country are the following:

- They recommended adoption of a comprehensive data protection law that complies with international human rights standards and establishes an independent data protection authority. This is because Tanzania lacks a comprehensive data protection law with the status of the development of the

27 United Republic of Tanzania. (2016). National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21. https://www.upr-info.org/en/review/Tanzania-%28United-Republic-of%29/Session-25---May-2016/National-report#top

28 THRDC et al. (2019). Tanzania CSOs UPR Mid Term Report. https://www.upr-info.org/sites/default/files/document/tanzania_united_republic_of/session_25_-_may_2016/tanzania_csos_upr_mid_term_report_october_2019.pdf

draft data protection bill that has been unknown since first announced in 2014.

- Another recommendation was centred on ensuring that data processing of personal data is conducted in compliance with national and international standards and obligations i.e. the processing of sensitive personal information such as biometrics during SIM card registration.[29]

## Regional and international frameworks

### African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014

Tanzania has an obligation to ratify the convention to meet their obligations as a member of the African Union. The framework that has been laid down by this convention provides a way forward to harmonising policies across the continent and more importantly makes the process of domestication much easier since it has laid down all necessary provisions for a comprehensive data protection and privacy policy.[30]

### International Covenant on Civil and Political Rights (ICCPR)

Tanzania has also ratified the ICCPR, in which Article 17 reinforces Article 12 of the UDHR, providing that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence or to unlawful attacks on his honor and reputation.” However, without a comprehensive data protection legislation, this ratification remains on paper only

29 Privacy International, THRDC, & CIPESA. (2015). *The Right to Privacy in the United Republic of Tanzania*. https://cipesa.org/?wpfb_dl=212

30 https://www.au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

and will not progress to implementation. According the UPR submission report by Privacy International, CIPESA and THRDC they state that the "Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to 'adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]'."[31]

## Measures to update laws in line with the GDPR

According to sources from relevant authorities "during the preparation to seek approval to enact a data protection and privacy act (which is still ongoing) in the URT [United Republic of Tanzania], the GDPR has been acknowledged and the thinking in place is to ensure that the proposed legislation adopts or is in-line with the GDPR." The reason is to enable interoperability (transborder personal data flow) and to avoid unnecessary legislative contradictions. It is, however, important to note that in circumstances where the GDPR is contradictory to URT norms such regulations may have to be compromised in favour of the URT context.

## A human rights-based approach to personal data protection in Tanzania

While human rights are not a new concept, governments such as Tanzania are aware that the essence of any policy development should be human centred. A human-centred policy development policy process will take into account the need to ensure that the process bears in mind the PANEL principles of policy development. Bearing in mind that policy is for the people, of the people and by the people such as is democracy then the government ought to recognise that rights are at the centre.

31 https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Policy development process needs to ensure it addresses the needs of the "rights holders" as well as ensure that "duty bearers" are aware of what they need to do to serve the need of the policy which fairly in itself is all about the "people". In certain policy development processes within Tanzania, a human rights-based approach is utilised, but not to its full extent. Currently, looking at existing policies within the legal frameworks that govern how the online world is operating, obvious gaps can be noted. For example not all "rights holders" are aware of the provisions and laws that help protect them, highlighting a gap in ensuring all people are on a par with each other in understanding how the law works for them and their rights.

Complaints from stakeholders have risen over the years, especially from civil society, of little engagement or time allocated to them to comment and submit recommendations on proposed bills in parliament. Such was the case when amendments were made to EPOCA, a legislation which raised concerns over its practicability to hinder progression of key rights and freedoms online i.e. freedom of expression and assembly online.[32] Lately, with newer SIM card regulations as well as the online regulations released in July 2020,[33] it is obvious that the human rights-based approach is not fully used or adhered to hence leading to a wave of policy legislations across countries which are not based on human rights, Tanzania not being an exception.

As Tanzania currently works to develop the data protection and privacy policy, it is an appropriate time to ensure that a human rights-based approach is used in the process. This is to ensure that the policy that comes out will be beneficial and be human rights centred, bearing in mind both rights holders and duty bearers.

32 Paradigm Initiative. (2020). *Policy brief: Tanzania's EPOCA and Cybercrimes Laws Offer No Protection for Citizen's Data.* https://www.paradigmhq.org/fr/policy-brief-tanzanias-epoca-and-cybercrimes-laws-off

33 Data Guidance. (2020, 21 August). Tanzania: Government publishes EPOCA Online Content Regulations. https://www.dataguidance.com/news/tanzania-government-publishes-epoca-online-content-regulations

- Participation: While previous regulations and/or policies have had some sort of participation it is more important now that a data protection and privacy policy should engage people from grassroots level. The role of civil society is critical in ensuring that they should be aware of such a process and given adequate time to comment and collate opinions and needs from the people. The process should ensure that the draft bill is publicly available to everyone; it should be translated to Swahili to cater for language barriers as for the majority of Tanzanians it will be their first language. To achieve “active participation in decision-making processes” every voice should be heard and their needs addressed in said legislation.
- Accountability: Carrying forward examples from the frameworks developed by regional bodies such as the AU as well as from existing comprehensive data protection policies and/or regulations such as the GDPR, the policy should ensure its provisions cater for mechanisms to observe how data is processed, which data is processed and clearly explain why such data is collected. For the sake of accountability, an independent body such as the “data protection commission/agency” should be established with the mandate to hold different service providers and all who handle data accountable in accordance with procedures established by the policy. This includes having provisions within the policy that mention or address how data breaches will be reported and handled. To ascertain accountability the process of developing the data protection and privacy policy ought to have provisions that specifically highlight the rights and responsibilities of both duty bearers and rights holders.
- Non-discrimination and equality: The policy should address special concerns of different groups of people within the

community including special groups such as women, children and people with disabilities. This will ensure that there is equity in addressing the varying concerns of different groups within society. With the rise in uptake of technology there has been a rise in the infringement of rights of women online, for example an increase in gender based violence online, which has led to women censoring comments or withdrawing from using the internet. In 2018 an intimate video of Tanzanian celebrity Nandy and her boyfriend went viral. They stated that they had no idea of the source of the video.[34] In the recent past more women have had their intimate photographs leaked and have suffered emotional torture as a result of the massive reach of such videos and images. However, the law does not have provisions that specifically protect women who are often victims of such leaks, rather it adds to their distress by charging them with the creation of pornographic content. To ensure a data protection and privacy policy that protects the needs of special groups there ought to be enough participation of special groups in the policy development processes to ensure that their concerns and rights are captured in a comprehensive policy.

- Empowerment: Just as participation is important, empowerment is equally a much needed ingredient, one cannot do one without the other. Participation cannot come without empowerment and people cannot be empowered without being offered a chance for participation. Hence in developing a policy that people can actually claim, it is essential that they have a policy which empowers them to claim their rights, hold duty bearers accountable as well as have a mechanism that ensures they are the centre of the policy. To achieve this the empowerment process ought to begin from the very start,

34 Nyasio, V. (2018, 13 April). Female Tanzanian artiste arrested following leak of her video in bed with lover. *TUKO*. http://www.tuko.co.ke/271361-female-tanzanian-artiste-arrested-following-leak-video-bed-lover.html#271361

at the initial phases of policy development and progress throughout the different stages of the policy till it is passed as a law. If Tanzanians are empowered throughout the different stages of the policy development the policy shall then represent them in its entirety.

- Legality: Keeping in line with the constitution, the treaties and conventions to which Tanzania subscribes, in the process of developing a comprehensive data protection and privacy policy it is essential that the legality of it all is put into consideration and ensured. The provisions in said law and policy should be legally binding and linked to national and international human rights standards.

For all this to be practical it is important that no one element of the human rights-based approach is given preference over the other but rather each of the principles build on from each other. For the policy development process of the data protection and privacy policy to be human-rights focused and people centric it is essential that at this juncture the authorities responsible for drafting this policy ensure that they adhere to the PANEL principles of a human rights-based approach.

## Concluding observations and recommendations

The data protection and privacy scene of Tanzania is currently lacking the presence and application of a comprehensive data protection and privacy policy. Despite the presence of various legislations that address some privacy concerns here and there, as long as there is no one piece of legislation clearly dedicated to this, rights will not be fully assured. The government of Tanzania needs to see that this is a policy that is long overdue especially with the ongoing increase in internet users across the country. The presence of different

mechanisms and agencies that require collection of data from users puts rights holders at risk as long as there is no net to fall back on in case of a breach or infringement of rights, especially the “right to privacy”.

## Recommendations to strengthen the privacy and data protection framework in the country

Recommendations for the government:

- Enact a comprehensive data protection and privacy policy as soon as possible: The most important aspect to ensuring rights is to have a policy in place and the first step the government of Tanzania needs is to hasten the process and make the bill available for comments.
- Ratify the Malabo Convention on cybersecurity and data protection: In line with developing a policy, ratifying the convention is key to ensure regional harmony on data protection and privacy in Africa; this will hasten the domestication process.
- Explore financial support mechanisms and viable solutions: To bear the financial burdens of the bill it is essential for the government to either allocate a budget or identify a source of support for realisation of the policy.
- Adopt a multistakeholder approach to the development process: The government of Tanzania should keep all stages of the bill development open to the public and encourage multistakeholderism by ensuring civil society, private sector and users among others have a say in the bill’s content.

Recommendations for civil society and government:

- Review existing legislations that address privacy and data protection to ensure they are in harmony with the constitution, regional and international treaties, so as to avoid having different laws being contradictory with each other on key issues.
- Contribution, adherence and response to human rights mechanisms such as the UPR, both the government and civil society have roles to play here. Civil society ought to ensure that it keeps up to date with data protection and privacy concerns in Tanzania, builds coalition and submits to mechanisms such as the UPR while the government has a role to respond to and address raised issues.
- Advocacy at grassroots level to ensure that citizens are aware and educated on data protection and privacy as this will ensure a balanced relationship where all parties are aware of their rights and responsibilities.

Recommendations for the private sector:

- They have a role to establish privacy guidelines for the use of their services, they should clearly indicate to their consumers why data is collected, for what purpose and how it will be handled. Strict guidelines should apply to agents they work with and ensure an all-round insurance of rights.

Recommendations on the application of the human rights-based approach:

- The government should ensure participation of different stakeholders: At all stages of the policy development process through consultancy meetings the government should keep all relevant parties aware and engaged i.e. civil society, private sector and the public in general.

- Civil society and the government should identify and engage special groups: Individuals or groups that are more vulnerable to data protection and privacy breaches or have less access should be contacted to ensure participation, empowerment and non-discrimination.
- The government should initiate localisation efforts of the bill: The bill should be translated into Swahili and drafts at different stages made public to ensure anybody and everybody can access and read it in a language they are comfortable in.
- The government should ensure that the policy clearly identifies and specifies the roles of duty bearers and the rights of rights holders: This is to ensure that everyone knows what is expected of them and what they should expect from others.
- The government would ensure the framework of the bill gains its foundation from international and regional human rights laws: While Tanzania has promised that the said policy will borrow widely from regional and international frameworks, it should be noted that previous laws enacted did not fully address human rights concerns, i.e. the Cyber Crimes Act. Hence it is imperative that this time around the United Republic of Tanzania should fully embrace what it signs up for.
- Civil society and government should carry out extensive research to identify sources of evidence (qualitative and quantitative) that would help to inform the policy: This involves information and comments gained from the public masses on their data protection and privacy concerns.

