



# Digital Identification Law in Kenya: **The State of Play**

Policy Brief No.5, August 2020  
Prof. Sylvia Kang'ara



# Digital Identification Law in Kenya: The State of Play

---



---

**Author:** Prof. Sylvia Kang'ara

**Edited by:** Grace Githaiga and Victor Kapiyo

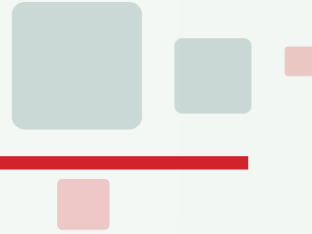
**Published by:** Kenya ICT Action Network (KICTANet) with support from Huawei.

**Design & Layout:** MediaForce Communications  
[www.mfc.ke](http://www.mfc.ke) | [@mfcafrica](https://twitter.com/mfcafrica)

---

© August, 2020 Kenya ICT Action Network (KICTANet)

# Table of Contents



A Executive Summary.....	2
B Introduction.....	3
C State of Play.....	7
D Policy Environment.....	11
E Legal Frameworks.....	15
F. Institutional Arrangements.....	28
G. Challenges.....	34
H. Conclusion.....	36
I. Recommendations.....	3

# Executive Summary



In 2018, Kenya launched a national digital identification system known as the National Integrated Identity System (NIIMS) and later as the Huduma Namba. It was initiated through Executive Order No. of 2018<sup>1</sup> and given legal effect through amendments to the Registration of Persons Act<sup>2</sup>. An Inter-Ministerial Coordination Committee on Huduma Namba was set up to steer the enrollment of the public among other functions. The process of enrollment began in early 2019. Subsequently, a lawsuit was filed challenging the constitutional validity of the legislation effecting NIIMS. After the preliminary hearing, the government was allowed to proceed with implementing NIIMS subject to limitations pending the hearing and final determination of the case. The judgement was delivered in January 2020 allowing Huduma Namba enrollment to continue subject to compliance by the government with the court's directives.

This brief discusses the policy and legislative framework for Huduma Namba. It highlights the issues that have arisen since its launch and the challenges the government has faced implementing the system, particularly the apparent disconnect between the National ICT Policy of 2019 which outlines the government's policies on digitization and integration of national population registers, on the one hand, and constitutional protections for privacy, data protection, security and inclusivity, on the other.

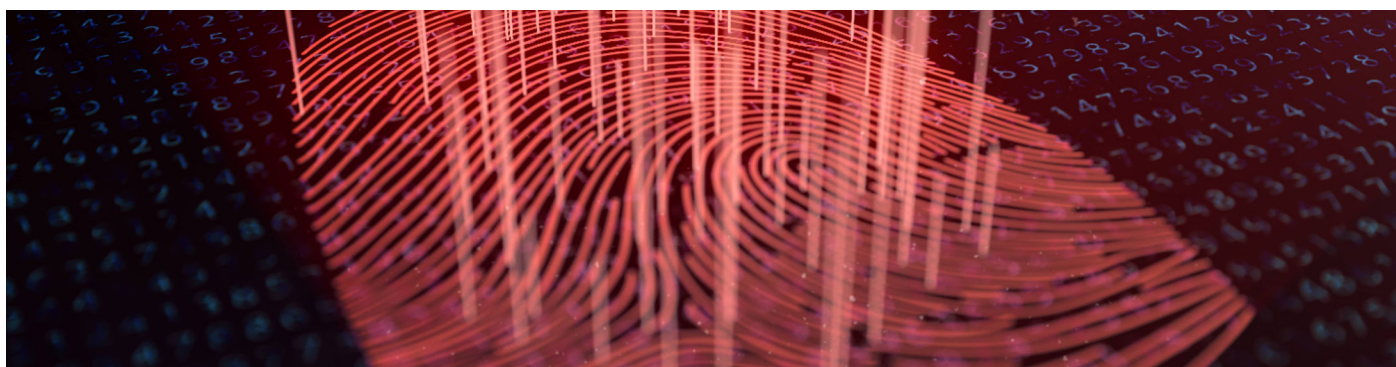
The key materials evaluated and analysed in this brief are government policy statements, relevant legislation and the documented evidence adduced in the Nubian Rights Forum Case by government officials, expert witnesses and citizen litigants. The review and analysis of these materials is done in order to identify the gaps in digital identification law in Kenya and to advise on how legal pitfalls may be avoided in future. The analysis also shows how the various pieces of legislation on digitization, registration of persons and data protection work together, the new obligations that arise as a result of new legislation and some of the administrative changes that new legislation will precipitate at the risk of legal liability for non-compliant entities. Given the fact of regional integration and globalization and the importance of digital identification in international governance questions, the brief also discusses the international laws and policies influencing decision-makers in this area.

