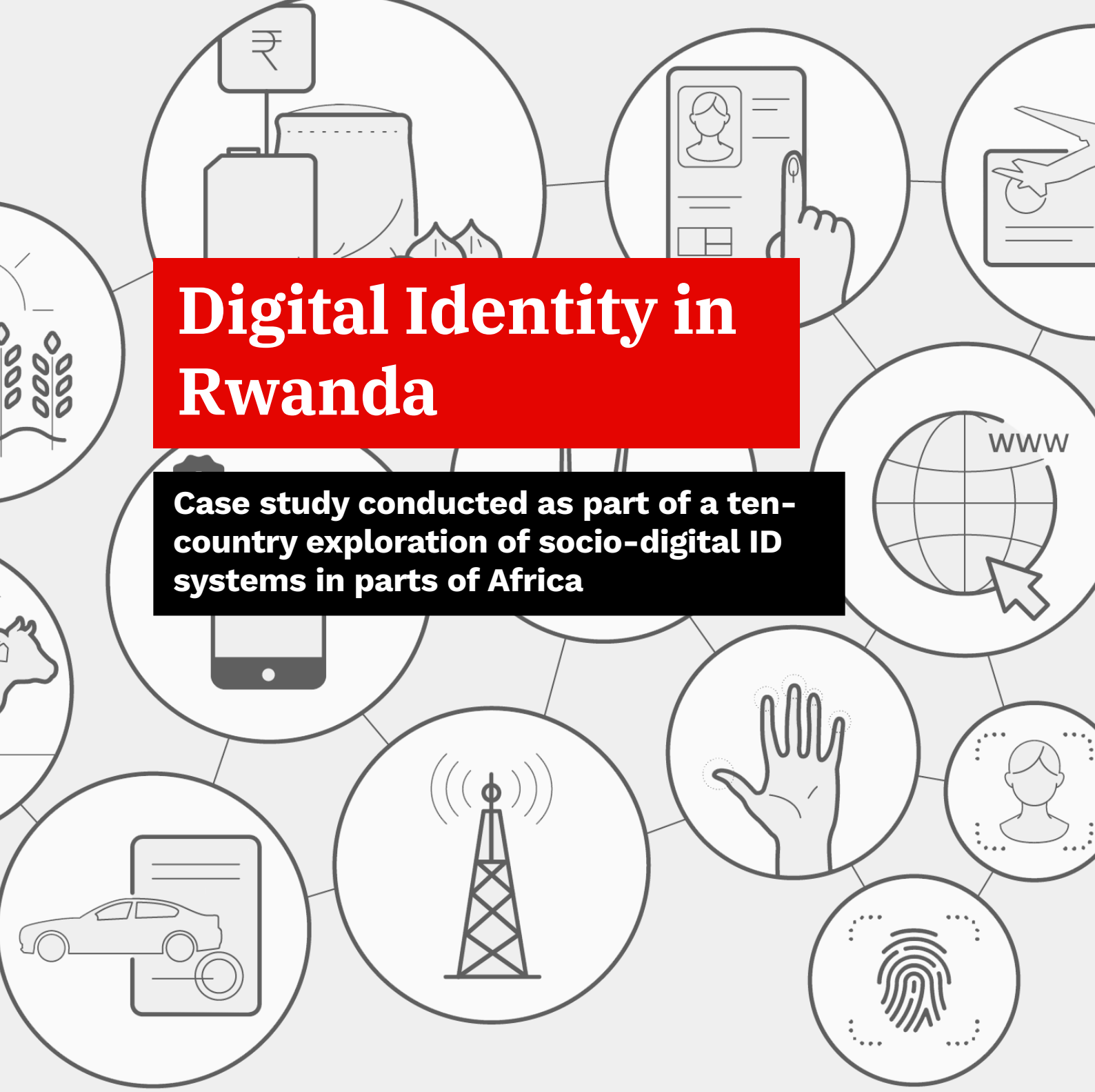

Digital Identity in Rwanda

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

RESEARCH & WRITING
Dr. Elvis M. Binda

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 Rwanda

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 ←

Shared under
Creative Commons Attribution 4.0 International license

Digital Identity in Rwanda

By Dr Elvis M. Binda, University of Rwanda

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 Rwanda case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Dr Elvis M. Binda, University of Rwanda. 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 Dr Elvis M. Binda 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

Rwanda started developing its modern ID system in the late 2000s with the enactment of the law governing the registration of the population and issuance of the national ID card in 2008. This law introduced two types of ID cards. The first and the most used is a plastic ID card bearing a 2D barcode on its back. The second is an integrated smart ID card with a chip. They both have a 16-digit unique number, which is currently used as a unique identifier number.

While the Rwandan ID system is commendable because it satisfies the daily identification needs in the physical world today, the national ID identification number is becoming more popularly used as a key to access services and to effect transactions electronically. However, the extent to which this development is backed by an effective legal framework has not received much attention. This research report uses CIS' Evaluation Framework to evaluate the extent to which the Rwandan digital ID system complies with international standards in the protection of the rights of data subjects.

It appears that, despite the tremendous functional development of the Rwandan ID system, the legal and institutional frameworks in support of the use of digital ID in Rwanda seem to be weak. A recommendation is made to adopt specific legislation on the use of digital IDs in addition to the recent promulgation of the law on data protection and privacy to strengthen the existing framework.

ACRONYMS AND ABBREVIATIONS

BOD	Board of Directors
CIS	Centre for Internet and Society
ID4D	Identification for Development
IECMS	Integrated Electronic Case Management System
KYC	Know Your Customer
MoU	Memorandum of Understanding
NID	National ID Card Database
NIDA	National Identification Agency
NIN	National Identity Number
No.	Number
NPR	National Population Registry
OG	Official Gazette
RIA	Research ICT Africa
USD	American Dollar

CONTENTS

INTRODUCTION

Rwanda is a small, landlocked country in Africa's Great Lakes region. With a population of about 12 million people, it is among the most densely populated countries in Africa. To identify its population and aliens living on its territory, the Government of Rwanda has built a robust ID system consisting of the National Population Register (NPR) and the National ID card database (NID). This system, which was developed in 2007, serves as a foundational system intended to support all of the identification needs of the country. The NPR contains identity data of almost all Rwandans, resident foreigners and refugees, including children. By contrast, the NID only contains data of Rwandans, foreigners and refugees aged at least 16 years old.