Advocacy points for civil society and the private sector:

- Need for comprehensive supportive data/research on data protection and privacy needs: This will help drive a policy development process which is demand driven, catering for what the people truly need. Groups such as civil society and private sector can make use of such data to inform authorities on the needs collected from grassroots level. In line with above research the impact of data breaches on different sectors of the economy such as financial concerns, i.e. leaking of phone numbers of clients leading to spamming of consumers' phones. These concerns are often at the forefront of concerns of the private sector, to advocate their engagement in ensuring that their entities uphold data protection and privacy, impact surveys can go a long way to convince them. It is also important to *engage with relevant bodies that currently have mandates over specific data collection practices* including ministries that have rights under specific legislations to create regulations.
- Civil society should lobby responsible government authorities to uphold human rights based approach in policy development process. This includes holding the government to account when it does not develop people-centric and human rights-focused policies. Where possible CSOs should monitor how PANEL is being applied and advise the government accordingly.

# Togo

**Emmanuel Agbenonwossi**[1]
Executive director, Afrotribune

## Executive summary

This report provides a fairly precise overview of the Togolese legal and regulatory framework with regard to the protection of personal data. The report highlights not only the existing situation, but also an analysis of the correspondence between the available national legal framework and the provisions of regional and sub-regional conventions to which Togo is a party, in particular the African Union Convention on Cyber Security and the Protection of Personal Data (Malabo Convention) and the Economic Community of West African States (ECOWAS) Supplementary Act (A/SA.1/01/10) on Personal Data. The report also establishes the connection between the Togo Data

1 This work would not have been possible without the support of the Togolese Telecommunications Regulation Authority, the Office of the Ombudswoman of Togo, and the staff of the General Directorate of National Documentation. I am especially indebted to Mr. Seyram Adiakpo, a digital rights researcher who has been supportive in assisting with the legal understanding of the various laws and regional conventions and local context. I am grateful to all of those with whom I have had the pleasure to work during this project (publicly and anonymously).

Protection Act and the principles of the African Declaration on Internet Rights and Freedoms, and considers the framework for the development of laws related to digital rights, taking into account the challenges of the human rights-based approach.

The purpose of the work is to provide a scientific perspective on the framework for the protection of personal data in Togo and to make recommendations. These recommendations are addressed to all stakeholders in the internet governance ecosystem, from the point of view of multistakeholder governance. These recommendations are not only to improve the institutional framework for the collection of personal data, but also aim to bring all the stakeholders involved to greater transparency in the collection and management of data.

## Introduction

Togo is a sub-Saharan West African country that shares borders with Ghana to the west, Burkina Faso to the north, and Benin to the east. It had an estimated population of 8.2 million inhabitants as of 2020, with a demographic growth rate of about 2.5%. Lomé, the capital, has the only deep-water port in West Africa, making the city an important transport hub for transit trade to landlocked neighbouring countries. The main economic activities are agriculture, phosphate mining, trade and transportation of goods. Agriculture employs about 66% of the population and accounts for about 41.3% GDP.[2] Over 50% of the population live below the poverty line (under USD 1.25 per day). Poverty is strongly linked to under-nutrition, food insecurity at household level is prevalent across the country and is particularly high in the northern regions.[3]

2 https://data.worldbank.org/country/Togo

3 https://www.wfp.org/operations/tg01-togo-transitional-icsp-january-2018-june-2019

Togo's human capital index remains low at 0.41. This means that a child born today in Togo will reach only 41% of his potential as an adult in terms of health, education and nutrition.[4]

The COVID-19 pandemic could further limit the economic momentum of recent years. Despite an unfavourable international situation, marked by a crystallisation of trade tensions and the persistence of the security threat, the Togolese economy maintained its good performance in 2019 with growth estimated at 5.3% by the International Monetary Fund.

Togo's constitution calls for a bicameral legislature, but the senate has never been established. Members of the current 91-seat National Assembly, which exercises all legislative powers, were elected for five-year terms in December 2018. The main opposition parties led a 14-party boycott, citing a number of unmet demands regarding constitutional and electoral reform. The ruling party Union for the Republic (UNIR) won 59 of the 91 seats, down from 62 in 2013.[5]

Faure Essozimna Gnassingbé, the incumbent 54-year-old leader, took office in 2005 after the death of his father Eyadema Gnassingbe, who led the country for 38 years after seizing power in a coup in 1967.

A series of major protests swept the country in 2017 and 2018 demanding that Gnassingbe leave power. However, demonstrations were choked by a fierce government crackdown, internet shutdowns and splits within the opposition.

4 https://data.worldbank.org/indicator/HD.HCI.OVRL.FE?locations=TG

5 U.S. Department of State. (2019). *2019 Country Reports on Human Rights Practices: Togo*. https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/togo

The president pushed through constitutional changes in May 2019 allowing him to stand again in 2020 and potentially stay in office until 2030.

In Togo, digital rights and internet freedom are still new concepts. There is a huge knowledge gap for the citizens regarding their rights, even though policy makers have shown interest in the digital rights issues in recent years.

This interest is not necessarily to protect the citizens but rather out of concern to adapt state policies to the global digital situation. The recent bills voted by the parliament take cognisance of existing international conventions and treaties and foreign laws, but do not necessarily take local realities into account.

## Internet shutdowns, surveillance of dissidents and the rise of digital rights activism

Citizen interest in digital rights comes after the government has been active in recent years in developing and refining a whole arsenal to surveil, manipulate and censor the digital flow of information. The most remarkable ones are the internet shutdowns during anti-government protests in 2017 and the 2020 presidential election.[6] These network restrictions were closely linked to political events.

More recently, religious and political opposition leaders[7] in Togo were targeted with spyware developed by Israeli software surveillance firm NSO Group, according to security researchers

6 Tadégnon, N. (2020, 25 June). L'Etat togolais condamné pour coupure d'internet. *DW*. https://www.dw.com/fr/letat-togolais-condamn%C3%A9-pour-coupure-dinternet/a-53943806

7 Tilouine, J. (2020, 3 August). Comment le Togo a utilisé le logiciel israélien Pegasus pour espionner des religieux catholiques et des opposants. *Le Monde*. https://www.lemonde.fr/afrique/article/2020/08/03/au-togo-un-espion-dans-les-smartphones_6048023_3212.html

at the University of Toronto Munk School's Citizen Lab. It was not clear who was responsible for using the surveillance software, but Citizen Lab previously reported in 2018 that the operator was a government agency.[8]

There are factors that do not favour the establishment of an effective data policy in Togo. These are the frequent changes of government and the internal socio-political context of the country, marked by the sovereignty of the state.

According to a report published in 2012 by the International Institute for Sustainable Development, 10 attempts had been made to produce a national ICT policy document without yielding much in the way of tangible outcomes.[9] Between 2005 and 2010, Togo had a total of four cabinet reshuffles. But this did not result in new policy dialogue or major reform in policy.

The recent violations and the activities of local activists have sparked the debate around digital rights in the country.

Although the country has a Mediator of the Republic who is the equivalent of the ombudsman and a National Commission of Human Rights, these two organisations have never been petitioned by citizens despite the violations arising. Contacted in line with this research, the Office of the Ombudswoman as well as the National Commission of Human Rights declared that they had not yet received any complaint relating to data protection and privacy. The Electronic Communications and Post Regulatory Authority (ARCEP) remains the only regulator in the sector but its

8 Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A., & Deibert, R. (2018). *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. The Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

9 Akoh, B. (2012). *Supporting Multistakeholder Internet Public Policy Dialogue in a Least Developed Country: The Togo Experience*. International Institute for Sustainable Development. https://www.iisd.org/system/files/publications/internet_policy_dialogue_togo.pdf

prerogatives remain fairly general. Although a decree issued by the Council of Ministers in 2019 announced the creation of a data protection agency, this is not effective yet.

The only case that has been brought to court is a lawsuit filed by Amnesty International Togo and other applicants at the ECOWAS Court of Justice. The court ruled that the September 2017 internet shutdown ordered by the Togolese government during protests is illegal and an affront to the applicants' right to freedom of expression.

The court ordered the government of Togo to pay two million CFA francs (USD 3,600) to the plaintiffs as compensation, and to take all the necessary measures to guarantee the implementation of safeguards with respect to the right to freedom of expression.[10] It is the only judgment that has for the first time stated clearly that digital rights are human rights.

## Constitutional underpinning

The Togolese Constitution of 14 October 1992 lays the foundations for data protection and privacy and guarantees the "respect for the private life, honour, dignity and image" of every citizen. Apart from that, Article 29 of the constitution states that "the State guarantees the secrecy of correspondence and telecommunications. Every citizen has the right to the secrecy of his correspondence and of his communications and telecommunications."

Drafted in 1992, this constitution came at a time when human rights activists began to assert themselves and when the

10 Paradigm Initiative. (2020, 25 June). Paradigm Initiative praises historic ECOWAS Court decision on internet shutdown in Togo. https://www.paradigmhq.org/paradigm-initiative-praises-historic-ecowas-court-decision-on-internet-shutdown-in-togo

democratic conditionality of development aid was still a reality to which French-speaking African states were trying to adapt. It should be noted that even if these provisions of the fundamental law remain a general declaration of faith, in the principle of confidentiality, they are explicit enough to be interpreted in the sense of benefit to the citizen or victim of violation of online privacy. However, the notion of confidentiality formulated as it is in the constitution, doesn't take into account online privacy and confidentiality.

On 17 November 1997, Togo connected to the internet for the first time. It thus became the first French-speaking country in West Africa to connect to cyberspace.[11] However, subsequent constitutional amendments did not make mention of provisions regarding online data protection, confidentiality and privacy.

This usually leads the courts to interpret these provisions in the primary sense. This interpretation *stricto sensu* remains very attached to the generalities of the inviolability of private correspondence. "The secret of communications and telecommunications" in the strict sense concerns telephone and radio communications.

## The decade of online laws and frameworks

Over time, a legal apparatus has been built on the issue of digital technology and specifically personal data. These laws are of two generations. There are, first of all, the laws which regulate the information society and the electronic communications sector in general, but more recently other laws have been adopted to deal with the online rights specifically.

11 Abalo, J. C. (2007, 20 November). Dix ans d'internet au Togo: l'âge de la coopération. *Afrik.com*. https://www.afrik.com/dix-ans-d-internet-au-togo-l-age-de-la-cooperation

Among the classic laws was the Telecommunication Act No. 98-005 of 11 February 1998[12] (repealed), which reiterated the secrecy of correspondence and the principle of the secrecy of communication and telecommunications set out in the constitution.

On the question of the protection of personal data, recent digital laws are becoming more precise as they are enacted. In order of appearance, the Electronic Communications Act No. 2012-018 (amended by Law No. 2013-003)[13] and the Electronic Transactions Act No. 2017-007[14] adopted in 2017.

These two laws laid the foundations for the electronic communication sector and electronic transactions. The Electronic Transactions Act No. 2017-007 was the first law in Togo's history which refers to the concept of "personal data". According to the law, personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to a person's physical, physiological, mental, economic, cultural or social identity (e.g. first and last name, date of birth, biometrics data, fingerprints, DNA, etc.). Subsequent laws voted by the parliament years later kept the same definition.

## To join or not to join the regional and international commitments?

In spite of the great legislative and institutional framework development in recent years in Togo, there remain obstacles to dealing effectively with cybercrime linked in particular to the

12 https://www.droit-afrique.com/upload/doc/togo/Togo-Loi-1998-05-telecommunications-MAJ-2004.pdf

13 https://numerique.gouv.tg/wp-content/uploads/files/2017/03%20-%20Mars/Loi_n_2013-003_portant_modification_de_la_loi_n_2012-018_du_17_decembre_2012_sur_les_communications_electroniques.pdf

14 https://jo.gouv.tg/sites/default/files/JO/JOS_07_07_2017-62E%20ANNEE%20N%C2%B021%20QUARTO.pdf

global nature of the phenomenon, which ignores state borders. This is a source of legal difficulty in conducting investigations and protecting citizens.

## Budapest Convention

It should be noted that in terms of commitment to confidentiality and data protection, Togo is not a member of the Council of Europe Convention for the protection of people with regard to the automated processing of personal data, nor the Budapest Convention on Cybercrime,[15] even though all its neighbouring countries such as Benin, Burkina Faso and Ghana have ratified the Budapest Convention.