The brief makes a number of recommendations, chief among them being the need to take into account and ensure compliance with the directives of the High Court. The Court made it clear that digital identification could not take place in a regulatory vacuum that lacked basic privacy protections for citizens and that also lacked an implementation strategy that installed key duty bears in Huduma Namba implementation. The required legislation will need to be passed, gaps in policy filled and vacant administrative positions filled.

---

<sup>1</sup> National Government Communication Centre, Brochure: NIIMS 2019 (26 June 2020, <http://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf>)

<sup>2</sup> Statute Law (Miscellaneous Amendments Act, 2018) <http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentsActs/2018/StatuteLawMiscellaneousNo18of2018.pdf>



Identification is the idea that information making up the legal identity of a person or entity should be so unique to that person or entity as to make them unique and distinguishable from others. When the distinguishing attributes are represented and utilized electronically, they no longer make up a physical form of identification but digital identification of the person or the entity.<sup>3</sup> Fingerprints or photographs taken on paper comprise the former but if the same are taken digitally they comprise the latter. Digital attributes may be stored and shared between electronic devices and processed as useful data by the same electronic mechanisms, and they are therefore preferred because they promote administrative and organizational efficiency.

Digital identity does not have to be represented as a person's real name as it can be a number, a nickname, a pseudonym, or a network address. However it is represented, it has legal, social, political and economic implications and is of foundational importance. Citizens are entitled to legal identity as of right which in turn enables them to participate in political exercises such as voting and economic activities such as concluding contractual agreements. Socially, legal identity may help establish affiliations, parentage, rights of inheritance and so on. The United Nations defines legal identity as the basic characteristics of an individual's identity. e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth.<sup>4</sup> It may also be conferred by a legally-recognized identification authority

Digital identity may be held by or assigned to individuals, groups, corporations and even equipment. It may be issued by the state, in which case it is issued to the entire or broad swaths of the entire population, or by a private entity whose coverage extends to a specific group for instance customers, employees or members of a club. Common examples of digital identification forms are: digital national ID cards, electronic passports, ATM cards, credit cards, business registration numbers, school identity cards. Some countries have allowed the use of mobile phones as a form of digital identity using their SIM Card technology.<sup>5</sup>

Kenya launched an electronic passport in September 2017 with the following

<sup>3</sup> International Telecommunication Union, Digital Identity, Roadmap Guide. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), p3 (29 May 2020, [https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU\\_eID4D\\_DIGITAL%20IDENTITY\\_ROAD\\_MAP\\_GUIDE\\_FINAL\\_Under%20Review\\_Until-05-10-2018.pdf](https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf))

<sup>4</sup> UN Legal Identity Agenda <https://unstats.un.org/legal-identity-agenda/>

<sup>5</sup> Countries where mobile phones are a form of digital identity.

features: “a contactless smart card (proximity card) chip and 13.56 MHz loop antenna embedded in the front cover page, in accordance with ICAO standards. The chip and antenna are not visually recognized, but their presence is indicated by ICAO biometric passport symbol at the bottom. It carries all the biometric data printed on the passport, JPEG file photo, digitally protected by a signature. Also an alphanumeric pseudorandomly assigned high-entropy serial number which is 45 bits. This improves the crypto-graphic strength of the basic access control (BAC) mechanism of the RFID chip, which makes brute force attack near impossible.”<sup>6</sup>



Creating a digital identity involves collecting personal information from individuals and creating an electronic record<sup>7</sup> of their attributes. The personal information data points all taken together should have sufficient detail and uniqueness to be the basis for creating distinguishable profiles capable of generating a unique digital identity. This unique digital identity is electronically assigned a unique number, in the case of NIIMS, the Huduma Namba.

Personal information is defined under the Access to Information Act No. 31 of 2016<sup>8</sup>, as “information about an identifiable individual”. The Act gives examples, including



(1) Any identifying number, symbol or other particular assigned to the individual



(2) Personal attributes such as nationality, race, gender, sex, marital status, ethnicity, religion, disability, language and birth



(3) Physiological attributes such as fingerprints and blood type; and



(4) contact details such as address and telephone number.

When it comes to government issued digital identification, the personal information

<sup>6</sup> Kenyan passport [https://en.wikipedia.org/wiki/Kenyan\\_passport](https://en.wikipedia.org/wiki/Kenyan_passport) (29 May 2020).

<sup>7</sup> Section 2 of the Access to Information Act defines an “electronic record” as “a record generated in digital form by an information system, which can be transmitted within an information system or from one information system to another and stored in an information system or other medium.”

<sup>8</sup> Section 2, Access to Information Act, No. 31 of 2016. (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=-No.%2031%20of%202016>).

attributes to be collected for purposes of issuance of national identity cards and numbers are prescribed by the Registration of Persons Act<sup>9</sup> which enumerates the personal information that must be submitted to the Principal Registrar whose mandate it is to create a national population register and issue identification documents. In the recent amendment to the Act which established NIIMS, biometric data, not just biographical information, was added to the list of personal information data that must be submitted by citizens and others eligible for registration under the Act.