Data collected through the NID are attested with the issuance of an ID card that has a unique National Identity Number (NIN) printed on the front of the card. This 16-digit NIN becomes an identifier of an individual for their entire lifetime. It is increasingly being used as the digital ID of Rwandans to obtain services provided by various public institutions through *Irembo*, the e-government portal. Even though some public services are exclusively accessible through *Irembo*, and the use of online services remains the only way to access judicial services through the Integrated Electronic Case Management System (IECMS), Internet penetration in Rwanda is still low. A RIA-conducted survey revealed that less than 10% of Rwandans have access to the Internet.[9] The ID also bears a 2D barcode on the back, containing biometric and biographic data. At a point of service, the barcode can be read using a terminal or a hand-held device to confirm the identity of the holder. The use of this feature does not yet appear to be very common, however.

The compulsory use of NIN as digital ID to access increasingly more public services online, coupled with the connection of public and private actors to the NID database, calls for a thorough analysis of the status of digital ID in Rwanda against internationally recognised standards to acknowledge good practices and to make constructive recommendations to improve the ID landscape of Rwanda. It must be borne in mind that this report was completed before the entry into

9 RIA, April 2019, p. 17. This must be contrasted by another source that claims that in January 2021, Internet penetration in Rwanda stood at 31.4%. S. Kemp, '*Digital 2021: Rwanda*' available at *https://datareportal.com/reports/digital-2021-rwanda* (accessed 20 June 2021).

force of the law relating to data protection and privacy.[10] Therefore, it does not unfortunately reflect this interesting development.

Analysis of Rwanda's Digital ID system

This report provides an assessment of Rwanda's digital ID systems (Digital ID) using the CIS Evaluation Framework for Digital Identity.

The Framework provides benchmarks to evaluate the governance of Digital ID across countries and helps determine whether a given use of Digital ID is appropriate. The evaluation is done against three types of checks. The first is Rule of Law tests that address a set of questions to ensure that a rule of law framework exists to govern the use of Digital ID. The second is Rights-based tests that look into the adherence of the use of Digital ID to basic principles of the right to privacy and inclusiveness. The third is Risk-based tests that assess how the legal and institutional framework s protect individuals against perceived or existing risks and harms related to the use of a digital ID.

10 The Law No. 058/2021 of 13/10/2021 relating to the protection of personal data and privacy entered into force on 15 October 2021 and can be accessed via the link *https://www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf (last visited 20 October 2021).*

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The project of establishing the Rwandan national ID is supported by Law No. 14/2008 of 04/6/2008, which governs the registration of the population and issuance of the national identity card, and was amended in 2018. Ministerial Order No. 02/07.01, which determines the specifications of the national ID card for Rwandans, as well as related fees, was passed on 4 September 2013.

Quality, clarity and precision of law

Despite the existence of these laws, the practical application of digital ID seems to extend beyond these legislative instruments and the project is thus not fully backed by a validly enacted law. The existing legal texts are not very detailed and do not provide enough information about some crucial aspects related to the use of the national ID. For instance, the existing legal provisions do not mention different types of ID cards to be issued, neither do they regulate the potential of NIN to be used as an online identifier.[11] Yet it is increasingly clear that the NIN is meant to be a single online identity, which could prove to be a challenge on a number of fronts.

In fact, through the *Irembo* platform (the e-government portal used by Rwanda's government), it is easy to gain access to personal information (such as full names, marital status, date of birth, place of birth, name of spouse, etc.) of any person when you type in their NIN. No password is required to have such access. For an ordinary citizen, the display of all this information after merely typing in an NIN can be disconcerting, as they can wonder how much information the government or anyone with access to their NIN could gain about them. The fact that the law is silent about the collection, storage and use of personally identifiable information through the national ID database, coupled with its accessibility by various public and private service providers, threatens the right to privacy of Rwandans.

11 The analysis of the Rwandan ID legal landscape suggests a discrepancy between the legal provisions and the actual practice. Apart from regulating the issuance of the ID card, there seems to be a big vacuum regarding legal provisions governing current and potential future uses of the NIN online. Also, Irembo as a platform and all facilities it provides do not fall under specific legal provisions, notwithstanding the importance of services people get through it and the risks associated with the online use of one's ID details.

Digital aspects of the Rwandan ID are not regulated by the law. The law that provides for the issuance of national ID in Rwanda, remains silent about the role of the NIN for online use and the amount of information linked to one's NIN stored on the national ID database.

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?

No specific legal provision states the aim of the law, leaving the aim to be deduced from its title, i.e. to regulate the 'registration of the population and issuance of the national identity card'. Article 12 of the Ministerial Order seems a bit clearer as it states that the integrated smart identity card helps "the owner to get various services in public and private sectors". However, this provision applies to the integrated smart identity card, which is more expensive, and it is unclear whether the smart ID card is already available for use by all Rwandans.[12]

Although the law does not clearly state its aim, its title suggests that its enactment aims at a legitimate goal, namely the registration of the population and issuance of the national ID. Nevertheless, other practical uses related to the benefits of the digital ID system – no matter how legitimate they may appear - seem not to have been considered at the outset as an aim for the establishment of the Rwanda ID card.

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?

Apart from the public servants involved in the registration of the population and the issuing of the national identity card – such as the Executive Secretary of a sector and representatives of Rwandan missions abroad – the law governing ID does not mention the intervention of other actors in the use or the management of the national ID database.

Instead, Law No. 43/2011 of 31/10/2011 establishes the National Identification Agency (NIDA law) and grants it the mission of population registration, civil

12 J. Atick, '*The Identity Ecosystem of Rwanda: A Case Study of a Performant ID System in an African Development Context*', 2016, p. 22.

registration and issuance of national identity cards.[13] There is no reference to a likely implication or connection of private actors or other public agencies with the ID database.

