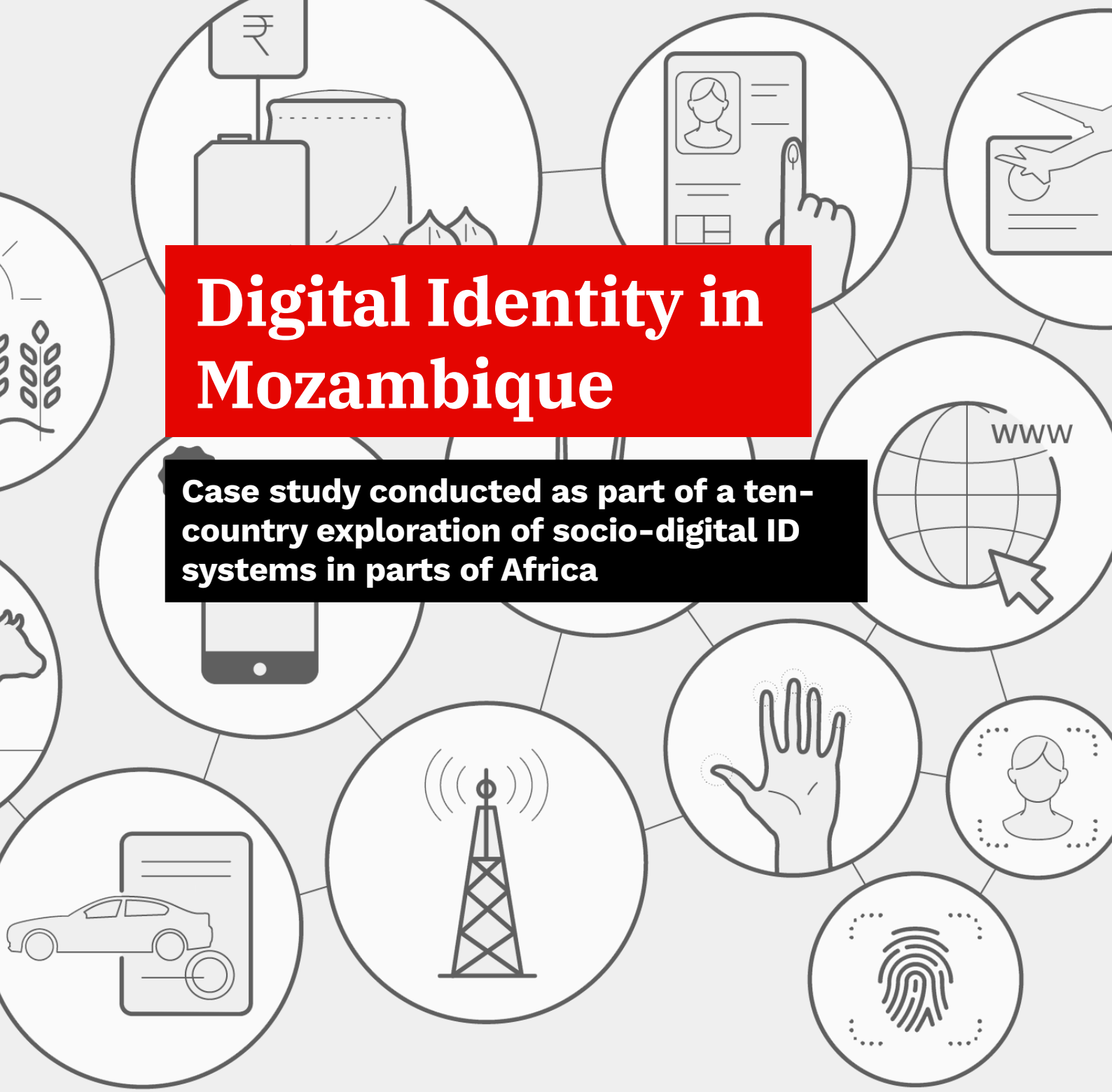

Digital Identity in Mozambique

Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa

RESEARCH & WRITING
Polly Gaster & Iazalde Martins

REVIEW & EDITING
Anri van der Spuy, Vrinda Bhandari, Shruti Trikanad & Yesha Tshering Paul

COPYEDITING
Samantha Perry

COVER ILLUSTRATION
Akash Sheshadri

LAYOUT
Aparna Chivukula

RESEARCH ICT AFRICA

THE CENTRE FOR internet & SOCIETY

OMIDYAR NETWORK™

Digital Identity in Mozambique

Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa

A project of the Centre for Internet and Society (CIS), and Research ICT Africa (RIA)

→ digitalid.design ←
→ cis-india.org ←
→ researchictafrica.net ←

Digital Identity in Mozambique

By Polly Gaster & Iazalde Martins, CIUEM

PREAMBLE

With an estimated 500 million people in Africa living without any form of legal identification (birth certificate or national ID),[1] the use of digital forms of identification has become increasingly popular because of their relative ease, low cost, and convenience compared to more analogue systems.

The Covid-19 pandemic has, if anything, increased the appetite for digital identification platforms and technologies.[2] The African Union Commission is currently working on a continental initiative to develop an interoperability framework for digital ID. Among other policy instruments, this effort draws its mandate from the *Digital Transformation Strategy* (DTS) *for Africa (2020-2030)*, which emphasises the importance of digitised legal identification mechanisms on the continent. The DTS highlights both the potential social and economic implications of digital IDs for Africans, noting that digital IDs not only support social development, but also enable meaningful participation in productive processes to generate economic growth, spur innovation, and support entrepreneurship. Besides being viewed as an enabler for realising all these policy objectives, digital IDs are seen as critical for the successful implementation of the African Continental Free Trade Area (AfCFTA).

With the growing enthusiasm for digital ID in Africa and across the world, there is a need to examine their impact on human rights, the rule of law, and the people who will be included (and excluded) from related systems. More critical analyses of digital ID's impacts in the global South, as well as the actors involved in designing and implementing them, are needed because digital identity programmes create an inherent power imbalance between the State and its people. The collection of personal data leave residents with little ability to exert

1 ID4D global dataset, 2018. See: *https://datacatalog.worldbank.org/dataset/identification-development-global-dataset*

2 Martin, Schoemaker, Weitzberg & Cheesman, 2021.

agency in its collection, storage and use, particularly when their right to privacy is not safeguarded or their personal data protected. And while increasing access to legal identification might appear to be a positive development for countries, this is not unequivocally the case.

In addition to the very real challenges of living without legal identification – whether digitised or analogue – those who *do* have digital do have digital identity may face other challenges. Experiences depend on (historical) context,[3] with some digital identities being developed in an attempt to segregate or even coerce people, while others are designed under the guise of national security concerns. Some countries have IDs that are no longer fit for purpose in a digital age,[4] while digitisation can also introduce novel harms. These include not only the direct risks associated with the collection and storage of personal data but arguably greater harms of exclusion or discrimination. Unless active measures are taken to counter such harms far from improving lives and potentially livelihoods, the introduction of digital ID systems could exacerbate inequality when analogue options are discarded – especially in African contexts with low connectivity levels.

On the other hand, digital identity systems, like all ICTs, are actively designed and shaped and therefore not inevitably detrimental from a developmental, human rights, and/or inclusion perspective.[5] If digital identities are conceived and designed with human rights, developmental goals, sustainability, and safety at the forefront, they might have a more transformative impact for the continent.[6] Critically examining the design, development, and implementation of these evolving systems remains crucial therefore, along with whether policymakers are doing enough (from a governance perspective) to ensure the positive outcomes of engagement with these socio-digital systems, while mitigating the risks that accompany many digital identities on the continent.

The Project

With this background in mind, Research ICT Africa (RIA) and the Centre for Internet and Society (CIS) partnered in 2020 and 2021 to investigate, map and report on aspects related to the state of digital identity in ten countries in Africa. The project looked at local (and digitised, in full or partially) foundational ID

3 Breckenridge, 2014.

4 African Union Commission, 2021.

5 e.g., Lievrouw, 2014; Parikka, 2012; Freedman, 2002; Wacjman, 2000; Williams, 1985.