Solutions to enable criminal justice access to evidence in the cloud are a priority of this convention. While Togo is confronted with the very same challenges, it is not participating in this work, thus; the country is not sharing its experience and not shaping future international solutions as it has not yet decided to join this treaty.

## Malabo Convention

Togo signed the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention,[16] on 2 April 2019.[17] In 2019, the National Assembly adopted the law authorising the ratification of the Malabo Convention.[18] Despite the fact that the law authorising the ratification of the convention

15 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

16 https://www.au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

17 https://www.au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

18 Tobias, S. (2019, 10 October). Cybersécurité : le Togo va ratifier la convention de Malabo. *CIO mag.* https://cio-mag.com/cybersecurite-le-togo-va-ratifier-la-convention-de-malabo

was adopted by parliamentarians,[19] the government did not ratify the convention.

At the sub-regional level, in the ECOWAS legal ecosystem, there is the additional Act A/SA.1/01/10 on protection of personal data in the ECOWAS region, to which Togo is a party. The Togo Data Protection Act is completely compatible with previous regional legal texts, which gives it the merit of being a “good” law only if the principles set out therein are observed and monitored by public authorities.

## Togo’s Data Protection Act, the almost copy-paste

The law dedicated to the protection of personal data in Togo is the Data Protection Act (DPA) No. 2019-014 of 29 October 2019, relating to the protection of personal data.[20] It regulates the collection, processing, transmission, storage and use of personal data. It applies to individuals, the state, local communities, private and public companies, as well as to automated or non-automated processing of data carried out within the territory of Togo or in any jurisdiction where the Togolese laws apply.

One of the aims of the data protection law is to empower individuals and give them control over their personal data. It has a chapter on the rights of data subjects (individuals) which includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing.

19 http://www.jo.gouv.tg/sites/default/files/JO/JOS_17_08_2018-63E%20ANNEE%20N%C2%B0%2015.pdf#page=12

20 http://www.numerique.gouv.tg/wp-content/uploads/2020/01/Loi-n-2019-014-du-29-octobre-2019-relative-a-la-protection-des-donnees-a-caractere-personnel-in-JO29102019.pdf

The DPA established seven core principles for the handling of personal data. These principles include: principle of consent and legitimacy, principle of lawfulness and loyalty, principle of finality, relevance and conservation, principle of accuracy, principle of transparency, principle of confidentiality and security and the principle of the choice of the subcontractor.

These principles required personal data to be:

- Processed fairly and lawfully
- Processed only for specified, lawful, and compatible purposes
- Adequate, relevant and not excessive for the intended purposes
- Accurate and up to date – individuals have the right to have inaccurate personal data corrected or destroyed
- Processed in line with the rights of the individuals
- Secured against accidental loss, destruction, or damage against unauthorised or unlawful processing
- Not transferred outside Togo unless there is adequate protection.

It should be noted that this law does not directly refer to the right to anonymity online. The concern was raised by civil society organisations (CSOs) after the law was voted but did not get much support to influence its amendment.

Note that the protection of anonymity is a vital component in protecting both the right to freedom of expression and the right to privacy. This could allow citizens to express themselves without fear of reprisal in Togo, where freedom of expression has been heavily censored for the last 50 years.

The direct consequence of this missing point is that whistleblowers and citizens are not able to come forward to disclose their innermost concerns on a variety of issues in internet chat rooms and other online platforms.

## The secrecy of the process

The DPA is welcome in a context where the framework and responsibilities for the protection of personal data were still uncertain. It is the first law that intervenes in the field. Proposed by the Ministry of Posts, Digital Economy and Technological Innovations, the bill was debated in the national assembly; however, it did not follow a multistakeholder process and an open debate.

Since it has a strong criminal aspect, this law can easily be implemented in the context of legal disputes, however, it has not yet been invoked in a court or tribunal since the president assented to it.

Within the framework of this law, it provides for the creation of a regulatory agency for the protection of personal data, the *Instance de protection des données à caractère personnel* (IPDCP).

According to the law, IPDCP will be an independent administrative authority responsible for ensuring that the processing of personal data is carried out in accordance with the provisions set out in law. It informs data subjects and data controllers of their rights and obligations. In this regard, it receives the formalities prior to the implementation of personal data processing, receives complaints, petitions and complaints relating to the implementation of personal data processing and informs their authors of the follow-up. IPDCP will work closely with the Office of the Public Prosecutor to carry out checks on any processing

and, where applicable, to obtain copies of any document or information useful for its mission.

IPDCP also has the right to impose sanctions on a data controller and then formulate opinions. Apart from this mission, the law allows it to authorise cross-border transfers of personal data, to cooperate with the personal data protection authorities of third countries and to participate in international negotiations on data protection at personal character. Finally, it publishes the authorisations granted and the opinions issued in the directory of processing of personal data.

The main challenge in the implementation of this law remains the important prerogatives which the state has always had in terms of data governance and in particular relating to its monitoring work. The DPA does not provide an overview of the limits of the state itself in handling the personal data of citizens. While this law has the merit of setting the framework for the protection of personal data, this fundamental element is still poorly defined.

Within the meaning of the law, the state appears as an authority which controls and sanctions. On the other hand, the data processing carried out on its behalf is only subject to a declaration regime with the Personal Data Protection Authority. The prerogatives of the state must respect the principle of the rule of law.

The other challenge remains that of informing the public about the legislation on personal data. People are still poorly informed about the existence of the law, apart from the community of people who are already accustomed to data manipulation and internet governance issues. The lack of public awareness of the common citizen about the existence of the DPA is in contradiction

with the principles contained in the law, if the citizens are to take advantage of it.

## Data neo-colonialism

In Togo, the key personal data protection issues relate to the sovereignty of the state as a public authority, in the exercise of its related prerogatives.

As a matter of fact, there is already a framework for collecting biometric data and its use at various levels. Biometric data is collected for passports, national IDs and voter ID by the National Identification Authority. However, it should be noted that the collection of personal data for national identity cards is not done equally in all police stations in Togo.

In the capital city Lomé, the biometric data collected are the fingerprints of 10 fingers while in other regions of the country the data collected are only those of the index fingers. A passport office technician who spoke to us in the course of this research on condition of anonymity, because he was not authorised to speak publicly, explained that the particular data collection has been in place for years due to the lack of infrastructure in police stations in the country. This implies that citizens' data is not collected equally for the same purposes. However, it was explained to us that an infrastructure deployment is currently underway to correct the inequality. It is important to point out that Togo has only one passport office based in Lomé at the General Directorate of National Documentation. Police stations only issue identity cards across the country.

On the other hand, the state leaves the management of all biometric data collection and management to foreign companies

without clearly informing the public about how the collected data is being managed and how safe they are. However, according to Gerry Taama, an opposition member of parliament who is also a member of the Committee on Constitutional, Legal and Parliamentary Affairs, the contracts with these foreign companies are software-as-a-service (SaaS) agreements. In his words, the data is secure in Togo and is not routed to the servers of the countries of origin of these companies.

In 2015, the Togolese government renewed its agreement with ZETES, a company incorporated under Belgian law, based in Brussels, for the fourth time.[21] The company had first administered the country's voter registration programme in 2007, using both fingerprint and facial biometrics. Today, ZETES has the biometric data of over three million Togolese citizens.

For the National ID Programme, Canadian Bank Note, an Ottawa-based company, is in charge of the issuance of the Togo ID card, a card that is used as proof of ID and enables people to apply for all government and financial services including obtaining a passport or driver's licence, writing national educational examinations and obtaining a bank loan, among others.

According to publicly available information, Togo contracted the company to build:

- A central registry that holds the data of all citizens
- A system that is deployed and operated at 39 locations across the country
- A biometric system to ensure that each individual is enrolled only once

21 https://peopleid.zetes.com/en/reference/biometric-voter-registration-togo

- An interface with other databases to authenticate individual identities
- Online and “store and forward” capabilities to allow for efficient operations in locations where infrastructure is a challenge.

The company is also behind the new professional and police ID cards and is leveraging the system to support identification for elections.

According to the information gathered from sources in the course of this research, the data is secured by the state and is not collected by the company, due to the contractual framework that links it with the Togolese state. No public information is available about the terms contained in the contract and one could not verify the level of implication of the company in the management of this data.

A passport office technician who spoke to us on condition of anonymity said, “Despite the fact that the data is collected on several different occasions, Togo is one of few countries in Africa which has a centralised database for personal data, due to the fact that the same system is used at all levels.” The risk being that, in the case of data breaches, all Togolese will be affected.

The legal framework for biometric identification data was set by the recent law on the identification of individuals in Togo (e-ID Act), voted in on 3 September 2020, by the parliament.

The new law, according to the government, will guide and regulate the collection of citizens’ data by the government. The e-ID Act is therefore the second law governing personal data.

Financed by the World Bank, the “e-ID Togo” project is part of the West Africa Unique Identification for Regional Integration and Inclusion Programme, a project which aims at building the foundational identification systems that are inclusive of all persons in the ECOWAS territory, irrespective of nationality, citizenship or legal status. The programme involves Côte d’Ivoire, Guinea, Benin, Burkina Faso, Niger and Togo.

## Key features of the comprehensive data protection law

The Togo DPA comes at a time when internet governance forums and a new generation of CSOs have started raising the question of the protection of personal data. To understand the law, taking into account the Togolese context, it is important to define certain keywords within the meaning of the law.

Within the meaning of the DPA, “personal data is any information relating to an individual identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, mental, cultural, social or economic identity”, the data subject is “any individual who is the subject of personal data processing” and the third party is:

> [A]ny individual, public or private entity, any other body or association other than the data subject, the controller, the processor and the persons who, placed under the direct authority of the controller or the processor, are authorized to process the data.

As for the data controller, it is defined as:

> [A]ny individual or legal person, public or private, any other body or association which, alone or jointly with others, takes the decision to collect and process personal data and in determining the purposes.

The processing of personal data means:

> [A]ny operation or set of operations [...] whether or not carried out using automated or non-automated processes, and applied to data, such as collection, use, recording, organization, conservation, adaptation, modification, extraction, saving, copying, consultation, use, communication by transmission, distribution or any other form of making available, reconciliation or interconnection, as well as the locking, encryption, erasure or destruction of personal data.

Finally, the body for the protection of personal data is defined as:

> [T]he body competent to formulate all useful recommendations with a view to ensuring that the processing of personal data is carried out in accordance with the provisions of the law relating to the protection of personal data.

The “data subject” is the object of rights contained in the law and their implementation is facilitated by the obligations to which the person in charge of the processing of personal data must submit. The rights of the data subject are the right of information, the right of access, the right of opposition, the right of rectification and deletion, the right to erasure and the right to update the data of a person after his/her death.

However, the existence of the principle of consent in the processing of data should be specified.

Clearly, the data processing is only legally founded if the data subject gives their consent. However, this requirement can be waived when the processing is necessary for:

- Compliance with a legal obligation to which the controller is subject.
- The performance of a task carried out in the public interest or in the exercise of public authority, devolved to the controller or to the third party to whom the data is disclosed.
- The performance of a contract to which the data subject is a party or the performance of pre-contractual measures taken at his request.
- To safeguard the interest or fundamental rights and freedoms of the data subject.

## The right to information

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data and the following information:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

- The right to lodge a complaint with a supervisory authority.
- Where the personal data is not collected from the data subject, any available information as to its source.

## The right of access

Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. This means that every individual is entitled to have their personal information protected, used in a fair and legal way, and made available to them when they ask for a copy. If an individual feels that their personal information is incorrect, they are entitled to ask for that information to be corrected. Anyone who, in exercising their right of access, has serious reasons to admit that the data communicated to them does not comply with the data processed, can inform the authority, which then carries out the necessary checks.