Yet, it has been reported that numerous programmes at as many as 45 institutions use the NIN as a customer identifier.[14] Banks and telecommunications companies reportedly sign Memorandums of Understanding (MoUs) with NIDA to access the national ID database to ensure Know Your Customer (KYC) functionality.[15] But because this third-party use is not regulated by the law governing ID in Rwanda, it poses the question of their accountability for the private data they are collecting.

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

Neither the law governing population identification and issuance of national ID cards nor the law establishing NIDA provide for the use of the National ID system by private actors. As mentioned above, only Article 12 of the Ministerial Order refers to access to private services as one of the ways the integrated smart card could help its owner.

The current state of affairs of the Rwandan digital ID legal framework arguably leaves a vacuum regarding the accountability of both public and private actors who happen to have access to the national ID database. Nevertheless, to fill this gap, NIDA signs MoUs with all institutions and entities before they gain access to the national ID database, in addition to the requirement of observing certain security standards and certification.[16] However, neither the binding force of this kind of MoU nor NIDA's capacity to monitor how these institutions and entities use data availed to them, can be ascertained. The lack of a clear and binding regulatory framework enables the likelihood of sensitive personal information collected for one purpose being used for an entirely unrelated purpose without the knowledge or consent of the data subject.

13 Article 4 NIDA Law.

14 World Bank Group, ID4D Country Diagnostic: Rwanda, 2016, p. 29. [ID4D] According to the Director General of NIDA, about 45 institutions are directly connected to the national ID database for online authentication.

15 ID4D, p. 29.

16 ID4D, p. 29.

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

The law governing population registration and the issuance of national ID does not clearly define the nature of data to be collected by NIDA during registration of the population and the issuance of ID. It seems, rather, to delegate that power to the minister in charge of local government. Indeed, the Ministerial Order determines specifications of the national identity card for Rwandans and the fee structures related to national identification services lists information to be printed on the ID card. They include the holder's names, date of birth, and sex.[17] However, the law does not specify the data that relevant authorities are supposed to collect to make and issue the ID.

In practice, however, any person who applies for an ID card is requested to submit biometric data, such as two fingerprints, a photograph, as well as details such as the names of their parents and place of birth. The collection of the names of parents and place of birth in addition to information displayed on the ID is particularly important in Rwanda, where the use of family names is not common.[18] In fact, it is rather common for parents to give their children names that are completely different from their own. In principle, a child is given a name that is usually expressive in its meaning (gratitude, love, wish, strength, etc.) and it must be unique within the family. So, it is generally impossible to deduct any familial relationship based on individual names. As much as siblings will generally have completely different names, it is also common for unrelated people to have the same name or even multiple same names.[19]

While these extra details can help to distinguish between two or more people who have exactly the same names, the fact that each person is issued with a unique NIN may obviate the need of collecting such data. Further, there is no evidence of circumstances where fingerprints are used to authenticate someone in connection with the use of their ID, nor do there appear to be future plans from government to use biometrics for such authentication. The collection of fingerprints for the issuance of an ID appears unnecessary as a result.

Of course, the collection of unnecessary data for the issuance of an ID card is nurtured by the silence of the law. This leads to the accumulation and storage of personal data on the ID database without any actual need to use them. In case of a breach, the collection of unnecessary information exposes the data subject to the risk of identity theft, for instance.[20]

17 Art. 14(4) Min Order

18 Atick, p. 16.

19 Atick, p. 17.

20 J. Darrow & S. Lichtenstein, 'Do You Really Need My Social Security Number – Data Collection Practices in the Digital Age', 10 N.C. J.L. & Tech. 1 (2008), p. 6.

Does the ID system provide adequate user notification mechanisms?

After the data subject has registered and submitted all needed information for the issuance of their ID card, they receive no further notification or communication from NIDA about changes or updates to their personal data. The database is still, however, regularly updated. Not only new civil status information such as birth, death, marriage, divorce, adoption, or recognition is added, but other socio-economic information, such as bank loans, criminal record, etc. can be linked with someone's NIN, depending on the type of actor or entity.[21]

All of this happens in the total ignorance of the data subject, which gives the impression that the national ID database operates as a blackhole. Considering the potential sensitivity of such information and the impact that any breach, mistake, or error may have on the life of the data subject, there is a need for proactive notification whenever an update or alteration is made on the data subject's digital ID profile. This notification should also include the right of rectification and the right of removal, should inaccurate data be appended to their NIN. These rights are currently not granted to data subjects.

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

Neither the law on population registration and ID card issuance nor the law establishing NIDA provide for the rights of data subjects to access, confirm or correct information, or to opt out. Once they have submitted their data to the national ID database, individuals are not aware of the content kept therein. The only information in their possession is what is printed on the ID card. Because they are not notified of updates or alterations done in the underlying database, technically there is no opportunity for them to confirm any data entered.

However, in general, Article 88 of the Law Governing Persons and Family provides for the right of any interested person to seek the rectification of clerical or material errors as well as material omissions made by civil registrar.[22] By interpretation, the application of this provision can be extended to the national ID.

It is not clear whether foreigners and refugees have any right to opt out from the national ID database either. If they do have such rights, the procedure to do

21 N. Kayser-Bril, 'Identity-management and citizen scoring in Ghana, Rwanda, Tunisia, Uganda, Zimbabwe and China', *Algorithm Watch*, 2019, p. 10.

22 Law No. 32/2016 of 28/08/2016 governing persons and family, OG No. 37 of 12/09/2016.

so is not regulated and the distinction between data that can be removed when one opts out and data that needs to be kept for security reasons or for further reference is not provided. However, since the possession and carrying of the national identity card is compulsory for every Rwandan aged 16 years and above, it is hard to envisage how they can opt out from the national ID database, which is the online support mechanism of the physical ID card.