6 c.f., Weitzberg, Cheesman, Martin, & Schoemaker, 2021.

systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe.

The research took place within parameters set by an Evaluation Framework for Digital Identities[7] (the 'Framework'), which was developed by CIS with the purpose of assessing the alignment of digital identity systems for compliance with international rights and data protection norms. (CIS initially developed the Framework with a view of using it to assess India's Aadhar system, but the Framework has since been used in other contexts too.)[8] By using this Framework, the ten country partners evaluated certain aspects of the existing governance and implementation mechanisms of digital identity in their respective and unique contexts.

The Framework introduces a series of questions against which digital identity may be tested, aiming to address the various rights and freedoms that are potentially impacted by the state use of a biometric digital identity program. More detail about the Framework can be found in Annex II.

This report on the Mozambique case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Polly Gaster & Iazalde Martins, CIUEM. Besides being an independent case study, the findings from this report were also used to inform a comparative report put together by the RIA and CIS teams to analyse the similarities, differences, and other aspects across the ten case studies – including key recommendations for policymakers, researchers, civil society actors, and other stakeholders.

An important limitation of the research is that the country case studies were conducted using the analytical lenses provided by the Framework, partly with the aim of assessing whether the Framework is relevant in African contexts, and might therefore not cover all aspects pertaining to digital identity in the context concerned. We elaborate on this limitation – which we feel significant in the contextually rich and diverse African context – in the comparative report.

PREAMBLE REFERENCES

African Union Commission (2021). *Draft AU Interoperability Framework for Digital ID* (August, 2021). [not published.]

Breckenridge, K. (2014). *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge: Cambridge University

7 *https://digitalid.design/evaluation-framework-02.html*

8 *https://digitalid.design/evaluation-framework-case-studies/estonia.html*, *https://digitalid.design/evaluation-framework-case-studies/kenya.html*

Press.

Freedman, D. (2002) *A 'Technological Idiot'? Raymond Williams and Communications Technology, Information, Communication & Society*, vol. 5(3): 425-442.

Lievrouw, L.A. (2014) "*Materiality and media in communication and technology studies: An unfinished project*." In: Gillespie, T., Boczkowski, P.J., Foot, K.A. (Eds.) (2014) Media technologies: Essays on communication, materiality and society. London: MIT Press.

Martin, A.; Schoemaker, E.; Weitzberg, K. & Cheesman, M. (2021) *Researching digital identity in time of crisis (workshop report).* London: The Alan Turing Institute. Available at: https://www.turing.ac.uk/sites/default/files/2021-08/3c_workshop_reporttimes_of_crisis_.pdf

Parikka, J. (2012) *New Materialism as Media Theory: Medianatures and Dirty Matter, Communication and Critical/Cultural Studies, vol. 9*(1): 95-100.

Weitzberg, K.; Cheesman, M.; Martin, A. & Schoemaker, E. (2021) *Between surveillance and recognition: Rethinking digital identity in aid. Big Data & Society*, January-June: 1-7.

Williams, R. (1985) *Towards 2000*. Harmondsworth: Penguin.

ACKNOWLEDGEMENTS

This report was made possible by the support received from Omidyar Network. The Evaluation Framework referenced in this report was developed by the Centre for Internet and Society. The case study was conducted by Polly Gaster & Iazalde Martins with the support of Research ICT Africa (Anri van der Spuy and Naila Govan-Vassen) and the Centre for Internet and Society (Shruti Trikanad, Vrinda Bhandari and Yesha Tshering Paul). The RIA and CIS teams do not necessarily agree with the views expressed in this country case study. The authors thank the people who made their time and expertise available to contribute to and review this report.

ABSTRACT

This study assesses the current stage of implementation of initiatives related to digital identity in Mozambique. It forms part of the Research ICT Africa project, in partnership with the Centre for Internet and Society, to assess the stage of digital identity in Africa, through comparative studies from 10 countries.

The study was carried out based on the aspects addressed in the Evaluation Framework developed by the Centre for Internet and Society, which provides for the analysis of three distinct areas: rule of law tests, rights-based tests and risk-based tests. The methodology included a review of the existing bibliography in Mozambique related to the digital identification of citizens and other associated digital initiatives; interviews with relevant institutions and/or personalities who work or have worked in the area to understand both the current situation and the perspectives and challenges that lie ahead; and the application of the evaluation framework.

During the research, it was found that although existing legislation includes references to a national integrated digital identification system, in practice different sectors have moved ahead with independent digital systems to meet sectoral needs, and there is limited coordination between them. For example, separate systems exist for the registration of births, the issuing of adult identity cards, the issuing of passports and social security. Of the researched software, the Electronic System of Civil Registration and Vital Statistics was selected for the purposes of this study as it is a system that is already in operation at national level and which is intended to be the starting point for a future foundational system of digital identity in Mozambique.

The Electronic System of Civil Registration and Vital Statistics is implemented by the Ministry of Justice, Constitutional and Religious Affairs through the National Directorate of Registries and Notaries and aims to register all the facts that form part of citizens' lives, with emphasis on the issue of birth and death certificates. Other aspects are still to be added as the system develops.

The study takes into account the Mozambican social, demographic and geographic context, which offers many challenges to the nationwide implementation of digital systems. A challenge of particular interest is physical internet access and the respective costs, as 65% of the population lives and works in rural areas.

These findings mean that when responding to the questions raised by the Evaluation Framework, the study is not analysing a single foundational system that is already in place, but uses the aims and functioning of the Electronic System of Civil Registration and Vital Statistics as its basis. It has therefore not been possible to provide a full response to questions that are predicated on the current existence of a foundational system.

The conclusions and recommendations thus focus on the steps that need to be taken to ensure the establishment of a functional digital ID system in the context of Mozambique's reality and perspective, and in accordance with the study's findings concerning legislation, regulation and policy.

ACRONYMS AND ABBREVIATIONS

API	Application Programming Interface
CIA	Centre for Internet and Society
DIC	Directorate of Civil Identity
DNRN	National Directorate of Registry and Notaries `
e-SIRCEV	Electronic System for Civil Registration and Vital Statistics
GovNet	Government Electronic Network
ICT	Information and Communication Technologies
ID	Identity Cards
INAGE	National e-Government Institute
INCM	Mozambique National Communications Institute
INE	National Statistics Institute
INTIC	National ICT Institute
MCTES	Ministry for Science, Technology and Higher Education
MINT	Ministry of Home Affairs
MJACR	Ministry of Justice, Constitutional and Religious Affairs
MTC	Ministry of Transport and Communications
NUIC	Unique Citizen Identification Number
RIA	Research ICT Africa
SENAMI	National Immigration Service
SMS	Short Message Service
USSD	Unstructured Supplementary Service Data

CONTENTS

INTRODUCTION

Population identification in Mozambique began in colonial times, when national citizens were separated from colonisers, being classified as an indigenous population. After World War II, an additional category was introduced, that of the "assimilated" population, which was supposed to cover the few national citizens who had access to education, among other requirements (Mondlane, 1969). After independence in 1975, Mozambique progressively developed its own legislation and regulations in all sectors, including that of civil identification.

Mozambique is a long, narrow country, with an Indian Ocean coastline of 799 830 km. It has land borders with six countries: Tanzania, Malawi, Zambia, Zimbabwe, South Africa and Eswatini. The estimated population in 2021 is 30, 832 244 people, with a GDP per capita of USD 522 in 2019.[9] Data from 2014 shows that 65% of the population were living in rural areas, that nearly 52% were women and 56% were 0-19 years old. The illiteracy rate had fallen from 50.7% in 2007 to 39% by 2017, with an illiteracy rate split of 67.7% female and 32.3% male.[10] The average population density was 30,2 per square kilometre.[11]

This data helps show the challenges involved in establishing nationwide digital systems that reach every corner of the country and every citizen; a context which is not helped by Mozambique suffering from armed conflicts and the drastic effects of climate change.