## The right of opposition

Any natural person has the right to oppose, for legitimate reasons, the processing of personal data concerning him. All natural persons have the right, on the one hand, to be informed before the data concerning them are first communicated to third parties or used on behalf of third parties for marketing purposes and, on the other hand, to be expressly offered the right of opposition, free of charge, to such communication or use.

Any natural person proving his identity may ask the controller to rectify, complete, update, block or delete, as the case may be, the personal data concerning him which is inaccurate, incomplete, ambiguous, out of date or whose collection, use, disclosure or storage is prohibited.

When the applicant makes a written request, in any medium whatsoever, the controller must justify, at no cost to the applicant, that he has carried out the required operations within one month of the registration of the request.

## The rights of rectification, deletion and erasure

Once the controller has made the personal data of the data subject public, he must take all reasonable measures, including technical measures, concerning the data published under its responsibility to inform third parties processing data that a data subject asks them to remove all links to copies or reproductions of such personal data.

If the controller has authorised a third party to publish the personal data of the data subject, he must be considered responsible for this publication and must take all appropriate measures to implement the right to be forgotten and delete the personal data.

In the event of failure to delete personal data or in the absence of a response from the controller, within a period of one month from the request, the data subject may refer to the authority (which must decide on the request within three weeks of the date of the complaint).

## The right to update personal data after death

Among other things, the law provides that the successors of a deceased person who can prove their identity can ask the controller to take into account the death of the person concerned in order to make the necessary updates.

In general, it is the responsibility of the controller to bear the burden of proof of the transactions carried out at the request of the data subjects.

## Cross-border data transfer

With regard to the transfer of cross-border data (or to a third country), the controller can only transfer personal data to a third country if that state ensures a sufficient level of privacy protection privacy, fundamental rights and freedoms of individuals with regard to the processing of which the data are or may be subject. This operation is subject to the principle of reciprocity. In addition, the other conditionality is that the data controller informs the Personal Data Protection Authority in advance, which gives a reasoned opinion.

There is a derogation from the requirements listed above. Indeed, the transfer of data to a third country which does not respect the conditions is possible if the transfer is occasional, not massive and if the person to whom the data relates has expressly consented to their transfer or if the transfer is strictly necessary under specific conditions (the safeguard of the life of this person, the safeguard of the public interest, the respect of obligations making it possible to ensure the establishment, the exercise or the defence of a right in justice and the execution of a contract between the controller and the data subject, or pre-contractual measures taken at the latter's request).

## Data protection authority: Wielders of superpowers

As indicated in the previous paragraphs, the DPA has set up an authority according to the recommendations of additional Act A/SA.1/01/10 relating to the protection of personal data and the Malabo Convention.

In accordance with the requirements of the two texts, the planned authority has specific characteristics, in particular as regards its legal form, its powers, its limits and the precautions with regard to its composition.

The national authority responsible for the protection of personal data is referred to as the “Personal Data Protection Authority (IPDCP)”. Its mandate is to ensure that the processing of personal data is carried out in accordance with the provisions of the law. It informs data subjects and data controllers of their rights and obligations and ensures that ICTs do not pose a threat to public freedoms and privacy. Its missions are defined in accordance with the mandate.

Thus, the authority is responsible for ensuring that the processing of personal data complies with the provisions of the law, informing the persons concerned and the data controllers of their rights and obligations, and approving the charters of use that are presented to it; keeping a directory of personal data processing bodies available to the public; advising people and organisations who have recourse to the processing of personal data or who carry out tests or experiments that lead to such processing, authorised under the conditions provided for by this law; cross-border transfers of personal data; presenting to the government any suggestion likely to simplify and improve the legislative and regulatory framework with regard to the processing data; cooperating with the personal data protection authorities of third countries and participating in international negotiations on the protection of personal data; publishing the authorisations granted and the opinions issued in the directory of personal data processing; and drawing up an annual report of activities addressed to the president of the republic, the prime minister, the president of the National Assembly and the president of the Senate.

The authority has very significant means of action with regard to data controllers, in particular the ability to search (under the conditions provided for by law and in compliance with procedures), the power of control, the power of injunctions, the power to sanction, but also the ability to take emergency or protective measures, when the implementation of processing or the use of personal data results in a violation of rights and freedoms.

In accordance with requirements of the two aforementioned international texts, the institution is an independent administrative authority composed of 10 members, none of whom must come from the government, nor from the governing bodies of companies in the IT or electronic communications sector.

While the institutional framework provided by the DPA regarding the creation of the independent authority exists, cabinet has not yet approved the creation of the authority.

## A virgin territory for digital rights activism

In the local Togolese context, the Internet Governance Forums organised every year since 2012 have been a forum for discussion on digital rights. In one way or another, the issue of personal data protection is discussed every year. The recommendations of this forum are sent to the stakeholders intervening on the issue of internet governance.

Currently, only one organisation has been identified as a local organisation working to foster digital rights in Togo. The organisation, Afrotribune, has drafted the country's Digital Rights and Freedoms Bill. This bill, if it is adopted, should give fairly important guarantees to citizens vis-à-vis the persons responsible for processing personal data, but will also affirm the responsibility of the state in matters of protection and control.

Other international organisations such as Paradigm Initiative, the #KeepItOn Coalition and Amnesty International are monitoring digital rights violations in the country. These organisations produce reports that point out violations, but also react directly to urgent situations such as network disruptions, so that they can be restored.

The reality of the collection of personal data can be observed in practice by the most common citizen in the context of the registration of SIM cards, the acquisition of identity cards, but more especially the acquisition of passports and voter cards.

## Data protection practices in internet country code top-level domain (ccTLD) registration

Like any country, Togo has a country code top-level domain (ccTLD) known under the code tg. The legal framework of this code is Decree No. 2016-103/PR, relating to the administrative, technical and commercial management methods of the national ".tg" internet domain name. Within the meaning of the decree signed by the president of the Togolese Republic, the .tg code is managed by the regulatory authority for posts and telecommunications.[22] Previously, the technical management of the domain name was provided by Café Informatique et Telecommunications, a private telecommunications company.

The "WHOIS" of domain names with the .tg code is available publicly and easily accessible to all. This page[23] refers to data after searching for the specific address ending in .tg. This query

22 Ministere de l'economie numerique et de la transformation digitale. (2016, 1 June). Nouvelle approche de gestion du domaine internet national <<.tg>>. https://numerique.gouv.tg/nouvelle-approche-de-gestion-du-domaine-internet-national-tg

23 http://www.nic.tg

returns data such as the first and last name, the subscriber's telephone number, the subscription date and the expiration date. The owners have the possibility to hide their private data.

## Togo Data Protection Act through the lens of the African Declaration on Internet Rights and Freedoms

Principle 8 of the African Declaration on Internet Rights and Freedoms states:

> Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law and are necessary and proportionate in pursuance of a legitimate aim.

In view of this statement, it is clear that the principle of respect for online privacy is echoed by the legal instruments available in Togo. However, the right to "use appropriate technology to ensure secure, private and anonymous communication" remains confronted with state concerns for security and sovereignty. Indeed, if citizens can enjoy the various encryption systems as part of their private online exchanges, it seems that the Togolese state remains very attached to surveillance, to the point of deploying infrastructure in order to pierce private conversations. While this system seems to be common to many countries, the actors targeted are generally people involved in politics and political activism. It appears that, in this sense, state resources intended to ensure the security or the external defence of

the state should not be used to slow down the expression of democracy. The ambiguity should be resolved in order to ensure that all internet users are able to appreciate the gap between the legal framework established and the reality of practice. This being the case, it is clear that the legal framework established is in line with the requirements of Article 8 of the declaration and the international conventions (regional and sub-regional) to which Togo is a party.

When it comes to the protection of human rights, digital rights are gradually being included in legislation. However, Togo is not yet part of any mechanism to monitor the implementation of digital rights protection. General human rights are subject to a Universal Periodic Review (UPR) in which Togo participates. As part of this periodic review, civil society is required to produce a report. However, digital rights issues in Togo have not yet been fully discussed during the UPR. The previous issues Togo was confronted with during a UPR review are human rights and the abolition of torture.

On the question of the implementation of the European Union General Data Protection Regulation (GDPR) in Togo, it should be noted that the laws on the protection of personal data were adopted after the GDPR. The influence of the GDPR is considerable in the legal corpus with regard to personal data, it is common ground that Togolese regulations have adopted the general principles contained in the GDPR (in particular, the right to information and to access, the right to rectification and erasure, the right to object, etc.). The legislation clarifies the responsibilities of the state vis-à-vis the controller.

## A human rights-based approach to personal data protection in Togo

Due to the strong links between digital rights and general human rights, it is important that personal data protection laws and policies take into account the human rights-based approach.

This approach strengthens the capacities of duty bearers to assume their responsibilities and encourages rights holders to uphold them. States have a threefold responsibility: they are required to respect, protect and assert fundamental rights. This notion has strong links with the notion of the rule of law and good governance. A human rights-based approach identifies the rights holders, the rights in question and the corresponding duty bearers. It works to build the capacity of rights holders to assert their claims and to ensure that duty bearers fulfil their duties.

As far as digital rights are concerned in Togo, the human rights-based approach mainly concerns the legal framework put in place by the state, but also its attitude towards citizens. The human rights-based approach includes the following principles: participation, accountability, non-discrimination and equality, empowerment and legality.

Regarding participation, the general rule implies that everyone has the right to participate actively in the decision-making processes that affect the enjoyment of their rights. Participation therefore implies that the laws and policies adopted by public authorities really take into account the wishes of citizens.

In the Togolese context, citizen participation in the drafting of laws follows *a priori* — a reputed model based on democratic principles. The mandate of the people is entrusted to the

legislative power which has the role of making the laws. However, the legislature does not have a monopoly on initiating laws.

The government can propose laws, after having identified the need for a law to be made in a particular area. This is the case, for example, of the e-ID Togo law, still pending approval by the head of state.

Government bills are submitted to parliament after having passed the Council of Ministers. The parliamentary committee concerned by the law does a work of study and critical appraisal of the proposed law. During this work, the ministry carrying the bill remains available to answer questions from the commissioners. It is common ground that citizens do not participate directly, but their right to participate is delegated to the appropriate bodies.

However, awareness around legislative work is not actually a reality. Its implementation could allow citizens to learn about the adoption of laws that affect their future and thus, by organising themselves, to propose issues that take into account their realities.

The other approach is accountability. It is understood to mean the responsibility for the holders of obligations vis-à-vis the non-respect of their obligations towards the holders of rights. This means the establishment of the appropriate rights of recourse, even towards the public authority which is guilty of failings or breaches of its obligations. In Togo, there are several remedies, both jurisdictional and non-jurisdictional.

Regarding legal remedies against the public administration and its branches, there is a possibility to petition the Administrative Chamber of the Supreme Court. However, there are other possibilities, in particular, a petition to the regulator (ARCEP).

Regarding protection of human rights, the Office of the Mediator of the Republic (French-speaking equivalent of the ombudsman), and the National Commission for Human Rights are in charge. With the emergence of digital rights, the institutions promised by recent laws (relating to personal data and e-ID), two additional institutions will strengthen the mechanism of state accountability. These include the Personal Data Protection Institution and the National Identification Agency. These are not conflict management mechanisms, but reflect the responsibility of the state to put in place a substantial institutional framework with regard to the protection of personal data.

The non-discrimination and equality approach are a dimension which implies that all individuals have the right to their rights without discrimination of any kind and that all types of discrimination must be prohibited, avoided and eliminated. In this area, reading the various legal texts suggests that the laws will be addressed to all citizens without any discrimination. On the other hand, no event has occurred to prove that in reality, the rights of citizens are guaranteed to them only on a case-by-case basis, taking into account their situation or social condition or their origin. Furthermore, within the meaning of the e-ID law, the definition of demographic data excludes data such as race, religion, ethnicity, income or medical history.