Nevertheless, in addition to the general right to information provided by the law governing access to information,[23] the law governing information and communication technologies (ICT Law) provides a list of obligations imposed on the data controller, who is defined as "any person who electronically requests, collects, collates, processes or stores personal information".[24] Those obligations can be interpreted as creating rights for the data subject. Among those obligations there is the obligation:[25]

- to obtain written permission specifying the object for data collection, collation, processing and storage;
- not to use electronic means to request, collect, process or store data relating to a subject not authorised by law or requested for being a research topic;
- not to use personal information for any purpose other than the purpose for which it is intended, unless the data subject or the law permits such use;
- to keep a record of the personal information and the specific purpose for which the information was collected;
- to keep secret the personal information disclosed to a third party and the date and reason for the disclosure, as long as the information is used or retained for a period of at least one year; and
- to delete all data which has become obsolete.

As the law on data protection has entered into force, the rights of the data subject will be clearly known and well protected.[26]

23 Law No. 04/2013 of 08/02/2013 relating to access to information, OG No. 10 of 11/03/2013 [Access to Information Law]

24 Art. 5 (24o) of the Law No. 24/2016 of 18/06/2016 governing information and communications technologies, OG No. 26 of 27/06/2016 [ICT Law]

25 Art. 209 of ICT Law.

26 See below (sect. 3.2) for details.

2.4 REDRESSAL MECHANISMS

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

The law governing population registration and national ID issuance provides for criminal penalties relating to the use of the national ID card. These penalties concern people who fraudulently deliver, receive or use an ID card.[27] However, the law does not provide for an adequate redress mechanism to handle violations of data subjects' rights when these violations are committed by NIDA or other institutions and entities that have access to the ID database associated with the digital ID. This leaves room for recourse to the general redress mechanisms provided under administrative law. They include an administrative review before NIDA and – if need be – subsequently filing a case before an administrative judge.

Criminal redress can be envisaged in cases where the rights of the digital ID holder are violated in ways prohibited by certain provisions of the law on the prevention and punishment of cybercrimes (Cybercrimes Law).[28] For instance, the Cybercrimes Law considers it an offence for any service provider not to exercise due care and skills to prevent the disclosure of computer data made available to a third party.[29] This offense is liable to a conviction of up to FRw 3 million (about USD 3 000). Upon conviction of the offender, the victim may be entitled to damages. This may apply to service providers which have access to personal data available on the population database if they do not take the necessary steps to protect the data against third parties. In this case, ordinary criminal procedure will be followed, and all due process principles must be observed.

27 Article 13 National ID Law.

28 Articles 44-50 of the Law No. 60/2018 of 22/08/2018 on the prevention and the punishment of the cybercrimes [Cybercrimes Law] punish offenses committed by service providers. They include disclosure of data made available to third party, provision of access to a computer system and cause them to send electronic content on another person's computer system, refusal to remove or disable access to illegal information stored, non-reporting of cyber threats incident, modification of stored information, illegal search results, and failure to take action on take-down notification.

29 Article 44 Cybercrimes Law.

2.5 ACCOUNTABILITY

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

As mentioned, NIDA is the administrator of the National ID database. According to Article 7 of the law establishing the NIDA and determining its mission, organisation and functioning, NIDA's Board of Directors (BoD) is the governing and decision-making organ of this institution.[30] It is composed of seven members appointed by the President of the Republic for a term of office of three years renewable only once.[31]

The fact that NIDA's BoD members are appointed by the President of the Republic gives them a high profile that allows them to exercise their supervision with a great degree of independence. In addition, no BoD member is allowed to perform any remunerated activity within NIDA, nor are they allowed to bid for tenders of NIDA. While this provision aims at preventing any conflict of interest between NIDA's appointed BoD members and the institution, it also enhances their independence as members of an oversight organ.[32] However, the Board does not appear to have the legal responsibility to ensure NIDA's accountability for the management and use of the national ID database. And while NIDA is under the supervision of the Ministry of Local Affairs from an administrative point of view,[33] the Ministry does not appear to have been assigned a clear role in holding NIDA accountable in case of poor management of the national ID database.

The fact that NIDA simultaneously plays the role of both the administrator and the regulator of the national ID database indicates the need for an independent regulatory board that can hold NIDA responsible for any breach in the use or the management of the system.

30 Article 7 NIDA Law.

31 Article 3 of the Prime Minister's Order No 83/03 of 08/10/2012 determining the competence, responsibilities and functioning of the board of directors of national identification agency (NIDA) and the term of office for board members, OG No. 43 of 22/10/2012.

32 Art 9 of the Prime Minister's Order No. 83/03 of 08/10/2012 determining the competence, responsibilities and functioning of the board of directors of the National Identification Agency (NIDA) and the term of office for board members.

33 Annex I to the Prime Minister's Order No. 38/03 of 11/04/2014 determining the organizational structure and summary of job positions of the National Identification Agency (NIDA).

2.6 MISSION CREEP

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

The law governing population registration and ID card issuance does not provide the proposed purpose of national ID database and NIN. When the ID system was first developed in 2007, its initial purpose was to register the population and to issue them with a physical card to facilitate identification. It was basically intended to be a paper-based system like civil registration has always been. However, with the development of the online database over time, some other uses have emerged for which the database was not originally intended. The fact that the database is now open and accessible to a certain number of public and private actors, for example, increases the likelihood of mission creep, illegal profiling and irregular surveillance, in addition to criminal activities of fraud and identity theft. This puts the data collected and/or generated through the use of the national ID database at risk of being used for a different purpose from that for which they were primarily collected.

If new purposes are identified, are there regulatory procedures in place to determine their legitimacy?

According to NIDA, the rationale for the Rwanda national ID database is threefold: (i) to computerise the population registry, (ii) to issue secure national ID cards and driving permits for Rwandans, refugees and foreign residents, and (iii) to enhance quick public service delivery by promoting online services through integration.[34]

While none of these purposes are set forth in the law governing population registration and ID issuance, they reflect the current situation. These additional uses that have now become the *de facto* norm have not, however, been developed in accordance with a legitimate legislative process.