Following independence in 1975, the manual systems for citizen registration and the issuing of identity cards for civil identification were split between the Ministry of Justice and the Ministry of Home Affairs (MINT) respectively.[12] Later on, with the increasing importance of information and communication technologies (ICT), a new Ministry of Science, Technology and Higher Education (MCTES) was created in 2005 to lead and coordinate the ICT sector. It was later renamed the Ministry of Science and Technology, before reverting to the original name. Since then, these three different Ministries have been directly involved in different aspects and components of digital identification systems.

In 1990, Mozambique changed its constitutional format to a country based on the democratic rule of law, the separation of powers and political pluralism.

9 *www.ine.gov.mz* – home page. Accessed 29/4/2021 9

10 *Mulheres e Homens, Instituto Nacional de Estatística, Moçambique, 2018*. Accessed at *www.ine.gov.mz*, 09/06/2021

11 *Moçambique em Números 2014, Instituto Nacional de Estatística, Moçambique, 2014*. Accessed at *www.ine.gov.mz*, 29/4/2021.

12 Interview with Dr Sérgio Cambaza, Head of the Department of Registry and Notary Information Systems,14/04/2021

The new Constitution of the Republic included, and subsequent revisions retained, an article on the Use of Informatics, which forbids the recording and use of individually identifiable data regarding political, philosophical, religious or ideological convictions. It also enforces the protection of personal data contained in computer records, including the transfer of files between services and institutions. Exceptions can only be made in accordance with the law or by judicial decisions.[13]

Recognition of the importance of these issues at a time when the IT sector hardly existed in either the public or private sectors of Mozambique, means that all subsequent legislation and decisions have been legally required to take the Constitutional provisions into account. This exhibits the Government of Mozambique's far-sightedness.

The study's findings are based on a wide-ranging literature review, focusing in particular on existing legislation, regulations, strategy and policy documents, as well as interviews with key actors linked to the MCTES and its subordinated institutions and the Ministry of Justice, Constitutional and Religious Affairs (MJACR).

1.1 THE EVOLUTION TOWARDS DIGITAL ID SYSTEMS AND GOVERNANCE

Mozambique does not yet have a fully integrated foundational digital identity (digital ID) system, nor does it have legislation on the protection of personal data. However, several separate initiatives have been undertaken by some governmental bodies with a view to furthering this objective, as it is a national necessity.

The starting point for Mozambique's digital ID approach was the strategic decision to create a unique attribute for the identification of Mozambican citizens, to be used by the various public and private institutions in the management of information, the issue of citizens' documents, and the facilitation of access to services. In 2010, Decree 44/2010 (November 2) was approved by the Council of Ministers. It defined the procedures for creating and using the Unique Citizen Identification Number (NUIC),[14] managing the database of national and foreign citizens and gave implementation responsibilities to the three key ministries, namely Science and Technology, Justice and Home Affairs.

These three ministries and their respective subordinated institutions and regulators have each had different roles in legislating, regulating

13 *Constituição da República*, Art 71 - 3

14 Currently the NUIC is being used by the e-SIRCEV system to record information relating to births and deaths.

and implementing activities related to digital ID. This situation persists, notwithstanding some changes of name and competencies in the respective ministries, and the additional involvement of the Ministry of Transport and Communications (MTC), which supervises the telecommunications regulator, the Mozambique National Communications Institute (INCM).

Currently, the MCTES has in its portfolio the National E-Government Institute (INAGE) and the National ICT Institute (INTIC), which is the ICT regulatory authority. INTIC and INAGE are not fully independent, considering that their leadership and senior posts are appointed by the supervising ministry and that their status is that of a governmental body.

INAGE is a public institution endowed with legal personality and administrative autonomy, with the responsibility to ensure the planning, implementation, coordination and management of the Government Electronic Network (GovNet), as well as ensuring the security and confidentiality of the information stored. It is also responsible for e–government services in general, and in that context drafted, implemented and still manages the Decree on Interoperability,[15] with the explicit objective of establishing conditions for implementation of the NUIC. An earlier attempt at launching a national system of digital ID did not reach the operational stage due to its complexity and coordination difficulties, and INAGE is currently preparing to test a new system.[16]

INTIC is a public institution endowed with legal personality and administrative autonomy, with the responsibility of providing technical support to state bodies and institutions, coordinating activities carried out in the field of ICT aimed at improving the provision of public services and governance. It also exercises the role of regulatory authority for ICT, in coordination with the National Institute of Communications of Mozambique (INCM).[17]

As the ICT regulator, INTIC will provide technical advice and take the necessary measures to ensure the effective interoperability of the subsystems involved in the process of civil registration and identification of citizens using NUIC, in coordination with INAGE.

The MINT has in its portfolio the Directorate of Civil Identity (DIC), which issues

15 Decree 61/2017 of December 1

16 Interview with Eng. Sergio Mapsanghane, INAGE, 23 March 2021

17 Decree 9/2011 of May 4

identity cards,[18] and the National Immigration Service (SENAMI), which issues passports, travel documents, residence permits for non-nationals, and the like.

The MTC has in its portfolio the National Communications Institute (INCM), which is the regulatory authority for telecommunications. The INCM regulates and supervises the communications sector and the management of the radio frequency spectrum.[19] In 2020, INCM ordered that all mobile phone users should register their SIM cards to guarantee the security and accountability of users in case of criminal use.

Finally, the MJACR has in its portfolio the National Directorate of Registry and Notary (DNRN), which oversees the implementation of the Electronic System for Civil Registration and Vital Statistics (e-SIRCEV) system, which tracks births and deaths in Mozambique. In the future, the system will also register other information relating to citizens such as marriage, divorce and parentage.

The Civil Registry Code (Law 12/2004 of December 8) was first approved in 2004, with a view to the mandatory registration of citizens in terms of birth, marriage, death and related data. This law was revised in 2018 (Law 12/2018 of December 4) to simplify and modernise registration acts through the introduction of e-SIRCEV.

Other instruments have also been developed that are related to issues of digital identification, the most relevant of which are:

1. Electronic Transactions Law (Law 3/2017 of January 9), which establishes the rules and legal framework for electronic commerce and electronic government, including issues of data protection,[20] privacy, security and others. It is implemented by INTIC, and some of the necessary complementary regulations have recently been approved by decree;
2. A draft proposal for a National Cybersecurity Strategy and Policy prepared by INTIC with support from the INCM, which covers the technicalities of providing data security,[21] which is still to be approved; and
3. Decree 67/2017 (December 1) Regulation on Interoperability, in which INAGE is responsible for implementing issues of interoperability among

18 The Mozambican ID card is a physical laminated card with a microchip that contains an ID number, photograph, full name, gender, date of birth, nationality, address, biometrics (fingerprints), place and date of issue, height, occupation, marital status, parents' names, expiration date, and signature of the owner.

19 Decree 32/2001 of November 6

20 A draft proposal of the Data Protection Law is in preparation by INTIC. It should cover the limits of the mandates of each relevant actor in this area

21 Interview with Eng. Sérgio Guivala from INTIC, 16 April 2021; PSC-INTIC *Draft-Final 8.03.2021_01_V1 (1) _harmonizada com ENSC*

public institutions and rules for protecting citizens´ rights and data security.

Over the past decade, each of the key sectors has developed their own discrete digital systems for registering identities and issuing birth certificates, ID cards or passports. Each system stands alone, though there are some data exchanged between the National Directorate of Registries and Notaries and the National Directorate of Civil Identification. The regulations and complementary activities form a patchwork of initiatives supervised by different entities, mostly approved and published by government decree rather than a law. However, inter-ministerial coordination and working groups have been established, seemingly with a view to redefining and implementing a national NUIC strategy.

1.2 AN EMBRYONIC FOUNDATIONAL SYSTEM

The e-SIRCEV was created in 2018 as a foundational system through Law 12/2018. It defines a set of processes through which the registration of all basic information related to citizens´ civil registration, such as birth, marriage, divorce and death, and other details such as name changes, place of residence, and the like, are carried out. Its design was based on a system used in Uganda. The e-SIRCEV aims to create a database that allows the efficient collection of statistical information and interoperability with other government systems through the allocation of the Unique Citizen Identification Number (NUIC) at birth, using ICTs.[22]

The e-SIRCEV works throughout the national territory integrated in the National Directorate of Registries and Notaries and has two implementation units, provincial directorates and civil registry offices. Provincial directorates oversee the justice area with coordination and implementation functions in each province, and civil registry offices look after the executive and administrative function of registration operations.[23]

The e-SIRCEV was officially launched in March 2019, and has been implemented in 121 of the 164 registries in Mozambique.[24] Its digital activities are underway, but still limited, with the first priority being the digital registration of births and deaths and the sharing of vital statistics with the National Statistics Institute (INE). All death certificates contain a code associated with the cause of death.