Within the meaning of the DPA, factors which are likely to make a value judgment on the person, are called “sensitive data”. This is the personal data relating to racial or ethnic origin, religious, philosophical, political, trade union opinions or activities, sexual life, health, social measures, legal proceedings, criminal or administrative penalties.

The collection and processing of this data is, moreover, prohibited within the meaning of the law on the protection of personal data. The law clearly states: “It is forbidden to carry out the collection and any processing which reveals racial, ethnic origin, filiation, political opinions, religious or philosophical convictions, trade union membership, sexual orientation, genetic data or more generally those relating to the state of health of the person concerned.” Such an operation is deemed to be “illegal” and governed by a very strict regime, insofar as it should occur. Even a supervision regime deemed to be strict in its application, remains permissive vis-à-vis a practice that should simply be banned from data culture in Togo.

It is regrettable that the law relating to the biometric identification of natural persons in Togo allows the collection of “optional” data under which “spoken languages” can be counted[24] in demographic data. Such practices, although they are “optional” and non-compulsory, have ethnic overtones and should be banned from a law whose implementation will be financed by human rights-complying organisations such as the UN, the World Bank, etc.

On the empowerment aspect which implies that everyone has the right to claim and exercise their rights, and that individuals and communities must understand their rights and participate in the development of policies that affect their lives, it is observable that in general, much remains to be done.

Latin-German legal culture demands that no one should ignore the law. It is right that a good knowledge of the law and the context of its development will allow citizens to react and participate in the development of policies. The demand for rights is generally made in a jurisdictional way, or through demonstrations.

24 Art. 6 of the Law on the Biometric Identification of Natural Persons.

In a country where public demonstrations are subject to the state authorisation while the law states otherwise, demonstrations are difficult to implement, even if they are peaceful. However, demonstrations seem to be a privilege for citizens to make themselves heard and also hold the state accountable. In addition, a great deal of digital education must be introduced to allow citizens to understand the implications of all these laws that are enacted around digital technology on their daily lives, and to understand the consequences of these innovations on their economy but also to take precautions to protect their personal data from any unlawful processing.

Lastly, the legality approach, which means that approaches must comply with legal rights set out in national and international laws. This compliance requirement makes good legal sense because good practices in terms of personal data are contained in the African and West African legal framework such as the Malabo Convention and the additional act to the ECOWAS Treaty, relating to the protection of personal data. Togo has adopted the provisions of these international instruments, taking into account the requirements. However, it is important that compliance with the international framework does not stop only with the law on personal data, but is consistent with the laws that will follow.

This is the case for the example of the law on biometric identification, which introduces the possibility of collecting data of spoken language (which will easily make it possible to guess the ethnicity) while the collection of data that reveals the ethnic origin is prohibited within the meaning of the Personal Data Protection Act.

## Recommendations

In view of the state of play of the protection of personal data, it is clear that the government of Togo is undertaking interesting efforts in order to build a fairly relevant legal framework on personal data. The two recent laws relating respectively to the protection of personal data and to biometric identification (e-ID) have shown the government's effort to adapt its legal framework in line with the so-called fourth industrial revolution. Overall, Togo follows the regional and sub-regional movement in the protection of personal data. However, the challenge of implementing this legal framework is still considerable, especially in the field of practice.

There is also the challenge of lack of public awareness and a multistakeholder approach in the process of these legislative efforts. Citizens feel the need to know how to protect themselves online. Recent allegations of surveillance of some political and religious leaders bring the debate to the surface again. This means that the legal framework is not enough. But the information around this law, followed by the implementation is cardinal.

On the other hand, there is still a lot to be done, because the contexts of collection of personal data by the state remain unclear. To improve the protection of personal data in Togo, the following recommendations are important.

To the government:

- Adopt and enforce a comprehensive law that governs the establishment of all identification documents in Togo and affirms the right to privacy to avoid overlap and duplication of legislation as seen in the case of the DPA and e-ID laws.

- Set up a multistakeholder independent data protection authority that is appropriately resourced and has the authority to oversee and ensure the implementation of the law.
- Establish a continuity of digital policy framework so that the work continues despite changes of government.
- Take necessary measures to strengthen independent judicial authorisation and oversight mechanisms of communications surveillance.
- Abolish mandatory SIM card registration and establish a clear and precise framework for the collection of telephone data and communicate about the responsibilities of telephone operators with regard to the location and listening of subscribers by third parties. Regulations should encourage, but not mandate, “point of sale” registration. Where technically possible, governments should develop systems to enable real-time, online (identity) verification and registration of prepaid SIM users.
- Implement media and information literacy programmes to enhance public awareness regarding the importance of privacy and how the data of the citizens is being managed by the state or the data collectors.
- Make citizens aware of their rights over personal data (right of access, erasure, modification, deletion, etc.).
- Make sure that the law on biometric identification does not contain any aspect that could let people guess the religious orientation, sexual orientations, ethnicities and tribes.
- Inform and educate citizens on the scope of their activities online and give them tools to protect themselves from the abusive collection of their data.

- Build the capacity of local service providers to safeguard the electoral register and prevent foreign service providers from manipulating citizens' data.
- Disclose what type of surveillance technologies are employed by Togolese law enforcement and security agencies, how their acquisition and use is regulated and monitored, and how agencies are complying with Togolese national and international obligations.
- Inform the public about the guarantees of citizens against espionage and the unauthorised collection of their data.
- Establish multistakeholder policy dialogues such as internet governance forums and take stock of recommendations from all the stakeholders such as the government, the private sector, the academia, the technical community, internet users, etc.

To civil society organisations and academia:

- Conduct prompt and independent investigations into credible reports of unlawful surveillance of citizens, journalists, human rights activists, religious leaders and others, with the view to bringing to justice the perpetrators and providing reparations, and make publicly available the results of these investigations.
- Monitor and document infringements (violations and abuses) related to digital rights.
- Initiate capacity building  programmes for digital rights.
- Advocate to involve Togo in the Universal Periodic Review with regard to digital rights issues.

To the private sector:

- Respect the laws and policies regarding the protection of personal data.

## Conclusion

In spite of the great legislative and institutional framework development in recent years in Togo, there remain obstacles to dealing effectively with cybercrime linked in particular to the global nature of the phenomenon, which ignores state borders. This is a source of legal difficulty in conducting investigations and protecting citizens. The effective ratification of the Budapest Convention and Malabo Convention would open up new perspectives in terms of data protection and cybersecurity.

Furthermore, on the issue of non-discrimination, as formulated in the law on personal protection, any question of ethnicity should be removed in the constitution of personal databases.

The data protection law should reflect general opinions and attitudes and adjust to the times. The general tendencies about the implementation of the law are not clear and the future is as always uncertain. Data protection may increase and it may decrease. Only one thing seems certain. The near future will present major challenges to data protection law in Togo and a paradigm shift in the way government, corporations and individuals carry on business and interact with respect to the data in their possession will be key.

# Uganda

**Paul Kimumwe**
Collaboration on International ICT Policy
in East and Southern Africa (CIPESA)

## Executive summary

The right to privacy and personal data protection is a fundamental human right that should have guaranteed protection nationally and across borders. In Uganda, the right is enshrined in Article 27 of the constitution and was further buttressed with the enactment of the Data Protection and Privacy Act, 2019[1] that provides for the protection of the privacy of the individual and of personal data by regulating the collection and processing of personal information. It marked a milestone as Uganda became the first country in East Africa to pass a data protection law.

1 https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf

The law provides for the legal rights of persons whose data is collected and the obligations of data collectors, data processers and data controllers, as well as regulating the use or disclosure of personal information.

Prior to the enactment of the Data Protection and Privacy Act, the government had passed several other laws and policies that contained several provisions that permitted the collection and processing of personal data, including biometrics, without proper safeguards.

These included the Regulations of Interception of Communications Act, 2010 that requires, under section 9(2), telecommunication service providers to ensure that existing subscribers register their SIM cards within the period of six months from the date of commencement of the act.

The other is the Registration of Persons Act, 2015[2] that sought to harmonise and consolidate the law on registration of persons; to provide for registration of individuals; to establish a national identification register; to establish a national registration and identification authority; to provide for the issue of national identification cards and aliens' identification cards and for related matters.

Unfortunately, it was not until August 2020 that the government issued the first draft of the Data Protection and Privacy Regulations that specify and give effect to the application of the Act. At the time of writing this report, the regulations were yet to be gazetted. Additionally, the government was also yet to operationalise the office of the Data Protection Officer, which affects the full implementation of the act.

2 https://www.nira.go.ug/wp-content/uploads/Publish/Registration%20of%20Person%20Act%202015.pdf

But even without the enabling law and regulations, there has been some successful litigation against the infringements on the right to privacy and data protection.

In May 2020, the High Court at Kampala ordered The Pepper Publications Ltd, the publishers of tabloid newspapers *Red Pepper* and *Kamunye* to pay to former Oyam South MP and Former LRA Commander Dominic Ongwen's lawyer Krispus Ayena Odongo UGX 75 million (USD 20,000) as compensation for violating his privacy and dignity when they published in 2016 leaked photos of him having sex with an unnamed woman.[3]

## Methodology

This was a purely qualitative research, and involved a combination of data collection methods, which included conducting a comprehensive literature review, including a detailed legal and policy and legal analysis; as well as conducting key information interviews.

The literature review entailed detailed analysis of all relevant literature (reports, submissions, newspaper articles, among others) on privacy and data protection in Uganda. There are a number of human rights organisations, such as Privacy International, ARTICLE 19, Human Rights Watch, Unwanted Witness, CIPESA, Freedom House and Human Rights Network for Journalists in Uganda, that have written extensively about privacy and data protection rights in Uganda, including making submissions to the United Nations Universal Periodic Review (UPR) mechanisms on the same. This review will provide a deeper understanding of the status of privacy and data protection rights in Uganda.

3 Ahikiria, B. M. (2020, 30 May). Ongwen's Lawyer Ayena Odongo awarded 75m in privacy case over leaked nude pictures. *The Legal Reports*. https://thelegalreports.com/2020/05/29/ongwens-lead-lawyer-ayena-odongo-wins-75m-in-privacy-case

Additionally, the legal and policy analysis of the different laws, policies and regulations that contain provisions on privacy and data rights (including the collection and processing) was conducted. These laws will include, the Privacy and Data Protection Act, 2019; the Regulation of Interception of Communications Act, 2010; the Anti-Terrorism Act, 2015 (as amended) and the Uganda Communications Act; 2013.

Key informant interviews with purposively selected stakeholders, with knowledge and expertise on privacy and data protection rights were conducted. The main purpose was to gain context and insight into the practices and behaviours of the state towards these rights.

## Country context

Since gaining independence from Britain in 1962, and up to 1896, Uganda endured a state of political instability that included a military coup in 1971, followed by a brutal military dictatorship which ended in 1979, disputed elections in 1980 and a five-year protracted war that brought current President Yoweri Museveni to power in 1986.[4] Since then, the country has enjoyed relative peace.