For instance, every Rwandan who is sentenced to imprisonment for a crime has their ID card confiscated and kept with NIDA until they have served their full sentence.[35] While this confiscation is not provided for by any legislation, it is used as an extra security layer to ensure that prisoners do not escape because it would be exceedingly difficult for anyone to survive in the country without an ID. Nevertheless, it should be noted that with the NIN, one does not need a printed ID card to have access to certain online services.

34 *https://www.id4africa.com/2019_event/presentations/PS1/5-Josephine-Mukesha-NIDA-Rwanda.pdf*, p. 2.[Mukesha]

35 ID4D, p. 26. See also GSMA, 'Digital identity opportunities for women – Insights from Nigeria, Bangladesh, and Rwanda', May 2019, p. 45.

RIGHTS-BASED TESTS

3.1 NECESSITY AND PROPORTIONALITY

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

Both the left and right thumbprints and a photograph of the person are collected during the ID card registration process and stored in the national ID database. These biometric data are associated with and stored alongside other relevant personal information of the ID card seeker, such as their name(s), age, sex, the names of their parents, and name(s) of their spouse where applicable, among other data.

The connection of other institutions and entities to the national ID database and the lack of clear information on what data they share (in terms of what additional information other institutions add to what NIDA already collected during the registration for an ID issuance) increases the likelihood of extra personal data being linked to the NIN of the data subject without the latter's knowledge. This might include any criminal conviction, the nationality of their spouse, etc. For instance, it has been observed that personal data of the *Irembo* platform users are automatically stored on the system, whether they are a registered or a 'guest' user. As soon as the user's NIN or passport number is typed in, all other ID information provided for a previous service is displayed.

While collecting and centralising this kind of information may be useful for government services and may facilitate people's identification for faster delivery of public services, it must be kept in mind that the "mere storage and retention of personal data for unspecified purpose or without regard for informed consent is a violation of the right to privacy".[36] Whether such collected and stored information is used or abused afterwards has no influence on whether a violation of their right to privacy has taken place.

Under Rwandan law, the right to privacy is not absolute. Article 23 of the Rwandan Constitution states that "the privacy of a person, his or her family, home or correspondence shall not be subjected to interference in a manner inconsistent

36 *Leander v Sweden,* ECHR 4 (1987) para 48*; MK v France,* ECHR 341 (2013*); S & Marper v UK,* ECHR 1581 (2008), para 67 cited in CIS, 'Governing ID: Principles for Evaluation', March 2020 available on *https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity* (last access 20 August 2021).

with the law".[37] Although this constitutional provision remains too general as to the law it is referring to, it is worth mentioning that the law relating to access to information grants every person the right to access information held by a public organ and by some private bodies. This could be the case of any information associated with an individual's digital ID stored on the national ID database. Yet Article 4(3) of the same law (relating to access to information) protects any information that may involve "interference in the privacy of an individual when it is not of public interest".[38] It appears that from this provision's perspective, any violation of the right to privacy must pass the public interest test. In assessing this public interest aim, it is advisable to assess the necessity and the proportionality of any measure that may affect the right to privacy, at the same time. From the above example of automatic storage of digital ID information on the *Irembo* platform, while this is not a legal requirement, it is clear that such storage is not necessary. Since the aim of such collection and storage of information associated with individuals' digital ID is not clearly stated in the law governing ID issuance and population registration and, given that there is no specific law governing the use of digital ID, it is challenging to assess whether it is proportional.

3.2 DATA MINIMISATION

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

The law governing population registration and ID issuance does not clearly state the amount of information needed when an individual registers to request an ID. It rather lists information that will be printed on the ID card. Although no specific need for fingerprints has been found in the use of the national ID card, individuals are requested to provide their biometrics (both thumbprints and a face photograph) during their identity registration. The law is silent on the need to collect fingerprints, and data collectors do not explain to data subjects the purpose for which fingerprints are collected. It has been reported that fingerprints are collected as a way to avoid the same person being registered twice[39] and as a means to fight fraud. However, given the preliminary background check of individuals conducted from their village to the Sector where they are registered for the issuance of an ID card, the collection of fingerprints to avoid

37 Constitution of the Republic of Rwanda 2015, OG No. Special of 24/12/2015.

38 Law No. 04/2013 of 08/02/2013 relating to access to information, OG No. 10 of 11/03/2013.

39 ID4D, p. 25

fraud appears superfluous.[40]

Since registration in the national ID database is compulsory to primarily serve identification purposes, it is unclear whether there is a time limit for the retention of individuals' data by NIDA. Nevertheless, the question relating to how long after someone's death NIDA should keep their personal data in the database remains unanswered.

3.3 ACCESS CONTROL

Does the law specify access that various private and public actors have to personal data?

The interpreted purpose of the law governing population registration and ID card issuance does not allow *prima facie* access by various private and public actors to the personal and sensitive data collected and stored on the national ID database. While the Ministerial Order determining specifications of the national identity card for Rwandans and the fee related to national identification services does make a vague reference to getting "various services in public and private sectors" as one of the uses of the integrated smart card,[41] it fails to specify how this should be done. This arguably increases the risk to individuals in relation to the registration of their personal and sensitive information in the national ID database, which is accessible to many public and private institutions without a clear and binding legal framework.

3.4 EXCLUSIONS

Is the use of digital ID to access services exclusionary?

The Rwandan ID card is reported to be among the cheapest worldwide,[42] which should make it very accessible and affordable. A mechanism is also provided to ensure that the most vulnerable members of the community can obtain an ID

40 A WB-backed research confirmed that only less than 0.5% of cases of duplication has been detected within the national ID database during the registration process. The majority involved cases of legitimate errors, and not attempts at defrauding the system. ID4D, p. 25.

41 Article 12 of the Ministerial Order No. 02/07.01 of 04/09/2013 determining specifications of national identifications of the national identity card for Rwandans and the fee related to national identification services, OG No. Special of 13/09/2013.