22 Law 12/2018 of December 4, Article 1

23 Law 12/2018 of December 4, Article 2

24 Presentation *Missão Diagnóstico ID4D - Resultados preliminares*, December 2019

For example, if someone died from COVID-19, this information will be registered through the allocation of a specific code. At the local level, e-SIRCEV coordinates with health centres and hospitals integrated into the Ministry of Health's database system, and incorporates the data provided.

Although e-SIRCEV is not a fully integrated ID system, we selected it for further study as it is expected to remain at the heart of a future national ID system.[25] It will be key to establishing and implementing the NUIC and/or the creation of new implementation bodies. As the system does not yet correspond to the definition of a foundational digital ID system, it cannot provide answers to all the indicators contained in the evaluation framework. However, at the same time, this makes it an important object of study, as the results of this report may feed into the future development of a full digital ID system. Some other existing laws and regulations provide at least partial information about the areas of interest. They also enable a more complete picture of which way government thinking and planning may be moving, and of existing gaps, so reference to them is included where relevant.

It is still very early to identify successes and failures of the system *per se*, and the main priority is to expand its reach at national level. From 2019 to date, 700,000 NUICs have been issued[26] during the registration of births.

Existing challenges with regard to the registration of births and issue of certificates with or without the digital system include the fact that not all citizens are registered even manually. This is due to distance from the registries but also due to population movements, displacement of households, and the loss of documentation during natural disasters. Statistics can also be affected by the way names are spelled differently at different times by the citizens themselves, or due to errors made by officials doing the registration.

Detailed research will also be required to assess important questions such as observance of existing rules and regulations at local level, awareness of citizens' rights on the part of both citizens and officials, the quality of information, etc. While coordination with interested parties, such as health authorities and the National Statistics Institute, is improving, it is not yet taking place within a common system. It is clear that coordination between the various national actors and overlaps in responsibilities constitute a major challenge. As stated above, the e-SIRCEV system is intended to be the starting point for digital ID, but it is still limited in its functions and decisions about the architecture and technical specifications of a foundational system are still unresolved.

25 Through the e-SIRCEV system, all the attributes necessary for issuing birth certificates (name, date of birth, address, parents' names, etc.) and death certificates (date and time of death, name, cause of death, etc.) are collected

26 Interview with Dr Rufaro Cashanje, IT, at the first civil registry office, 11 May 2021

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The Civil Registry Code in Mozambique, which lays the foundation for e-SIRCEV, is approved by a validly enacted law (Law 12/2018 of December 4) passed by the legislative power (the Parliament of Mozambique - Assembleia da República de Moçambique). The law does not allow excessive delegation to the executive.

The law was published in the contained in the law is clear and understandable, however not all of the language used would be easily understood by the average citizen, especially in rural areas. Almost half of the Mozambican population is illiterate, contributing to the lack of awareness of existing legislation and their civil rights and duties. Another barrier is that the Code is extremely dense, with 387 Articles detailing every step and every process. Having said that, the detail is necessary.

The Code is clear that it was created for the issuing, in digital format, of birth certificates, including the attribution of NUICs, marriage certificates and death registrations of citizens, among other documents.

Since the start of the digitisation process in 2019, existing citizen records in physical format are being digitised individually by each registry office across the country.[27] According to Law 3/2017, citizens can request offline access to their own information from the data controller[28] for the purpose of alteration, rectification or removal.[29] If the controller does not provide the information requested, he or she must justify the decision according to the law.

QUALITY OF LAW

The Code lays down concrete procedures in factual detail without delegating procedures to other institutions and defines procedures for appeals and sanctions

27 Law 12/2018 of December 4, Article 18

28 The role of data controller is not defined in Law 3/2017 nor in the glossary of the Law but there is a definition of data processor that looks similar to the data controller, which states that it represents "*any public or private person, natural or legal, who requests, collects, processes or electronically stores personal information from or about a data subject*". We have not been able to clarify the tasks of the data controller.

29 Law 3/2017 of January 9: Electronic Transaction Law, Articles 63 to 66

dealt with internally or by courts. It also defines the civil responsibility of civil servants.[30] In terms of the evaluation framework, the Code contains the three main components of validation (legality, quality of law, clarity and precision of law) and does not amount to excessive delegation to the executive power.

CLARITY AND PRECISION OF LAW

Law 12/2018 is accessible to all citizens in Mozambique in digital format and hardcopy, generally free of charge although in some cases they will be required to pay a nominal amount. The language used in the law is clear and easily understood by the average citizen, but it may be a challenge to the large illiterate population, especially those living in rural areas. In these cases, the Code provides mechanisms for clarifying the information to be provided by officials of the registration and notary directorates.[31]

2.2 LEGITIMATE AIM

Does the law have a legitimate aim? Does the law clearly define the purposes for which the ID can be used?

The aim of the Civil Registry Code is legitimate. It intends to modernise the registration and conservation of the basic facts of citizens´ lives such as births, parentage, marriage, divorce, death, and to implement a digital system that will improve the collection of vital statistics and lead to the full implementation of the NUIC.

The revision of the Code was made primarily to simplify and modernise registration acts by introducing the e-SIRCEV, and to introduce the NUIC, assigned at birth and valid until death, that will eventually incorporate all the documents (such as identity card, passport, driver's license, etc.) of every Mozambican citizen during their life.

Before the introduction of the e-SIRCEV through Law 12/2018, facts related to citizens were registered manually by conservatories in their books stored on shelves. For the issuance of a document or alteration of some aspect of the citizen's information, it was necessary to physically search for this information in the books available according to the year of registration of the citizen. This process was slow and complex. With the introduction of the new system, the process of obtaining documents through the conservatories will become more flexible and it will be possible to integrate with other governmental services.

30 Law 12/2018 of December 4, Article 373

31 Law 12/2018 of December 4, Article 49

2.3 DEFINING ACTORS AND PURPOSE

Does the law governing digital ID clearly define all the actors that can use/manage or are connected to the ID database in any way?

The e-SIRCEV operates throughout the national territory, integrated in the National Directorate of Registries and Notaries and has the following implementation units: provincial directorates that superintend the area of Justice, with coordination and implementation functions in each province and Civil Registry Offices, with the executive and administrator function of registration operations.

In the e-SIRCEV system, all the facts subject to civil registry are registered, aiming at the creation of the citizens ´ database that allows the efficient collection of statistical information and interoperability with other governmental systems. Apart from the institutions described in the Code that have access to this information, other governmental institutions (ministries and other governmental bodies) can access and use the database according to the defined interoperability framework (still to be implemented). The type of access and the information requested and used is not clearly stated in the Code.

According to Decree 67/2017, applying the principle of interoperability "public administration entities are obliged to share the data in their possession and to reuse the data available or collected by other State entities, except in the cases established in specific legislation".[32] However, this decree is yet to be fully implemented.

Is the use of the ID system by private actors adequately regulated? Are private actors held to the same level of accountability?

The e-SIRCEV system is not currently used or accessed by private actors. It is only used by the National Directorate of Registries and Notaries and its implementation units, and cannot be accessed by private actors. During its implementation, integration with other government and private systems is envisaged through use of the NUIC. This integration will have to be enabled by new legislation or regulations produced by the competent bodies, in particular the regulators, such as the INTIC INAGE and the respective ministries.

According to Decree 67/2017, the private sector may have access to data

32 Decree 67/2017 of December 1, Article 11

shared by public administration bodies when they are contracted to develop technological solutions and information systems to provide public services using systems of electronic government. This has to happen in compliance with the provisions of this decree and/or according to specific procedures to be adopted by INTIC.[33] The specific procedures to be adopted by private actors are not clarified but they should have different access to the information as the public administrations have to safeguard the rights of citizens, respecting the confidentiality of information.