Boasting one of the youngest populations in the world, where more than half the population is younger than age 15,[5] Uganda's economy is reported to have experienced a slowdown in growth due to the severe impact of the COVID-19 pandemic crisis, a locust invasion and flooding caused by heavy rains. Real gross domestic product (GDP) in 2020 is now projected to be between 0.4 and 1.7% compared to 5.6% in 2019.[6]

4 BBC. (2018, 10 May). Uganda Country Profile. *BBC*. https://www.bbc.com/news/world-africa-14107906

5 Republic of Uganda. (2019). *The State of Uganda Population Report 2019*. https://www.finance.go.ug/sites/default/files/press/REPORT%20SUPRE%202019%20SIG-FINAL2_0.pdf

6 https://www.worldbank.org/en/country/uganda/overview

And while the country conducts regular elections, their credibility has deteriorated over time. The ruling party, the National Resistance Movement (NRM), retains power through patronage, the manipulation of state resources, intimidation by security forces, and politicised prosecutions of opposition leaders.[7] According to Freedom House (2019), internet freedom in Uganda continues to suffer as the government intensifies its crackdown on online expression, including by blocking over two dozen pornographic websites and imposing a tax on social media and communication platforms for the purpose of curbing "gossip".[8]

While the country has registered an increase in internet connectivity, with the latest figures from the Uganda Communications Commission (UCC), indicating that there were 16.9 million (about 41%) internet subscribers by the end of December 2019,[9] there are also growing concerns over the government's increasing surveillance capability over citizens' communications.[10]

The government has continued to infringe on individual privacy rights and narrowed civic space through various activities including the alleged planting of FinFisher intrusion malware on hotel Wi-Fi to illegally spy on targeted persons;[11] enactment of restrictive legislation such as the Regulation of Interception of Communication Act, 2010 and the Anti-Terrorism Act, 2020, which authorise the interception of individuals' communications.[12]

7 Freedom House. (2019). *Freedom on the Net: Uganda*. https://www.justice.gov/eoir/page/file/1234706/download

8 Ibid.

9 Uganda Communications Commission. (2020). *Market Performance Report January 2020.* https://www.ucc.co.ug/wp-content/uploads/2020/05/Market-Performance-Report-Jan-2020.pdf

10 Mbah, F. (2018, 21 August). Uganda: The changing face of political opposition. *Al Jazeera*. https://www.aljazeera.com/news/2018/08/uganda-changing-face-political-opposition-180821104936104.html

11 Privacy International. (2015). *For God and My Country: State Surveillance in Uganda*. https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

12 CIPESA. (2018). *State of Internet Freedom in Africa 2018 – Privacy and Personal Data Protection: Challenges and Trends in Uganda*. https://cipesa.org/?wpfb_dl=338

The passage of the Data Protection and Privacy Act, 2019, and the recent publication of the attendant regulations therefore came as a relief as it provides some safeguards in preserving the privacy and protection of personal data. For example, section 4 provides for the establishment of a Personal Data Protection Office responsible for the protection of personal data, under the National Information and Technology Authority. Unfortunately, both the regulations and Data Protection Office are yet to be gazetted and operationalised, respectively, which affects the full implementation of the Data Protection and Privacy Act.

## Constitutional underpinning

In Uganda, the right to privacy of a person, home, or other property (including personal data) is explicitly provided for under Article 27 of the Constitution, which states that:

> (1) No person shall be subjected to:
>
> (a) unlawful search of the person, home, or other property of that person; or
>
> (b) unlawful entry by others of the premises of that person.
>
> (2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication, or other property.

The provisions have been used as basis in successfully litigating against invasions of privacy. For example, in May 2020, the High Court at Kampala ordered The Pepper Publications Ltd, the publishers of tabloid newspapers *Red Pepper* and *Kamunye* to pay to former Oyam South MP and former Lord's Resistance Army (LRA) Commander Dominic Ongwen's lawyer Krispus

Ayena Odongo UGX 75 million (USD 20,000) as compensation for violating his privacy and dignity when they published leaked photos of him having sex with an unnamed woman in 2016.[13]

## Existence of other laws dealing with privacy and data protection online

Besides the Data Protection and Privacy Act, the government has, over the years, passed several other laws and policies that contain several provisions that permitted the collection and processing of personal data, including biometrics, without proper safeguards.

The Regulations of Interception of Communications Act, 2010[14] requires, under section 9(2), telecommunication service providers to ensure that existing subscribers register their SIM cards within the period of six months from the date of commencement of the act. The law also requires intelligence officials and the police to seek judicial authorisation for the interception of specific communications.

Under section 3, the act also provides for the establishment of a Monitoring Centre under the control of the minister – the "sole facility through which authorised interceptions shall be effected."

The other is the Registration of Persons Act, 2015[15] that sought to harmonise and consolidate the law on registration of persons; to provide for registration of individuals; to establish a national identification register; to establish a national registration and identification authority; to provide for the issue of national identification cards and aliens identification cards and for related matters.

13 Ahikiria, B. M. (2020, 30 May). Op. cit.

14 https://ulii.org/ug/legislation/act/2015/18-2

15 https://www.nira.go.ug/wp-content/uploads/Publish/Registration%20of%20Person%20Act%202015.pdf

The other law is the Computer Misuse Act, 2011,16 which criminalises unauthorised access (section 13), unauthorised modification of data (section 14), unauthorised use or interception of computer services (section 15), unauthorised disclosure of access codes (section 17), and unauthorised disclosure of information (section 18).

## Regional and international commitments on privacy and personal data protection

Uganda is a signatory to several international and regional instruments that provide for the protection and promotion of the right to privacy and data protection. These include the Universal Declaration of Human Rights (UDHR),[17] International Covenant on Civil and Political Rights (ICCPR),[18] United Nations Convention on the Rights of the Child (UNCRC),[19] and United Nations Convention on the Rights of Persons with Disabilities (CRPD).[20]

Article 12 of the UDHR provides that:

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

On the other hand, Article 17 of the ICCPR provides that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and

16 https://ulii.org/ug/legislation/act/2015/2-6

17 https://www.un.org/en/universal-declaration-human-rights

18 http://hrlibrary.umn.edu/instree/b3ccpr.htm

19 http://hrlibrary.umn.edu/instree/k2crc.htm

20 http://hrlibrary.umn.edu/instree/disability-convention2006.html

> reputation. Everyone has the right to the protection of the law against such interference or attacks.

The UNCRC recognises the right to privacy of children under Article 16, stating that:

> No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

Meanwhile, the CRPD provides that:

> No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

As a state party, Uganda is also bound by the December 2014 UN Resolution 69/166 on Privacy in the Digital Age,[21] which affirmed that the same rights that people have offline must also be protected online, including the right to privacy.

On the continent, Uganda is a party to the African Charter on the Rights and Welfare of the Child,[22] which, under Article 19, guarantees the right of the child, stating:

> No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents

21 https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

22 https://www.un.org/en/africa/osaa/pdf/au/afr_charter_rights_welfare_child_africa_1990.pdf

or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children.

At the time of writing this report, Uganda was yet to sign the African Union Convention on Cyber Security and Personal Data Protection (AU Convention).[23]

## Uganda Data Protection and Privacy Act, 2019 and Regulations 2020

In 2018, Uganda passed the Data Protection and Privacy Act, 2019 that provides for the protection of privacy of the individual and of personal data by regulating the collection and processing of personal information.[24] The act entered into force in February 2019 after it was assented to by the president.[25]

The enactment provides Ugandans with the strongest safeguards of their right to privacy as enshrined in Article 27 of the constitution.[26]

The act provides for the legal rights of persons whose data is collected and the obligations of data collectors, data processers and data controllers, as well as regulating the use or disclosure of personal information.[27]

For example, section 18 of the Data Protection and Privacy Act, 2019, provides that personal data shall be retained only for a period necessary to achieve the purpose for which the data is collected and processed.

23 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.pdf

24 https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf

25 NITA Uganda. (2019, 28 February). President Museveni signs Data Protection and Privacy Bill into law. https://www.nita.go.ug/media/president-museveni-signs-data-protection-privacy-bill-law

26 CIPESA. (2019). *The Highs and Lows of Uganda's Data Protection and Privacy Act 2019*. https://cipesa.org/?wpfb_dl=303

27 Ibid.

Section 4 provides for the establishment of a personal data protection office responsible for the protection of personal data, under the National Information and Technology Authority, and reports directly to the authority's board. The government is also yet to start the process of establishing the personal data protection office and appointing the office bearers.

## Lack of enabling regulation

However, the lack of the regulation and the failure to establish the personal data protection office have hampered the effective implementation of the law.

For example, it was not until August 2020 that the government published the draft Data Protection and Privacy Regulations, 2020, specifying the procedural aspects and guaranteeing effective implementation of the act. Also, in the draft regulations, regulation 4 expounds on the functions of the Data Protection Office to include coordination and guidance, capacity building, monitoring and regulating standards, undertaking research and issuing recommendations on interpretation of data protection rules.[28]

Regulations 14(2)(k) and (3) and 28(1-5) provide more protection of data subjects' rights whose data may be transferred across national borders by putting in place checks and balances on measures for data protection outside Uganda, and requiring the data subject's consent before such data is processed.[29]

And yet the government and its agencies such as the National Identification and Registration Authority (NIRA), Ministry of

28 CIPESA. (2020). *Uganda's Draft Data Protection and Privacy Regulations, 2020*. https://cipesa.org/?wpfb_dl=359

29 Ibid.

Health, and private entities such as telecom companies are still engaged in unregulated collection, processing and sharing of personal data for national identity cards, contract tracing of COVID-19 suspected infections and patients, as well as SIM card registration.

## Key features of the Data Protection and Privacy Act, 2019

### Key definitions

Under section 1, the Act provides interpretations of the terms used in the act. Below are some of the most critical:

- *Consent* means any freely given, specific, informed and unambiguous indication of the data subject's wish in which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her.
- *Data* means information which (a) is processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or (d) does not fall within paragraph (a),(b) or (c) but forms part of an accessible record.
- *Data collector* means a person who collects personal data.
- *Data controller* means a person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.

- *Data processor* in relation to personal data means a person other than an employee of the data controller who processes the data on behalf of the data controller.

- *Data subject* means an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.

- *Information* includes data, text, images, sounds, codes, computer programmes, software and databases.

- *Personal data* means information about a person from which the person can be identified, that is recorded in any form and includes data that relates to (a) the nationality, age or marital status of the person; (b) the educational level, or occupation of the person; (c) an identification number, symbol or other particulars assigned to a person; (d) identity data; or (e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

## Data subject rights

The Data Protection and Privacy Act, 2019 defines a data subject as “an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.” The act contains several provisions on the right of data subjects.

Under section 7 of the act, data collectors are required to seek consent of the data subject prior to the collection or processing of personal data.

While section 8(a) prohibits the collection or processing of personal data relating to a child without prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child.

Section 10 provides for the privacy of the data subject, noting that “a data collector, data processor or data controller shall not collect, hold or process personal data in a manner which infringes on the privacy of a data subject.”

Under section 16, a data subject has the right to correct, delete or even seek to destroy a record of personal data which is (a) inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or (b) which the controller no longer has the authority to retain.

Part V of the act provides details on the specific rights of data subject including the right to access personal information from a data controller (section 24), the right to prevent the processing of personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject (section 25.1), the right to prevent the processing of personal data for direct marketing (section 26), and rights in relation to automated decision-making, noting that, “A data subject may by notice in writing to a data controller require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects that data subject is not based solely on the processing by automatic means of personal data in respect of that data subject” (section 27).

Under section 28, data subjects also have rights to rectification, blocking, erasure and destruction of personal data where such data is inaccurate.

## Conditions for lawful processing

Section 7(2) of the Data Protection and Privacy Act provides for the lawful collection and processing of personal data, noting that:

> Personal data may be collected or processed: (a) where the collection or processing is authorised or required by law; (b) where it is necessary; (i) for the proper performance of a public duty by a public body; (ii) for national security; (iii) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law; (c) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (d) for medical purposes; or (e) for compliance with a legal obligation to which the data controller is subject.

## Relevant exemptions in the public interest

Although section 7(1) provides that a person shall not collect or process personal data without the prior consent of the data subject; this does not apply to section 7(2) where data being collected is required by law or necessary for national security, among others.

## Breach notification requirements

Section 23 of the act provides guidelines of notification in case of data security breaches.

Specifically, section 23(1) requires data collectors, data processors or data controllers, who believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, to immediately notify the authority, in the prescribed manner, of the unauthorised access or acquisition and the remedial action taken.