42 It costs about USD 0.5 (FRw 500) to obtain an ID card. See Atick, p. 22.

card for free.[43] This is probably one of the reasons why more than 99% of eligible citizens hold an ID card.[44]

Of course, this must be contrasted with the number of individuals who can actually use a digital ID, keeping in mind the low levels of Internet access in the country, coupled with barriers like limited access to electronic devices and digital (il)literacy.[45]

The Rwandan national ID system was primarily developed to be used in its printed format or version as a physical ID card. In the 2000s, the Rwandan Internet infrastructure was not developed enough to envisage the widespread online use of a digital ID from the national ID database (and neither is it today).[46]

Today, however, the NIN printed on the ID card plays a paramount role in the implementation of a digitised ID system. This makes the Rwandan ID system a hybrid one that relies mostly on its offline use. To access public services, the service seeker has to use their NIN as a digital ID, because many government services have to be applied for online. This includes applying for things like civil status documents, travel documents, all applications related to citizens' identification (ID card, certificate of nationality, certificate of full identity, etc.), land-related transactions, applications for driving licenses and administration of traffic fines, the legalisation of documents by public notaries, applications for COVID-19 and yellow fever vaccines, the registration of NGOs and faith-based organisations, applications for a criminal record certificate, and the like.[47]

As the government is still working toward digitising the remaining public services, most other services still rely on a photocopy of a physical national ID as a proof of identity. However, the current exclusive use of the digital ID to request certain public services or products (such as passports, declaring taxes, etc.) may easily lead to delayed, denied, or restricted services or products due to poor Internet connectivity.[48]

43 Article 11 of Ministerial Order determining specifications of the national identity card for Rwandans and the fee related to national identification services.

44 Mukesha, p. 25.

45 Only 8.4% of Rwandans aged 15+ are computer literate. NISR 2015, p. 47.

46 In 2008, Internet penetration was reported to cover only 2% of the population compared to 9% in 2017. A. Gillwald & O. Mothobi, 'After Access 2018 – A Demand-Side View of Mobile Internet from 10 African Countries', RIA, April 2019, p. 17.

47 All these services are accessible through the Irembo platform (*www.irembo.gov.rw*).

48 Only 9.3% of households have access to the internet at home. See NISR, Rwanda Integrated Household Living Conditions Survey 2013/2014, Main Indicators Report, August 2015, p.67 [NISR 2015]

Does failure of the ID system lead to exclusion?

Internet use is very low (roughly 9%) in Rwanda.[49] This may cause significant risk to the use of data collected in the national ID database during system outages. On several occasions, people have reportedly missed deadlines to declare their taxes due to a system failure, for example. It is not possible to ascertain whether the failure was at the national ID database or on the revenue authority's website. It indicates, however, that failure to connect to the national ID database for one reason or another may lead to automatic exclusion from the services or products that the individual needed to use. The likelihood of such exclusion due to ID system failure is high for public services and products for which the use of digital ID is mandatory and offline/analogue alternatives are hard – if not impossible – to obtain. The problem is that the compulsion and deprivation of choice to use an alternative to digital ID (such as using a paper-based offline system) to access some public services is not supported by clear legislation.[50]

3.5 MANDATORY USE

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

The use of digital ID to access some public services has become compulsory through the *Irembo* platform. For instance, to request a passport and certain other important documents from public institutions, every person must initiate the request on *Irembo*. These services are not provided in person or in any analogue way. It is not clear which legislation made it mandatory to go through *Irembo* to have access to certain basic public services. It is only known that the *Irembo* platform – where the use of digital ID is required to access certain public services - is an outcome of a public-private partnership between the Government of Rwanda and RwandaOnline Platform Ltd, a private company.[51] Even though this platform has enabled businesses and individuals to digitally access and

49 Despite heavy investments by the government in the sector, only 9% of Rwandans are reported to use the internet mainly in Kigali. RIA, April 2019, p. 17.

50 It is contended that making access to public services and products dependent on the use and authorization of only one form of digital ID is a violation of "citizens rights to choose how to identify themselves to the government in a reasonable and non-intrusive fashion". Governing ID: Principles for evaluation, p. 22.

51 RwandaOnline Platform Limited Information, available on *https://rocketreach.co/rwandaonline-platform-limited-profile_b548103ff6a2bed1* (last access 20 august 2021).

pay for more than 80 public services, making enrolment to it the only option for public service recipients raises some concerns. It must always be borne in mind that "various benefits and services provided by the States are not State largesse or 'gifts' to citizens of a country".[52] Therefore, "making access to these benefits contingent on the use of and authorization on only one form of Digital ID violates these citizens' rights to choose how to identify themselves to the government in a reasonable and non-intrusive fashion".[53] In Robinson v the Attorney General of Jamaica, the Supreme Court of Jamaica ruled that "it is discriminatory to prevent citizens and residents using other means of identification in order to access public goods and services".[54] In the case of Rwanda, citizens who hold a valid ID card should be allowed, for the purpose of identification, to use their physical ID card or its copy to access public goods and services – as it was in the past – if they choose not to use their digital ID through the *Irembo* platform. The absence of any strong justification for the absence of such an opt-out provision is "not justifiable in a free and democratic society" and should be seen as unconstitutional.[55]

52 CIS, '*Governing ID: Principles for Evaluation*', March 2020, p. 22 available on *https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity* (last access 20 August 2021).

53 *Ibidem*

54 *Julian J. Robinson v The Attorney General of Jamaica*, [2019] JMFC, Para 346.

55 CIS, '*Governing ID: Principles for Evaluation*', March 2020, p. 21 available on *https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity* (last access 20 August 2021).

RISK-BASED TESTS

4.1 RISK ASSESSMENTS

Is this use case regulated taking into account its potential risks?

The Government of Rwanda is strongly promoting e-governance, with a paperless administration and cashless economy. This has resulted in many initiatives and support from the government to realise this vision, including the leading role that Rwanda plays in the Smart Africa initiative, which has a strong focus on digital ID. But there is no clear policy to raise awareness among citizens about the risks related to the use of digital ID.