According to the principle of interoperability "public administration must collect the citizen's data only once, without prejudice to what is established in the specific legislation, making them available for the use of other public entities, in the pursuit of e-government services. The data already made available by the citizen must be reused by the public administration entities in accordance with the framework and the interoperability platform".[34]

The interoperability framework does not describe the purpose of enabling information sharing between public administration entities, but establishes that they must pursue the public interest without prejudice to the rights and interests of individuals protected by law.[35]

Does the law clearly define the nature of data that will be collected?

The e-SIRCEV system defines a set of foundational data that will be collected for all citizens in the process of issuance of different documents.

The system requires all the necessary data to be provided by the citizens, without reservation.[36] For every document requested, a list of necessary information is required from the citizen. For instance, when issuing a birth certificate, the citizen is asked to provide date and time of birth, place of birth (province, district, health unit), type of delivery, gender, weight, height, name and parents' information (name, age, marital status, nationality, occupation, academic level, residence, contact and NUIC if it has been assigned).

33 Decree 67/2017 of December 1, Article 3 - 3

34 Decree 67/2017 of December 1, Article 12

35 Decree 67/2017 of December 1, Article 7

36 Law 12/2018 of December 4, Article 127

Does the ID system provide adequate user notification mechanisms?

The system does not notify the citizen if his or her data is used by public or private institutions, though it does inform them about the status of their registration requests, via text messages (SMS), e-mails and other electronic means.[37] However, it is not clear how well this system is functioning, and it is only available to citizens who have access to mobile phones and/or the internet. Current statistics indicate that 65% of the population have access to a mobile phone and only 18% have access to the internet.[38]

The Code determines that notifications generated by the e-SIRCEV system include information about the digitised data related to births and deaths that occur in the health units and communities, and the attribution of a NUIC, even if the registered person does not yet have a name. The reported data is used to complete the records and to feed statistical and health information.[39]

The notifications generated on the e-SIRCEV system are produced by civil servants working in the registry, health care workers, administrative entities and other administrative authorities and others duly accredited by the National Director of Registries and Notaries.[40] These accredited personnel collect the information in the health units across the country using the e-SIRCEV system.

With this information, the MJACR and Minister of Health can segregate different types of information, for example, know the number of births or deaths from a health unit, a district, or province. It is also possible to garner periodical global statistics about births and deaths, including the cause of death.

Do individuals have rights to access, confirmation, correction and opt out?

Citizens and foreign nationals have the right to obtain all information about themselves from the data controller. They also have the option of rectifying, completing or changing the information registered. Individuals do not, however, have the right to opt out of the system, it is obligatory.[41]

The physical documentation of citizens' data will be kept in the respective

37 Law 12/2018, Article 18B - 4

38 *http://hootsuite.com/resources/digital-in-2018-emea*, accessed 31/05/2021

39 Law 12/2018 of December 4, Article 18B – 1 e 2

40 Law 12/2018 of December 4, Article 18B – 3

41 Law 12/2018, Article 1A

registry to allow national citizens and foreign citizens to review them to give their consent to electronic registration. This documentation must remain unchanged, serving as a means of proof in case of contradiction of the electronic record. If the information presented is not accurate, a new record will be issued since the information is manually written in the conservatory books.[42] Following the issue of a document by the e-SIRCEV system, the recipient has up to three months to request the registry to change his or her information free of charge. Requests for changes outside the defined period incur additional costs.[43]

As explained above, at this time the private sector does not have access to the system, and cannot access citizens' records.

2.4 REDRESSAL MECHANISMS

Are there adequate civil and criminal redress mechanisms in place to deal with violations of their rights arising from the use of digital ID?

The Code does not prescribe any avenues for redress in the case of violations or abuse of the law. However, Article 68 of the Electronic Transactions Law defines types of misuse and penalties for the misuse of information in the citizens' database by civil servants, with various fines or the application of a more severe penalty under criminal law.

The Law 3/2017 establishes the principles, general rules and the legal regime for Electronic Transactions in general, and e-commerce and e-government in particular, aiming to guarantee the protection and use of ICT. The e-SIRCEV system may be considered an e-government system since it deals with citizens' data and is used by a governmental body, therefore the provisions of Article 68 are applicable. This Article details all the criminal sanctions for illegal access, illegal interception, data interference resulting in damage or elimination or alteration, misuse of ICT equipment[44] and others. This shows the need for unifying legislation and regulations, as few ordinary citizens having a problem with the use of their data in the e-SIRCEV system would think of looking for information in a different law, or would have the means to search or access such a law.

Different aspects of digital ID in Mozambique are scattered across various existing legislation. In the process of creating a national foundational system, it is

42 Law 12/2018 of December 4, Article 5

43 Interview with Dr Rufaro Cashanje, IT at the first civil registry office,11/05/2021

44 Law 3/2017 of January 9, Article 67

important that there is a single law that includes all the necessary aspects for the creation and implementation of a national digital ID system.

2.5 ACCOUNTABILITY

Is there an independent and adequate regulatory mechanism to ensure accountability of the administrator of the digital ID?

There is no regulatory mechanism: the system is supervised by the National Directorate of Registries and Notaries (NDRN) under supervision of the MJACR. The Civil Register Code does not mention independent or watchdog bodies.

Public or private institutions are not allowed to access files, computer or database records for gathering information about personal data related to third parties, nor to transfer personal data from one to another computer file belonging to different services or institutions, except in cases arising from a legal diploma[45] or a judicial decision. The Civil Registry Code requires respect for personal and family privacy. The only body above the National Directorate is the ministry and there is no regulatory body for this sector, independent or otherwise, though there is an Ombudsman with no mandatory powers.

According to the principle of interoperability, public administration must collect a citizen's data only once, without prejudice to what is established in the specific legislation, making it available for the use of other public entities, in the pursuit of e-government services. The data already made available by the citizen must be reused by the public administration entities in accordance with the framework and the interoperability platform. This point on interoperability creates serious doubts about safeguards for citizens' data since any public administration body can share information in its possession.

To address the lack of coordination between different institutions regarding digital identity, INAGE is in the process of creating and formalising a Technical Council that will bring together all interested parties, such as the MCTES, MINT, MCT and their subordinate bodies.[46]

To safeguard the digital rights of citizens in the use of ICT, civil society organisations, as well as private and academic organisations were consulted and involved in the preparation of some legislation, with emphasis on the National Cybersecurity Policy and Strategy.[47]

45 A legal diploma is a document that officially indicates a title, power, privilege or capacity of one or more individuals.

46 Interview with Eng. Sérgio Mapsanghane, INAGE, 23 March 2021

47 Interview with Ernesto Saul, MISA, 15 March2021

2.6 MISSION CREEP

Does the governing law explicitly specify the proposed purposes of the digital ID?

The e-SIRCEV System does not explicitly cover the needs of a fully integrated digital ID system. It instead explicitly specifies the purpose of the Civil Registry Code.

The e-SIRCEV system is a starting point for a future national digital ID system. The clear definitions of its ambit of action would make it easy to detect signs of mission creep and contest them under established law. However, applying the interoperability framework creates serious doubts about safeguards for citizens' data, since any public administration bodies can share information in their possession.

In terms of the purpose of its creation and functionalities, the system has a legitimate goal to register and store the basic facts of citizen's lives such as birth, parentage, marriage, divorce, death, and others, as well as implementing a system that will improve the collection of vital statistics.[48] It is suitable for the purpose of its creation, namely the need to create a system aiming at giving notice of births, deaths and other vital events by electronic means. This law is foundational, since it deals with citizens' information at national level and citizens are obligated to register to have access to other services provided by the state.

Mozambique does not yet have a data protection law, though a draft is in preparation. The data protection law is expected to cover the limits of the mandates of each actor and therefore reduce the possibilities for mission creep.[49] This law should clearly define the role of the different actors involved in digital ID and safeguard the interest of citizens regarding the use of their personal data. The law must also create sanctioning mechanisms in case of misuse of stored citizens' information and access control measures.