Once notified, the authority shall determine and notify the data controller, data collector or data processor whether the data controller, data collector or data processor should notify the data subject of the breach (section 23.2).

Section 23(3) states that where the authority determines that the data collector, data processor or data controller should notify the data subject, the notification shall be made by (a) registered mail to the data subject's last known residential or postal address; (b) electronic mail to the data subject's last known electronic mail address; (c) placement in a prominent position on the website of the responsible party; or (d) publication in the mass media.

Section 31 of the act provides for complaints in case of breach and non-compliance by the data collector, processor, or controller. Section 31(1) notes that a data subject or any person who believes that a data collector, data processor or data controller is infringing upon their rights or is in violation of this act may make a complaint in the prescribed manner to the authority. Section 31(2) says that a data collector, data processor or data controller may, in writing, make a complaint to the authority about any violation or noncompliance with this act.

## Cross-border data transfers

Section 19 of the act requires a data processor or data controller who is based in Uganda but processes and or stores personal data outside Uganda, to ensure that (a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this act or (b) the data subject has consented.

## Other relevant features

In Part IV, the act provides for security of data, specifically, section 21 requires a data controller, data collector or data processor to secure the integrity of personal data in their possession or control by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage, or unauthorised destruction and unlawful access to or unauthorised processing of the personal data.

In regard to data retention, the act under section 18 states that personal data shall be retained only for a period necessary to achieve the purpose for which the data is collected and processed. Once that period elapses, the personal records must be deleted or destroyed beyond reconstruction in an intelligible form.

## Personal Data Protection Office

Section 4 of the Data Protection and Privacy Act, 2019 provides for the establishment of a Personal Data Protection Office, responsible for personal data protection under the National Information Technology Authority – Uganda (NITA-U), which shall report directly to the board.

Under section 4(2) the office shall be headed by a national personal data protection director, appointed on such terms and conditions as may be specified in his or her instrument of appointment.

Among its functions, as outlined under section 5, are to:

- Oversee the implementation of and be responsible for the enforcement of this Act.

- Promote the protection and observance of the right to the privacy of a person and of personal data.
- Monitor, investigate and report on the observance of the right to privacy and of personal data.
- Formulate, implement and oversee programmes intended to raise public awareness about this Act.
- Receive and investigate complaints relating to infringement of the rights of the data subject under this Act.
- Establish and maintain a data protection and privacy register.
- Perform such other functions as may be prescribed by any other law or as the office considers necessary for the promotion, implementation and enforcement of this Act.

Section 5(3) provides for the independence of the office, noting that "in performing its functions under this Act [it] shall not be under the direction or control of any person or Authority."

However, the implied oversight of the data protection office by the NITA-U board raises questions as to whether the office will be run independently or not. Additionally, the draft data protection and privacy regulations do not provide for independent financing of the office. By implication, the data protection office is supposed to rely on finances from NITA-U.[30]

Furthermore, the data protection office, which should oversee the overall implementation of the law, providing for administrative, civil or criminal sanctions and penalties, among others, has yet to be established.[31]

30 CIPESA. (2020). Op. cit.

31 Unwanted Witness. (2020, 3 March). One Year On, What Has Uganda's Data Protection Law Changed? *Privacy International.* https://privacyinternational.org/news-analysis/3385/one-year-what-has-ugandas-data-protection-law-changed

## Organisations/associations involved in advocacy related to data protection

Several organisations have been at the forefront of advancing data protection and privacy rights in Uganda.

### The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

CIPESA[32] has been consistent in engaging with and raising pertinent issues on data protection and privacy, including making submissions to the different versions of the Data Protection and Privacy Bill, since it was first published in 2014. In 2015, CIPESA made submissions[33] on the first draft calling for expansion in the consultations with different stakeholders including civil society, private sector, government and academia for an extended period prior to tabling before parliament.

In 2018, CIPESA again made submissions[34] to the the Committee on Information and Communication Technologies of the Parliament of the Republic of Uganda about the 2015 version of the Data Protection and Privacy Bill, calling for the establishment of an independent data protection commission instead of the proposed National Information Technology Authority Uganda (NITA-U).

CIPESA also made a legal analysis of the enacted law,[35] highlighting the positives and weaknesses in the laws, and

32 https://cipesa.org/about-us/

33 CIPESA. (2015). *Reflections on Uganda's Draft Data Protection and Privacy Bill, 2014.* https://cipesa.org/?wpfb_dl=185

34 CIPESA. (2018). *Comments Presented to the Committee on Information and Communication Technologies of the Parliament of the Republic of Uganda.* https://cipesa.org/?wpfb_dl=263

35 CIPESA. (2019). Op. cit.

submitted comments[36] and on the draft regulations that were published in August 2020.

## Unwanted Witness

Unwanted Witness[37] has written extensively about personal data protection in Uganda and has been very active in the making submissions and reports on the different bills and laws. In 2019, it conducted a study about the Safeboda privacy policy and its practice, considering that it is Uganda's leading transport application.[38] Unwanted Witness has also issued several statements condemning the collection of citizens' personal identifiable data by all *boda boda* riders and salon operators.[39]

## Human Rights Network for Journalists in Uganda (HRNJ-Uganda)

The network has also been active in defending human rights, especially of journalists. In 2012, the organisation was instrumental in opposing the SIM card registration, terming it an infringement on freedom of expression and the right to privacy.[40] The organisation went ahead and sued the communication regulator, UCC, although the case was later dismissed on the grounds that the "petitioners had failed to provide an exact number of the people likely to suffer from the process of unregistered SIM cards being switched off."[41]

36 CIPESA. (2020). Op. cit.

37 https://www.unwantedwitness.org

38 Unwanted Witness. (2019). *Trading Privacy For A Cheap Transport System.* https://www.unwantedwitness.org/download/uploads/Trading-Privacy.pdf

39 Unwanted Witness. (2020, 27 July). Collection of Personally Identifiable Data Threatens National Security and Human Rights. https://www.unwantedwitness.org/collection-of-personal-identifiable-data-threatens-national-security-and-human-rights-warns-unwanted-witness

40 Human Rights Network for Journalists – Uganda. (2012, 21 September). SIM card registration in Uganda curtails freedom of expression and right to privacy. https://www.hrnjuganda.org/sim-card-registration-in-uganda-curtails-freedom-of-expression-and-right-to-privacy

41 Genrwot, J. (2013, 3 September). High Court Dismisses Suit Against SIM Card Registration Deadline. *PC Tech Magazine*. https://pctechmag.com/2013/09/high-court-dismisses-suit-against-sim-card-registration-deadline

## Privacy International

Through its local partners, including CIPESA and Unwanted Witness, Privacy International has been vocal in raising issues of privacy and data protection in Uganda, including making a joint submission to the United Nations Human Rights Council[42] on the state of privacy in Uganda and documenting this state of privacy.[43]

## Data protection practices in internet country code top level domain name (ccTLD) registration

In Uganda, the government of the country is involved in a struggle over who should have the custodial rights to manage the .ug domain, the country code top-level domain (ccTLD), which is currently run by a third party.[44]

The .ug domain is currently managed by a privately owned company, Infinity Computers and Communication Company (i3C),[45] based in Uganda. This management includes the setting of policies on domain usage, technical and administrative functions of the ccTLD, domain registrar and sponsor.[46]

Unfortunately, the "WHOIS" records for .ug return personal data, in total breach of the regulations on personal data protection imposed by the European Union (under the GDPR) on all data processors and controllers including registries and registrars, regardless of whether the registrant is a resident of the European

42 Unwanted Witness, CIPESA, the East and Horn of Africa Human Rights Defenders Project, & Privacy International. (2016). *The Right to Privacy in Uganda*. https://privacyinternational.org/sites/default/files/2017-12/uganda_upr2016.pdf

43 Privacy International. (2019, 26 January). State of Privacy in Uganda. https://privacyinternational.org/state-privacy/1013/state-privacy-uganda

44 Muheebwa, H. (2014, 6 October). Uganda Government Moves Towards Top-Level Domain Management. *Intellectual Property Watch.* https://www.ip-watch.org/2014/10/06/uganda-government-moves-towards-top-level-domain-management

45 https://i3c.co.ug

46 Ibid.

Economic Area or not. For example, at https://whois.domaintools.com/dynamaps.ug and https://domainr.com/dynamaps.ug?q=dynamaps.ug, the data is publicly available and there is no need to request it. But in the case of Uganda, even if it were not, it would be tricky since the ccTLD is managed by a private entity, and not bound by the provisions of the Access to Information Law, which limits citizens right of access to information and records in the possession of the state or any public body.[47]

## Analysis in line with AfDec and other relevant instruments

The African Declaration on Internet Rights and Freedoms[48] is a pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. The declaration is intended to elaborate on the principles which are necessary to uphold human and people's rights on the internet, and to cultivate an internet environment that can best meet Africa's social and economic development needs and goals.

The declaration has 13 key principles, including openness; internet access and affordability; freedom of expression; right to information; freedom of assembly and association on the internet; cultural and linguistic diversity; right to development and access to knowledge; privacy and personal data protection; security, stability and resilience of the internet; marginalised groups at risk; due process; democratic multi-stakeholder internet governance; and gender equity.[49]

47 Section 5, Access to Information Act, 2005. http://judiciary.go.ug/files/downloads/access%20to%20informatioinformation%20Act2005.pdf

48 https://africaninternetrights.org/en/about

49 Ibid.

For purposes of this study, we will look at Principle 8, which deals with privacy and personal data protection. According to this principle:

> Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.

The principle requires that:

> The collection, retention, use and disclosure of personal data or information must comply with a transparent privacy policy which allows people to find out what data or information is collected about them, to correct inaccurate information, and to protect such data or information from disclosure that they have not authorised.

For its part, the African Union Convention on Cyber Security and Personal Data Protection (also referred to as the Malabo Convention)[50] under Article 8 calls upon state parties to commit to establish a "legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data." Under Article 9, state parties are required to provide for the establishment of a national data protection authority/office, which is independent and is responsible for ensuring that the processing of personal data is done in accordance with the provisions of the convention.

50 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Section IV of the convention also provides for the rights of data subjects, including the right to information (Article 16), the right to access (Article 17), the right to object to the processing of the data relating to him/her (Article 18), and the right to rectify, complete, delete or update personal data in cases where the data is inaccurate, incomplete, or outdated. The convention also provides for confidentiality (Article 20) and security (21) of all personal data being processed.

The Personal Data Protection Guidelines for Africa,[51] which were developed jointly by the Internet Society (ISOC) and the African Union Commission, emphasise the importance of ensuring trust in online services and set out 18 recommendations for governments and policymakers, data protection authorities (DPAs), data controllers and their partners, and citizens and civil society based on the multistakeholder model.[52]

The guidelines reiterate the essential principles relating to online personal data protection including: consent and legitimacy; fair and lawful processing; purpose and relevance of data; management of the data lifecycle (retention, accuracy, deletion); transparency of processing and confidentiality and security of personal data. It remains to be seen how they will be received and implemented by states.[53]

The revised Declaration of Principles on Freedom of Expression and Access to Information in Africa[54] provides for exemptions for withholding information if the release would result in the

51 Internet Society & Commission of the African Union. (2018). *Personal Data Protection Guidelines for Africa.* https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

52 CIPESA. (2018). *State of Internet Freedom in Africa 2018 – Privacy and Data Protection in the Digital Era: Challenges and Opportunities*. https://cipesa.org/?wpfb_dl=278

53 Ibid.

54 https://www.achpr.org/legalinstruments/detail?id=69

unreasonable disclosure of the personal information to a third party, endanger the life, health, safety of an individual, result in the disclosure of confidential communication between medical practitioner and patient, lawyer and client, journalist and sources, or is otherwise privileged from disclosure in legal proceedings, among others (Principle 33).