As mentioned, Internet access levels are low in the country. About 42% of Rwandans do not own computers or smartphones that would allow them to apply for services or products online directly from their devices.[56] They therefore have to go to public access facilities like cybercafés or other "*Irembo* services providers" to apply for services when the use of digital ID is required. To do this, they need to give their NIN to the café staff or store it in the computer's cache. This bears a high risk of someone else having access to their NIN, which they can use to obtain the original user's personal and sensitive information from various government websites such as *Irembo*,[57] the tax authority's website, etc.

So far, it appears that risk related to the theft of personal data is not a primary concern of data subjects in Rwanda. Some people think that they do not have any information so private that they need special protective measures. This attitude is especially prevalent among women who perceive a low risk of misuse of their personal data.[58]

Is there a national data protection law in place?

When this report was completed, the law relating to data protection and privacy was a draft, that was waiting for its promulgation by the President of the Republic. It was eventually published on 15 October 2021. Due to time constraint, it was not

56 RIA, April 2019, p. 22.

57 Irembo is a platform where about 97 government services can be applied from using one's NIN (*www.irembo.gov.rw*)

58 GSMA, p. 50.

possible to make detailed analysis of this law. Nevertheless, it must be noted that despite its entry into force Article 67 of the law on data protection and privacy gives a moratorium of two years to existing data controllers and data processors to start complying with the provisions of this law. This means new data controllers and data processors who start operating after the law has come into force will have to comply with its provisions immediately after its publication in the Official Gazette.

The coming into force of this law is expected to substantially change the digital ID landscape. In fact, in addition to establishing an independent institution in charge of data protection and privacy, the law introduces a set of rights for the data subject and obligations for the data controller/processor. Regarding the rights of the data subject, it is worth mentioning that the right to information, the right to request that the data controller or processor stop processing personal data which may cause damage or distress, the right to rectification or erasure, and the right to data portability are some of the rights recognised in the new legislation.

The obligations or duties of the data controller and data processor include – among other things – the obligation to ensure that personal data are processed in accordance with the rights of data subjects and are collected for explicit, specified and legitimate purposes. It also imposes an obligation to perform a data protection impact assessment, an obligation to notify and report any personal data breach within 48 hours after having become aware of it to the competent authority, and an obligation to communicate a data breach to data subjects within 48 hours.

The entry into force of this law is a real game-changer for data protection in general, and especially for the protection of data related to the use of digital ID. But of course, this must be accompanied by robust efforts to not only build the capacity of newly established institutions but also to raise awareness among the public of their rights and obligations under the new law. This will ensure that the situation that prevailed before the enactment of the law is replaced by a strong data protection attitude and dynamics.

Are there privacy-by-design systems that minimise the harms from data breaches?

It is not clear whether privacy by design systems have been put in place to minimise harms from data breaches if they occur. Because the national ID database is a closed system in which only NIDA and its partner institutions have access to data, there is not much information about its built-in systems to mitigate risks following a data breach. This clearly highlights a lack of transparency that

makes it particularly difficult for data subjects to hold either the data controller or the data processor accountable should their privacy be breached. If the data subjects are not aware of digital ID's built-in systems, they can hardly take their own measures to prevent third parties and other actors from accessing their personal data stored on the population registry.

4.2 DIFFERENTIATED APPROACHES TO RISKS

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

There is currently no specific law governing the use of digital ID in Rwanda. Therefore, the assessment of differentiated approaches may not apply to the analysis of the Rwandan digital ID system.

4.3 PROPORTIONALITY

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

The absence of specific legislation governing digital ID in Rwanda, and the silence of the law governing registration of the population and issuance of the national identity card do not allow a proper assessment of proportionality between digital ID governance and the likelihood and severity of possible risks of its use.

4.4 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure or breach of the ID system?

Not much information is available about existing mitigation strategies in cases of failure or breach of the Rwandan ID system.

In 2017, the law on cybercrimes, aimed at helping the government to prevent

and fight online crimes and cyber-attacks, was gazetted.[59] Among other things, this law provides for severe penalties against people who cause failure or breach of online systems,[60] including the ID system. For instance, the law considers it an offence to cause, directly or indirectly, a degradation, failure, interruption or obstruction of the operation of a computer or computer system, or a denial of access to or damage of any program or data stored in the computer system.[61] The offender is liable to a maximum of five years of imprisonment and a fine that can go up to FRw 5 million (about USD 5 000).

59 Law No. 60/2018 on prevention and punishment of cybercrimes [Cybercrimes law).

60 Arts. 16-52 of the Cybercrimes Law.

61 Art. 20 of Cybercrimes Law

CONCLUSION AND RECOMMENDATIONS

The Rwandan ID ecosystem has been acclaimed as a "model for a robust, harmonized, and multi-element identity ecosystem, which provides several lessons that could be useful for other African countries".[62] Among other things, this acknowledgement is supported by the fact that more than 95% of the population is covered by the national population registry with an online identity verification.[63]

Rwanda issues a digital ID card with a 2D barcode, issued to every citizen in addition to an optional e-ID, which is offered to those who need and can afford it. The Government of Rwanda has put in place the *Irembo* platform, where various public services and documents can be requested and issued to citizens upon their identification through the unique NIN printed on the ID card. Other private entities, such as banks and telecommunication operators have also been granted access to the NPR database to facilitate the implementation of their KYC policies.

Over the years, the NPR and the NIN have undisputedly become the backbone of digital identification in Rwanda. However, the increased use of digital ID in Rwanda must be contextualised by the country's arguably deficient legal and institutional framework to guarantee the protection of personal data. In fact, the law governing the registration of population and the issuance of national ID, last amended in 2018, does not contain provisions that could be considered relevant to some key aspects of the current use of the ID and NPR. For instance, the law does not provide for the electronic use of the NIN as an identifier on a platform like *Irembo*, nor for the storage of personal population data in a digital registry and their access and processing by private entities, and neither does it provide for the rights of data subjects nor for the responsibility of NIDA and/or other data processors in case of data breach.