Another problem resides in the excess of information collected for issuing documents. Some of the collected attributes are not present in the final document and the purpose of further use is not explicit in the code.

48 Law 12/2018 of December 4, Article 2

49 Interview with Eng. Sérgio Guivala, INTIC, 16 April 2021

RIGHTS-BASED TESTS

3.1 NECESSITY AND PROPORTIONALITY

Are the privacy violations arising from the use of digital ID necessary and proportionate to achieve the legitimate aim?

The collection and use of data defined in Article 1 of the Civil Registry Code specifies the steps in a citizen´s life that require registration, primarily: birth, parentage, adoption, marriage, other changes in status, attaining adulthood and death. The data would not necessarily all be included in a fully integrated ID system, but this is not yet discussed or defined.

The Civil Registry Code states that when issuing a document such as birth certificate, marriage certificate or death certificate, the citizen needs to provide all the required information for the documents. These details are stored on the e-SIRCEV database and can be used by other systems in MJACR or other governmental institutions. This follows from, the interoperability framework in Decree 67/2017 Article 11, stating that "Public Administration entities are required to share the data in their possession and to reuse the available data or collected by other State entities". However, the Code does not define how the interoperability with other public and private systems will work, nor the type of information these systems will require. The sharing of citizen information may violate their privacy since public administration entities are obligated to share data in their possession in pursuit of state activities.

At the moment, the e-SIRCEV is linked to the database of the Ministry of Health through an application programming interface (API) used to integrate different systems, to provide statistical data of births and deaths.

3.2 DATA MINIMISATION

Are principles of data minimisation followed in the collection, use, and retention of personal data?

When using the e-SIRCEV system, large amounts of information, such as name, address, gender, date of birth, parents' names and NUIC are collected, used and stored to register birth, deaths and other vital information as defined in the Code. Much of this information may remain unused and does not appear in the documents.

The minimisation of information collected when issuing different documents using the e-SIRCEV system is not observed. According to the Code, all necessary information is collected even if it is not included in the final documents. It is also not clear in the Code what the purpose is of some information collected, such as the academic level of the child's parents, in the act of issuing birth certificates.

This information, once collected, may be shared and used on other public or private systems according to the interoperability framework, and there is no clear definition of the purpose of uses that differ from the initial purpose for which it was collected. This raises questions regarding the privacy of citizens, as they are not aware of any subsequent use of their information.

3.3 ACCESS CONTROL

Are there protections in place to limit access to the digital trail of personally identifiable information created through the use of digital ID by both state and private actors?

The Civil Registry Code was designed to be used by the National Directorate of Registries and Notaries and limits access to the citizen database by private institutions. Public institutions will be able to access the information when the interoperability framework is implemented.

There is no clear legislation that deals with protections related to digital ID. However, there are some definitions in Decree 67/2017 (December 1) that regulate the interoperability framework, but which are still to be implemented by INTIC and INAGE.

The Constitution of the Republic of Mozambique provides that no public or private institutions are allowed to access files, computer records or databases for knowledge of personal data relating to third parties, nor to transfer personal data from one to another computer file belonging to different services or institutions, except in cases established by law or by court decision.[50]

In accordance with the principle of interoperability, public administration data must comply with the law and cannot be used to pursue purposes other than those assigned.[51] The e-government must ensure the integrity of the data

50 *Constituição da República*, Article 71 to 73

51 Decree 67/2017 of December 1, Article 5

and that it cannot be altered, unless by persons authorised by law.[52] The public administration must collect citizens' data only once, without prejudice to what is established in the specific legislation, making it available for the use of other public entities, in the pursuit of e-government services.

Biometric information is not yet in use for ID purposes, though digital fingerprinting is part of the process for receiving an ID card issued by the Ministry of Home Affairs.[53]

3.4 EXCLUSIONS

Are there adequate mechanisms to ensure that the adoption of digital ID does not lead to exclusion or restriction of access to entitlements or services?

There are no concrete mechanisms to prevent exclusion. At the moment, the main objective is to increase the percentage of births and deaths that are legally registered, either manually or digitally. The country is not yet adequately provided with digital points of access, so manual registrations will continue for some time to come, particularly in rural areas. The issue of digital access to other public services has not yet arisen, but digital access will be a major challenge to implement universally, considering Mozambique's geographic and socio-economic context, as outlined in the Introduction.

In addition, the lack of electricity in remote areas alone will be a constraint in terms of guaranteeing digital access, while system failures or power cuts are not uncommon, especially in the rainy season. This probably means that there will be some ongoing system of parallel registration, and also means that the public services will not be able to abandon their existing manual systems to ensure they can comply with the Constitutional injunction to guarantee access to records. This means that the physical records kept manually will continue to exist, since this information is kept in the respective conservatory, unchanged, and serves as evidence of a citizen´s status.[54] To overcome these restrictions, the e-SIRCEV system has introduced the possibility of access without internet access, using USSD,[55] thus making it possible to collect information offline. After connecting to the internet, the data is updated.[56]

52 Decree 67/2017 of December 1, Article 8

53 Decree 11/2008 of April 29, Article 1

54 Law 12/2018 of December 4, Article 5

55 Unstructured Supplementary Service Data (USSD), for instance *123#

56 Interview with Dr Rufaro Cashanje, IT at the first civil registry office,11/05/2021

At this stage there are no severe consequences arising from being excluded from a digital ID system, because the interoperable system does not yet exist. Therefore, there is theoretical equality of access – all citizens currently need to register in different systems, for birth certificates (which now come with a NUIC) and register separately for an ID card for identification purposes. However, if these documents are lost, the voter cards issued at election time, and cards confirming a tax number, are also generally accepted, though people who work in the large informal sector do not generally want or need tax numbers.

However, it is clear that citizens who live in remote areas are more at risk of exclusion than others, as they have to travel further, and possibly a number of times, to complete the registration, and thus, bear higher costs. Costs, though they are nominal, can also be a problem for the urban poor. Another recurring difficulty that results in exclusion of various kinds is that of citizens having to abandon their homes in a hurry due to cyclones, armed conflict and other problems. During such times, they often lose their documents and identity cards as well as their other belongings. This problem is partially resolved by the work of mobile brigades that can issue new digital ID cards on the spot.

As a result of natural disasters, armed conflicts or other problems that affect, physical information stored in public institutions such as registries can be lost or destroyed. This is a very serious problem, but the introduction of e-SIRCEV will assist the preservation of citizen information, as it is stored digitally. This type of emergency problem obviously prejudices citizens as well as the authorities, but cannot be called exclusion because the problem does not arise from a decision or act on the part of the authorities.

3.5 MANDATORY USE

In case enrolment and use of digital ID are made mandatory, are there any valid legal grounds for doing so?

Civil registration is mandatory, fixed by law in the Civil Registry Code. As already stated, however, there is not yet a complete law on the use of a digital ID, and the question has not yet arisen. The first target is to define and implement the universal use of the NUIC.

When existing identity cards are used, such as the digital voter cards issued for voting in national and local elections, other options can normally be used. The Electoral Law also allows other forms of identification, including a driver's license or simply two witnesses.

Currently all the country´s physical records, except those from the provinces of Cabo Delgado and Sofala, are digitalised and can be accessed from any part of

the country, making it easier, fast and secure for the citizen to have the desired documents[57].

57 Interview with Dr Rufaro Cashanje, IT at the first civil registry office, 11/05/2021

RISK-BASED TESTS

4.1 RISK ASSESSMENT

Are decisions regarding the legitimacy of uses, benefits of using digital ID, and their impact on individual rights informed by risk assessment?

We have no knowledge or evidence of risk assessment being done prior to the laws and regulations being drafted or approved. The Civil Registry law provides that e-SIRCEV system aims to create interoperability mechanisms with other governmental sectors[58] using the NUIC.

When the interoperability framework is fully operational, data sharing between the different state systems may be a problem, as the definition of responsibility of the institutions that will make use of the shared data is not clear.

The e-SIRCEV system was designed based on an operational system from Uganda. In 2016, a pilot of the functionality of the system was carried out in Magude district, Maputo Province. The report of this pilot is available in the MJACR but special clearance is required to access it.[59] This suggests a lack of transparency from the MJACR. This kind of information should be in the public domain for any citizen to access.