The current data protection and privacy framework in Uganda conforms to the provisions of the AfDec and other regional instruments.

Section 3 of the Data Protection and Privacy Act, 2019 details the key principles of data protection, including accountability; fair and lawful processing; specification and purpose limitation; data retention for only specified periods; quality assurance; transparency and participation of the data subject; and observance of security safeguards. The authority is required to ensure that every data collector, data controller, data processor or any other person collecting, or processing data complies with the principles of data protection and this act.

The act under section 9 prohibits the collection and processing of special personal data which relates to beliefs in religion or philosophy, political opinions, sexual life, financial information, health status or medical records of an individual save for data collected within the acceptable lawful limits.

The act also provides for various data subject rights, including the right of access to information (section 24), the right to prevent processing of personal data (sections 25 and 26), the rights in relation to automated decision making (27) right to rectification, blocking, erasure and destruction of personal data (28), which are all provided for under the AfDec and other instruments.

Section 12 also provides for limitations and requires data controllers or controllers to only collect or process data for specific purpose which should be explicitly defined and is related to the functions or activity of the data collector, or data controller.

Section 13 requires calls for data subjects to be informed and given explainations that data is to be collected for a particular purpose.

In processing data, section 14 requires the data processor to ensure that only necessary or relevant data is processed. Such data must be complete, accurate, up-to-date and not misleading. Further, the data subject should, in line with section 16, be given an opportunity to correct or delete or destroy their data.

In line with the data retention principle which is to the effect that data should be kept for no longer than is necessary for the purposes for which it is being processed, the act under section 18 subsections (1), (3), (4) and (5) provides that personal data shall be retained only for a period necessary to achieve the purpose for which the data is collected and processed. After this period, such data should be deleted or destroyed beyond reconstruction in an intelligible form.

The act also provides for the establishment of a data protection office, as envisaged by the AU Convention.

As a state party to the International Convention on Civil and Political Rights, Uganda is required to provide regular updates on its human rights record to the United Nations Human Rights Council, during the Universal Periodic Review (UPR). In 2011, when Uganda underwent her first review, both the Ugandan

government[55] and civil society reports[56] did not explicitly mention the rights to privacy and data protection.

During the 2016 UPR, one of the civil society joint submissions called for the immediate enactment of the 2014 Privacy and Data Protection Bill to curb targeted surveillance and protect the enjoyment of privacy, and revision of existing legislation and policies.[57] However, the final report did not include any recommendation to Uganda regarding the enactment of the Data Protection and Privacy Bill 2014.[58]

In regards to any measures taken by the country to update its laws in line with the European Union's General Data Protection Regulation (GDPR), the principles of data protection in the act, accountability to the data subject for their data, collecting and processing data fairly and lawfully, and observing security safeguards in respect of such data, appear to have been borrowed from the GDPR.[59]

## Analysis of the status of a human rights-based approach to personal data protection in Uganda

According to the human rights-based approach principle on *participation*, everyone is entitled to active participation in decision-making processes which affect the enjoyment of

55 United Nations. (2011). National report submitted in accordance with paragraph 15 (a) of the annex to Human Rights Council resolution 5/1. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/12/UGA/1&Lang=E

56 United Nations. (2011). Summary prepared by the Office of the High Commissioner for Human Rights in accordance with paragraph 15 (c) of the annex to Human Rights Council resolution 5/1. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/12/UGA/3&Lang=E

57 United Nations. (2016). Summary prepared by the Office of the United Nations High Commissioner for Human Rights in accordance with paragraph 15 (c) of the annex to Human Rights Council resolution 5/1 and paragraph 5 of the annex to Council resolution 16/21. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/26/UGA/3&Lang=E

58 United Nations. (2017). Report of the Working Group on the Universal Periodic Review: Uganda. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/34/10&Lang=E

59 Sendi, B. K. (2019, June). Uganda: Overview of the Data Protection and Privacy Act, 2019. *Data Guidance.* https://www.dataguidance.com/opinion/uganda-overview-data-protection-and-privacy-act-2019

their rights. The participation must be from all affected parties, individuals, men and women, communities, civil societies, indigenous populations, and others. Participation must be active, free, and meaningful.[60]

Unfortunately, this does not seem to have been the case in Uganda during the enactment of the Data Protection and Privacy Act, 2019. According to the report of the Parliamentary Sectoral Committee on Information, Communication Technology and National Guidance on the Data Protection and Privacy Bill, 2015,[61] the committee held consultative meetings and received memoranda from only 34 stakeholders, including telecom companies, government ministries, department and agencies, pay television companies, professional bodies, and media entities, among others. Conspicuously absent from the list were marginalised groups including the elderly, persons with disabilities, women, youth and children. This is despite the existence of numbers of groups and associations representing these sectors.

The *accountability* principle requires that duty-bearers are held accountable for failing to fulfil their obligations towards rights holders. There should be effective remedies in place when human rights breaches occur. Although the UDHR has been interpreted as primarily applying to states, and it has operated as a template for conventions that impose legal duties exclusively on states, the role of non-state actors such as such as transnational corporations, and their impact on the enjoyment of human rights has become more prominent, making them duty bearers as well.[62]

60 UNESCO Bangkok. (2008). *The human rights-based approach to journalism: Training manual Viet Nam.*

61 Parliament of Uganda. (2018). *Report of the Sectoral Committee on Information, Communication Technology and National Guidance on the Data Protection and Privacy Bill, 2015.* https://parliamentwatch.ug/wp-content/uploads/2019/11/ICT3-18-Report-on-the-Data-Protection-and-Privacy-Bill-2015-1.pdf

62 Tasioulas, J. (2019, 19 November). The connection between human rights, duties and duty-bearers. *ABC*. https://www.abc.net.au/religion/human-rights-duties-and-duty-bearers/11719722

Additionally, business corporations have a responsibility to respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.[63]

The Data Protection and Privacy Act, 2019 provides distinction on the rights of data subjects and obligations of the data collectors or controllers. In order to foster accountability, the act also creates offences and penalties for breaches.

The act criminalises the unlawful obtaining or disclosing of personal data (section 35); unlawful destruction, deletion, concealment, or alteration of personal data (section 36) and the sale of personal data (section 37). Conviction as a result of any of these offences attracts a fine not exceeding 240 currency points or imprisonment for years or both; a fine not less than 240 currency points or imprisonment not exceeding 10 years or both; and a fine not exceeding 245 currency points or imprisonment not exceeding 10 years or both; respectively.

The act under section 38 provides for special offences committed by corporations, the biggest data collectors.
In addition to the punishment, the court can order the corporation[64] to pay a fine not exceeding 2% of the corporation's annual gross turnover. In their report to parliament on the Data Protection and Privacy Bill, the committee observed that the fines levied therein are not deterrent enough for corporations and thus there is need to provide for additional penalties. In their recommendations, the committee recommended that a fine of not more than 4% of the corporation's annual gross turnover be

63 United Nations. (2011). *Guiding Principles on Business and Human Rights*. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

64 According to the Data Protection and Privacy Act, 2019, a corporation is defined as an entity created under a law and is separate and distinct from its owners.

imposed in addition to other penalties imposed under the law in case of breach.[65]

Within the context of the human rights-based approach, the *non-discrimination and equality* principles provides that all individuals are entitled to their rights without discrimination of any kind. All types of discrimination should be prohibited, prevented, and eliminated. The human rights requirement for non-discrimination demands that particular focus be given to the status of vulnerable groups, to be determined locally, such as minorities, Indigenous peoples or impoverished groups, within the context of a Rights-based approach.

Unfortunately, the act does not make any special mention of other vulnerable groups, such as persons with disabilities and the elderly. It only mentions the children whose data can be collected after seeking consent from their parents or guardians (section 8).

*Empowerment* under the human rights-based approach requires that everyone is entitled to claim and exercise their rights. In addition, individuals and communities need to understand their rights and participate in the development of policies which affect their lives.

As noted under participation, there was little involvement in the development of the Data Protection and Privacy Act, 2019, especially from the most vulnerable and marginalised groups. However, there is a growing evidence of empowerment with more people filing court cases against infringement on their rights to privacy.

65 Parliament of Uganda. (2018). Op. cit.

In November 2010, high court judge, Vincent Musoke-Kibuka issued an injunction against the *Rolling Stone* tabloid from further publication of names or pictures of anyone the tabloid perceived to be gay, lesbian or homosexual in general as this would be tantamount to an infringement or invasion of the right to privacy of those persons.[66]

In another landmark case, in May 2020, the High Court at Kampala ordered The Pepper Publications Ltd, the publishers of tabloid newspapers *Red Pepper* and *Kamunye* to pay to former Oyam South MP and Former LRA Commander Dominic Ongwen's lawyer Krispus Ayena Odongo UGX 75 million (USD 20,000) as compensation for violating his privacy and dignity when they published in 2016 leaked true photos of him having sex with an unnamed woman.[67]

In another case, in March 2018, Hon. Lady Justice H. Wolayo, awarded one Basajjabaka Yakub UGX 40 million (USD 12,000) nominal damages for infringement of the right to privacy.[68] Basajjabaka had sued MTN Uganda accusing them of using his image in an advertisement without his consent.

While these court cases can spur interest from the population to appreciate their rights, a lot needs to be done to continue empowering them to demand their rights and hold duty bearers, especially data collectors and processors, accountable.

And lastly, the human rights-based approach principle on *legality* requires that approaches should be in line with the legal rights

66 Kimumwe, P. (2020). *Media Regulation and Practice in Uganda: A Journalists Handbook*, *2nd ed*. https://www.scribd.com/document/226805466/Media-Regulation-and-Practice-in-Uganda-A-Journalists-Handbook

67 Ahikiria, B. M. (2020, 30 May). Op. cit.

68 Uganda Legal Information Institute. (2018). *Basajjabaka v MTN Uganda Ltd* (HCCS. NO. 100 OF 2012) [2018] UGHCCD 22 (26 March 2018). https://ulii.org/ug/judgment/hc-civil-division-uganda/2018/22-0

set out in domestic and international laws. As discussed the analysis in line with AfDec and other instruments, the current data protection and privacy framework conforms, to a large extent with the provisions on privacy and data protection as contained in international instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the General Data Protection Regulation.

## Conclusion and recommendations

### Conclusions

The enactment of the Data Protection and Privacy Act, 2019 in Uganda marked a milestone in the protection of privacy rights. Additionally, the publication of the draft Data Protection and Privacy Regulations, 2020 in August 2020, which specify the procedural aspects for effective implementation of the act, was yet another step in the right direction.

As discussed earlier, the act is progressive and comes at a time when government and other private entities are engaged in massive collection and processing of personal data. The law also ticks most of the boxes of international human rights instruments on privacy and data protection, such as the UDHR and ICCPR. However, the act however falls short of the human rights-based approach, specifically on participation as there was limited participation in terms of wider consultations. The law is also yet to be translated and widely disseminated.

There are also some concerns on the independence of the personal data protection office, which was yet to be set up, at the time of writing this report. The draft data protection and privacy regulations do not provide for independent financing of the office.

Additionally, despite the existence of the constitutional provision on the right to privacy, and now the act, these have not yet been translated into local languages nor widely disseminated for access by the wider public, thus limiting the ability of the rights holder from demanding respect for their right to privacy and data protection.

## Recommendations

- The government should expedite the passage of the Data Protection and Privacy Regulations (2020) and ensure that there is wider and meaningful consultation of all stakeholders, especially among the marginalised and most vulnerable groups.
- The government should also expedite the establishment of the Data Protection Office including financial independence from the National Information and Technology Authority
- It is necessary to translate into local languages and widely disseminate the act and regulations to reach the wider population in Uganda.
- Civil society and media should continue to monitor, document and report data protection and privacy breaches especially during this election season, when telecom companies regularly share personal data with political aspirants.