Despite some provisions in the ICT Law and the Cybercrimes Law that could be used to prosecute those who may violate personal data, the legal framework of the digital ID in Rwanda appears anachronistic and lacunary. There is therefore an urgent need to fill in the gaps by adopting a comprehensive law to regulate current and future uses of the national ID, especially online. The entry into force of the data protection law adds a critical layer in the protection of data in general. This effective implementation of the provisions of the data protection law

62 Atick, p. 5.

63 Atick, p. 4.

together with an adequate law on population registration, ID issuance, and the use of the national ID, will enhance the position of the Rwandan ID ecosystem as a model to inspire other African countries and beyond.

Based on the above discussion, the following recommendations can be formulated to policymakers in Rwanda to assure a robust and well-functioning digital ID system:

- Adopt policies and/or guidelines to ensure that the overall ID landscape is transparent and more protective of the rights of data subjects;
- Strengthen the current legal framework through the adoption of separate and specific legislation on the collection, storage and use of data collection during ID registration;
- Use this specific digital ID legislation to separate the role of the administrator, who is in charge of storage of personal data, and the role of the regulator, who licenses other agencies to perform registration and authentication responsibilities. The latter should also oversee complaints related to the breach of privacy from the population registry database.
- Conduct more campaigns to raise the awareness of government authorities at different levels and the population about the sensitivity and the risks associated with the use of digital ID. As people become more aware of the risks, they will be able to take appropriate measures to protect access to databases and to prevent risks that arise from breaches.
- Streamline the implementation of the law on data protection and privacy, which contains provisions that are relevant to addressing issues around the use of a digital ID. Specifically, prioritise the establishment of an independent authority in charge of data protection and privacy.

It is recommended to civil society that it should become more interested in the governance of digital ID. Rwanda is a country where many services are digitised and, given the propensity of the world to go digital, it is the responsibility of civil society to initiate research on the state of policies and laws regulating the use of digital ID in Rwanda in order to support the government. This will help to ensure that the government's vision to give Rwanda a paperless administration is not done to the detriment of people's constitutional rights and freedoms.

It is recommended that the private sector take necessary measures to ensure that they adopt internal rules and regulations that comply with their customers' data protection and privacy rights. Awareness should be raised in businesses that have access to the national ID database that they have a responsibility to take privacy more seriously and to ensure that personal data are not negligently processed. It is important for the private sector to remember that as their customers become more aware of the risks associated with sharing their

personal data with businesses, they will become more critical of those which do not take appropriate steps to protect their personal data and privacy. Therefore, businesses that delay in building their data protection and privacy frameworks may face clients' outrage in the long run.

To the donor community, the recommendation is to support in-depth research and programmes about not only the digital ID but also about the digitisation process in general. The world is migrating very quickly to digital everything, in some countries faster than others, particularly in the developing world. For an equal world, it is important that donors put the supporting developing countries high on their agenda, so that they can be equally ready to face and tackle challenges related to world digitisation, as well as to reap its benefits. In so doing, it is critical to keep an eye on issues related to individuals' rights and freedoms. The influence of digitisation on rights and freedoms should not be considered as marginal but rather as central for a successful digitised world.

REFERENCES

Law No. 14/2008 of 04/6/2008 governing registration of the population and issuance of the national identity card as amended to date, OG No. Special of 16/07/2008.

Law No. 43/2011 of 31/10/2011 establishing the National Identification Agency and determining its mission, organization and functioning OG No. 51 of 19/12/2011

Law No. 24/2016 of 18/06/2016 governing information and communications technologies, OG No. 26 of 27/06/2016.

Law No. 04/2013 of 08/02/2013 relating to access to information, OG No. 10 of 11/03/2013.

Law No. 32/2016 of 28/08/2016 governing persons and family, OG No. 37 of 12/09/2016.

Law No. 60/2018 of 22/08/2018 on the prevention and the punishment of the cyber-crimes.

Prime Minister's Order No. 83/03 of 08/10/2012 determining the competence, responsibilities and functioning of the board of directors of the National Identification Agency (NIDA) and the term of office for board members.

Prime Minister's Order No. 38/03 of 11/04/2014 determining the organizational structure and summary of job positions of the National Identification Agency (NIDA).

Ministerial Order No. 02/07.01 of 04/09/2013 that determines the specifications of the national identity card for Rwandans and the fee related to national identification services, OG No. Special of 13/09/2013

Gillwald, A. & Mothobi, O. (April 2019) '*After Access 2018 – A Demand-Side View of Mobile Internet from 10 African Countries*'.

GSMA (May 2019), '*Digital identity opportunities for women – Insights from Nigeria, Bangladesh, and Rwanda*', May 2019,

Atick, J. (2016), '*The Identity Ecosystem of Rwanda: A Case Study of a Performant ID System in an African Development Context*'.

Darrow, J. & Lichtenstein, S. (2008), '*Do You Really Need My Social Security Number – Data Collection Practices in the Digital Age*', 10 N.C. J.L. & Tech. 1.

Kayser-Bril, N. (2019), '*Identity-management and citizen scoring in Ghana, Rwanda, Tunisia, Uganda, Zimbabwe and China*', Algorithm Watch, 2019.

NISR (2015), *Rwanda Integrated Household Living conditions survey 2013/2014*, main indicators report.

'*Rwanda: Chamber of Deputies Adopts draft data protection law*', https://www.dataguidance.com/news/rwanda-chamber-deputies-adopts-draft-data-protection last accessed 10 May 2021.

S. Kemp, '*Digital 2021: Rwanda*' available at https://datareportal.com/reports/digital-2021-rwanda (last access 20 June 2021)
World Bank Group, *ID4D Country Diagnostic: Rwanda, 2016* available at https://thedocs.worldbank.org/en/doc/573111524689463285-0190022018/original/RwandaID4DDiagnosticWeb040318.pdf (last access 21 June 2021)

J. Mukesha, '*Rwanda National ID Agency*', ID4D available at https://www.id4africa.com/2019_event/presentations/PS1/5-Josephine-Mukesha-NIDA-Rwanda.pdf (last access 28 June 2021)

Julian J. Robinson v The Attorney General of Jamaica, (2019)

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. ■