4.2 DIFFERENTIATED APPROACHES TO RISK

Do the laws and regulations envisage a differentiated approach to governing uses of digital ID, based on the risks it entails?

Governance of the use of digital ID for multiple digital activities has not yet arisen because, as explained earlier, there is not yet a complete and interoperable digital ID system legislated for and in operation.

There are various processes underway which are directly or indirectly related to digital ID issues, including a data protection law in preparation by the INTIC, but the processes are not yet unified. Mozambique has already ratified both the African Union Convention on Cybersecurity and the Protection of Personal Data

58 Law 12/2018, Article 2 - d)

59 Interview with Dr Rufaro Cashanje, IT at the first civil registry office, 11/05/2021

(through the Resolution no. 5/2019) which was adopted by AU Heads of State and Government in 2014, and the Budapest Convention on Cybercrime.[60] MCTES is currently leading processes to achieve approval of a number of important documents, including the Cybersecurity Policy and National Cybersecurity Strategy; and the Regulation on Internet Use.

4.3 PROPORTIONALITY

Does the law on digital ID envisage governance, which is proportional to the likelihood and severity of the possible risks of its use?

Currently, there is inadequate or no independent governance in this area. The existing laws and regulations are based on internal sectoral supervision and decision-taking, and in some cases the ICT or telecoms regulators, which are not independent bodies. ICT policies and strategies under discussion make some provision for external participation in boards and councils, making it possible to discuss and receive inputs from private institutions and civil society organisations.[61] However, to date the legislation to govern the creation of these bodies and define their nature and competencies has not been published or approved. It is therefore too soon to say whether they will be independent. However, MISA Mozambique led a group composed of civil society organisations, academia and private organisations, which organised meetings with the MCTES and the Assembly of the Republic to discuss aspects related to safeguarding the rights of citizens in the preparation of different legislation around digital identity.[62]

4.4 RESPONSE TO RISKS

In cases of demonstrable high risk from uses of digital ID, are there mechanisms in place to prohibit or restrict the use?

There are currently no known risk mitigation mechanisms in place. They will need to be defined in a new law or in the competencies of the regulator.

The National Cybersecurity Policy and its respective Strategy are being

60 Interview with Dr Constantino Sotomane, National Director of ICT at MCTES, 26/02/2021

61 Interview with Ernesto Saul, MISA Mozambique, 15/03/2021

62 *Ibid.*

prepared by INTIC with support from INCM. They detail the needs and processes for implementing a cybersecurity environment in the country, focusing on a risk-based approach in assessing responses to cyber threats and risks, ensuring cybersecurity in Mozambique.

In the preparation of these documents, different sectors were consulted, including governmental institutions, private sector, academia and civil society, to harmonise and make sure that all necessary aspects were considered. After the consulting process, these documents will be subject to government approval and implementation.[63]

63 Interview with Dr Constantino Sotomane, National Director of ICT at MCTES, 26/2/2021

CONCLUSION

Mozambique does not yet have a fully integrated foundational digital ID system, nor does it have complete legislation on the protection of personal data.

This research into the legislation, complemented by interviews, shows that the main actors are fully aware of the need to progress in implementing a national digital ID system. Similarly, some steps are being taken and are already visible in the creation of digital systems and the development of relevant laws and regulations.

It is evident that existing laws and decrees approved for the various sectors already include general statements about procedures for interoperability. However, in practice these statements are for the future, as detailed procedures are still lacking and functioning interoperability systems are practically non-existent.

Application of the evaluation framework shows that the e-SIRCEV system can develop into the basis of an integrated digital ID system, and already meets some of the concerns of this framework, but that the process has only just begun. The framework also helps to highlight the need for a deeper discussion of issues of rights and risks during the ongoing discussions and development of strategy, plans and legislation.

Improved coordination to facilitate discussions among the three main ministries currently involved is essential. It is clear that there has to be alignment or integration between the e-SIRCEV system and the existing system for issuing ID cards. In the terms of the Decree defining the NUIC, the ministry that supervises ICTs is defined as the lead coordinator among the main actors, and this definition is still valid.

Relevant issues already coming under discussion during the finalisation of the Cybersecurity Policy and National Cybersecurity Strategy include the need to:

- consider other countries ´ experiences regarding the structuring of a lead or central organisation such as a central ID authority;
- investigate the patchwork of existing legislation and the competencies of the various bodies to be revised, possibly producing a single law and harmonising the existing legislation accordingly; and
- involve other sectors in the discussions and potentially in some kind of consultative or oversight group.

The need for independent regulators is being raised in current media debates, most immediately around a current government proposal to establish a media

regulator. Like the others referenced in this document, the media regulator would have some forms of administrative autonomy but be supervised by a ministry or government institution that decides policies. Having an autonomous institution that is not subordinated to a public governmental body would facilitate the inspection and regulation of issues related to ICT or telecommunications, for instance.

Due to the existence of many actors, coordination and leadership must establish a holistic vision of the future digital ID system and deepen the joint thinking about its goals, citizen rights, risk mitigation issues, the dangers of exclusion, practical implementation questions, and so on. There remains a risk that each actor ends up advancing in its specific sector, without having the opportunity to think through the strategic vision and the challenges and practicalities of implementation.

The bottom line is that while all the actors are thinking about what their sectors need to do technologically, legally and organisationally, and are working on digitalisation-related activities, the existing legislation does not include a specific law about digital ID other than the 2010 Decree on creating the NUIC. At the same time, several of the laws and regulations and other instruments that are new or in preparation will be of considerable help when the actual digital ID work begins. At the same time, the competencies of some of the institutions may need revision to eliminate overlap or duplication, and possible conflicts of interest.

Finally, the digital ID needs to move higher up the government agenda, and there are expectations for this to happen. A World Bank team has been working with the Government of Mozambique to prepare a program called *ID4D - Identification for Development*. A preliminary analysis was made in 2019, but the work planned for 2020 could not be carried out due to the Covid-19 pandemic. It is expected to be resumed in the near future. Additional named partners in the work so far include the Bill and Melinda Gates Foundation, the Australian Government and the Omidyar Network. The initial analysis, like our research, recognised that there is a long way to go, but that progress has been made.

Recommendations for different stakeholders include:

For civil society:

- The framework concepts should be made available to other interested parties in the public, private and civil society sectors to inform their engagement in consultative processes or to demand greater consultation.
- Civil society organisations should press for future legislation in this area to be submitted to Parliament for debate and approval rather than approved by Decrees.

- Civil society organisations should press for the independence of regulatory bodies in the areas of ICTs, telecommunications, e-government and digital ID systems.

For policymakers:

- Steps should be taken to ensure that the actors involved in discussing and planning digital ID activities in Mozambique have access to the evaluation framework, so that the ideas and approaches contained in it can be considered before policies and legislation are formalised.
- Public consultations, including with the private sector and civil society, should be instituted to facilitate debating legislation on digital ID, and contributions should be solicited; legislation should be submitted to Parliament for approval.
- Coordination procedures and the definitions of the roles of the three main actors should be updated, and the possible establishment of a single Digital ID Authority should be considered.
- Results obtained and the experiences of other countries should be analysed to enrich the national debates and define best practices.
- Government must ensure that citizens are not excluded from use of the system for lack of access, and that parallel solutions are maintained.

For technologists:

- The future foundational digital identity system must take into account the type and limit of information to be collected from citizens, provide access control mechanisms to the data collected and stored to ensure the privacy of citizens, as well as clear mechanisms for sharing and accessing the data by public and private institutions.
- System architecture should take into account the issues of sustainability, data security, cybersecurity, maintenance capacity, modular components that permit expansion and adaptation, and user-friendliness.
- System documentation must be available to Mozambican technicians, and training for technical support and maintenance should be included in the development programme.

For further research:

- Qualitative research into the functioning of the e-SIRCEV system, covering elements such as technical issues, operational implementation, as well as citizens' awareness of their rights.

- Studies of foundational ID systems already in operation in other countries - covering implementation procedures and results as well as technical, legal and social issues - will provide new insights for establishing a novel system such as is envisaged in Mozambique.

REFERENCES

Mondlane, E. (1969) *The Struggle for Mozambique.* Penguin Books, London.

Decree of the Definition of procedures for the creation and use of the NUIC and attributions of the institutions involved, No. 44 of 2010.

The Revision of the Civil Registry Code Act, No. 12 of 2018.

Electronics Transaction Law Act, No. 3 of 2017.

Decree of the Approval of the Regulation on the Interoperability Framework, No. 67 of 2017.

Punctual Review Law of the Constitution of the Republic of Mozambique Act, No. 1 of 2018.

Decree of Creation of INAGE, No. 61 of 2017.

Decree of Creation of INTIC, No. 9 of 2011.

Decree of Creation of INCM, No. 32 of 2001.

Decree of Introduction of the Identity Card for the national based citizen in biometric elements, No. 11 of 2008

Draft proposal for a National Cybersecurity Strategy and Policy.

Presentation *Missão Diagnóstico ID4D - Resultados preliminares.*

Interview with Dr. Constantino Sotomane, National Director of ICT at MCTES, 26/02/2021.

Interview with Eng. Sérgio Guivala, INTIC, 16/04/2021.

Interview with Dr. Sérgio Cambaza, Head of the Department of Registry and Notary Information Systems - MJACR, 14/04/2021.

Interview with Dr Rufaro Cashanje, ICT staff member at the First Civil Registry Office - MJACR, 11/05/2021.

Interview with Eng. Sérgio Mapsanghane, INAGE, 23/03/2021.

Interview with Ernesto Saul, MISA Mozambique, 15/03/2021.

www.ine.gov.mz – home page (accessed 29 April 2021).

http://hootsuite.com/resources/digital-in-2018-emea (accessed 31 May 2021).

ANNEX 1

OVERVIEW OF EVALUATION FRAMEWORK

In 2019, the Centre for Internet and Society (CIS) published "Governing ID: Principles for Evaluation" ("Evaluation Framework"), which set out a framework for the evaluation of digital identity. The Evaluation Framework should be read alongside CIS' glossary of 'Core Concepts and Processes' that explains different principles such as identification, authentication, foundational and functional identity systems, that are present in any Digital ID system. Early draft frameworks were published in the lead up to RightCon 2019 held in Tunisia and were discussed at an event organized by Omidyar Network titled "Holding ID Issuers Accountable, What Works?"

The impetus for this document came from Clause 16.9 of the UN Sustainable Development goal, "By 2030, provide legal identity for all, including birth registration". Thus, countries across the world have begun implementing new, foundational, digital identification systems ("Digital ID"), or begun to modernize their existing ID programs.

The history of digital ID programmes in countries such as India, Kenya, Estonia, Jamaica, and the U.K. demonstrated the different concerns associated with privacy, surveillance, exclusion, and mission creep. CIS felt that there was urgent need for further analysis and discussion into the appropriate (and inappropriate) uses of digital ID systems. Through research, we realised that the use of a Digital ID system is inextricably linked to the governance structure and fundamental attributes of the Digital ID system. Hence, a use analysis of Digital ID systems is best accomplished through an evaluation framework that provides principles against which Digital ID may be evaluated.

Consequently, the Evaluation Framework lays out a series of tests that can be used across jurisdictions to assess the legitimacy and governance of Digital ID. CIS selected three sets of tests – the Rule of Law tests, Rights-based tests, and Risks-based tests – to form the bedrock of the Evaluation Framework for Digital ID. CIS adopted the definition of 'digital identity' provided by David Birch, as a "system where identification (the process of establishing information about an individual), authentication (the process of asserting an identity previously established during identification) and authorisation (the process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity) are all performed digitally". Such a definition departs from the ID4D Practitioner's Guide that defines authorisation from the lens of eligibility, i.e. the process of determining whether a person is 'authorised' or 'eligible'.

In coming up with these tests, CIS adopted a first principles approach, drawing from methodologies used in documents such as the international Necessary & Proportionate Principles on the application of human rights to communication surveillance, the OECD Privacy Guidelines, and international scholarship on harms based approaches.

RULE OF LAW TESTS

Digital ID systems per se involve a vast collection of personal and sensitive personal data that infringe the privacy of individuals. Any such restriction on fundamental rights must be legal, backed by a legitimate aim, narrowly tailored in scope and application, accountable, and prevent mission creep. Hence, the Rule of Law tests evaluate whether a rule of law framework exists to govern the use of Digital ID and ensure sufficient deliberation before a Digital ID system is implemented for public and private actors. These tests ask six questions about:

1) **Legislative mandate** – whether the Digital ID project is backed by a validly enacted law, and whether the law amounts to excessive delegation.

2) **Legitimate aim** – whether the law has a validly defined legitimate aim.

3) **Actors and purpose** – whether the law clearly specifies the actors who use digital ID and the purposes for which the Digital ID is used.

4) **Grievance redress** – whether the law provides for adequate redressal mechanisms against actors who use the Digital ID and govern its use.

5) **Accountability** – whether there are adequate systems of accountability for all the (public and private) actors and users in the Digital ID system.

6) **Mission creep** – whether there is a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of Digital ID.

RIGHTS-BASED TESTS

Criticism of Digital ID systems focus on their violations of privacy – whether through the mandatory collection of sensitive personal data, risk of surveillance and profiling, or the lack of robust access control mechanisms – and the risk of exclusion. Hence, the Rights-based tests put forth certain rights-based principles, such as necessity and proportionality, data minimisation, access control, exclusion, and mandatory use that should be used to evaluate the extent to which the rights of citizens are being infringed through the use of Digital ID systems.

These tests ask five questions about:

1) **Necessity and proportionality** – whether the privacy violations arising from the use of Digital ID necessary and proportionate to achieve the legitimate aim.

2) **Data minimisation** – whether there are clear limitations on what data may be collected, how it may be processed, and how long it is retained for, during the use of Digital ID.

3) **Access control** – how is access by state and private actors to personal and sensitive personal data controlled through the law.

4) **Exclusion** – whether there are adequate mechanisms to ensure that the adoption of Digital ID does not exclude citizens/residents or restrict their access to benefits and services.

5) **Mandatory use** – whether there are valid legal grounds to justify the mandatory nature of Digital ID, if any.

RISK-BASED TESTS

A rights-based constitutional approach to evaluating Digital ID is necessary, but not sufficient, to ensure a well-functioning Digital ID system. Regulation of Digital ID must be sensitive to the different types of harms caused by its uses (such as privacy harms, exclusion harms, and discriminatory harms), the severity and likelihood of the harm, and must build in mitigation mechanisms to reduce the probability or impact of the harm. Although most countries do not perform such risk-based tests, CIS hopes that by incorporating these tests into the Evaluation Framework, governments will have a more realistic picture of the harms that are likely to occur in a Digital ID system and take appropriate steps to reduce the risk of the same. These tests ask five questions about:

1) **Risk assessment** – whether decisions regarding the legitimacy of uses, benefits of using Digital ID, and their impact on individual rights is informed by risk assessment.

2) **Differential risk approach** – whether the law adopts a differentiated approach to governing uses of Digital ID (such as per se harmful, per se not harmful, and sensitive), based on the risk factors.

3) **Proportionality** – whether the governance framework in the Digital ID law is proportional to the likelihood and severity of the possible risks of its use.

4) **Response to risks** – given certain demonstrably high risks from the use of Digital ID, whether the law has built in mitigatory mechanisms to restrict such use.

Using the Evaluation Framework, CIS published case studies on the use of Digital ID for the delivery of welfare, for verification, and in the health care sector. Country specific case studies were carried out for Estonia's e-Identity program, India's e-KYC framework, India's Unique Identity (Aadhaar) programme, and Kenya's Huduma Namba programme.

The eventual aim of the Evaluation Framework is to evolve these three tests into a set of best practices that can be used by policymakers when they create and implement Digital ID systems; provide guidance to civil society to evaluate the functioning of a Digital ID system; and highlight questions for further research on the subject. Through this project, in collaboration with RIA, we hope to fulfil some of these goals. ■