The information in the national population register comprises the National Integrated Identity Management System from which, among other functions, the Principal Registrar will issue the two types of digital identification recognised under the Act - the Huduma Card and the Huduma Numba. Other statutes that prescribe personal information to be collected for purposes related to identity are: Births and Deaths Registration Act<sup>10</sup>, Citizenship and Immigration Act<sup>11</sup> and the Refugee Act.<sup>12</sup> These disparate registers will now be integrated under NIIMS to create the single source of information register and a single source of identification documents.

With the launch of NIIMS, personal information collected in the national population register will be integrated, centralized and linked to the various government agencies operating under these hitherto disparate departments. Registered persons will have a single identification document, the Huduma Namba and Huduma Card, serving multiple functions and their information will be verifiable and capable of authentication by various service providers. Consequently, under the Draft Regulations of the Registration of Persons Act specific to NIIMS, the government has adopted the data categorization of the International Telecommunications Union, namely, foundational data and functional data. Functional data is function specific data culled from foundational data held in NIIMS. Functional data is culled for a specific purpose concerning the work of a specific government agency. This distinction comports with the requirements of the Data Protection Act<sup>13</sup>, that personal data should be limited to purpose. It is also a data security strategy since the government designed NIIMS as a centralized database rather than the typically more secure decentralized database.

Although technology based services offered by the government can be issued without digital identification, those with digital identification are poised to enjoy the benefits of convenience. This convenience accrues only if the card readers and other equipment work properly and the data collected is accurate and relevant for the purpose it is needed. The information presented by the service seeker must be capable of authentication. Should this fail, what will be the solution given to the service seeker?

---


9 Section 9, Registration of Persons Act.

10 Births and Deaths Registration Act.

11 Citizenship and Immigration Act.

12 Refugee Act.

13 Data Protection Act.



The government plays a very important role as the provider of legal identity and actually enjoys a monopoly as a source of personal information related to identity. Given this monopoly, it is important that government systems work efficiently and without interruption. Kenyans might recall the failure of Biometric Voter Registration (BVR) kits during the 2017 general election and the confusion and anxiety that followed. No other institution can produce legal identity that has the backing of law, of legal institutions such as courts and private institutions such as banks when they open customer accounts, for example.

This brief gives a comprehensive overview of the policies, laws and institutions governing Kenya's nationwide digital identification system. It provides an assessment of the state of play, existing and emerging shortcomings, systemic risks and problems, gaps in the law and institutions and ends with recommendations.







Kenya now has a digital identification system anchored in the National Integrated Identity Management System<sup>14</sup> (NIIMS) which is a national population register and the primary source of information on personal information and identity. It is the system anchoring the issuance of a unique digital identification number and digital identification card. The randomly generated unique digital identification number, known as Huduma Namba, is being issued (or will be issued once legal bottlenecks have been resolved) to citizens and registered foreign residents who enroll in NIIMS. Those enrolled are also issued with a digital identification card known as the Huduma Card. The Huduma Card is issued to each individual and bears the Huduma Namba and other personal information prescribed by the Registration of Persons Act. The number and the card when authenticated against the biometric data held in the NIIMS shall be conclusive evidence of legal identity in Kenya.

The amendments to the Registration of Persons Act allowed the government to introduce a digital national population register as a “single source of personal information for all Kenyan citizens and registered foreigners resident in Kenya.” It also gave the government the mandate to “assign a unique national identification number to every person recorded in the register”. In digital form, the register would centralise all government held identification information currently in disparate registers and under disparate legislation making it possible for the government to collate the information for use in various ways at one go.

It is expected to harmonize all government databases containing personal information and make it possible for all identification documents to be issued from and verified by this one source. The range of documents to be issued, printed and distributed are national identity cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passports and foreign travel documents, student identification cards. This wide range makes the NIIMS administration an assembly line for verification and issuance of official documents prescribed by a range of statutes: the Registration of Persons Act, Citizenship and Immigration Act, Births and Deaths Registration Act, Basic Education Act, Traffic Act and any other statutory provisions enacted in future or approved by the Cabinet Secretary of the Ministry of Interior and Coordination of National Government. Enrollment in the national population register requires collection of personal information relating to biographical and biometric personal attributes. The Registration of Persons Act defines biometric data as “unique identifiers or attributes including fingerprints,

<sup>14</sup> Kenya's National Integrated Identity Management System. <https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68-25ef390170c3/briefing-kenya-nims-20190923.pdf>

---

hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form”.

In addition, the amendments allowed the government to collect and include in its register new types of identification information that it had not collected before, namely, biometric data and Global Positioning Systems (GPS) coordinates. Both were defined in the new provisions of the statute. Biometric as “unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form.” Global Positioning System Coordinates as “unique identifier of precise geographic location on the earth, expressed in alphanumeric character being a combination of latitude and longitude”.

Administrative responsibility for NIIMS lies with the Principal Secretary of the Ministry of Interior and Coordination of National Government. NIIMS is a centralized digitized database meaning that it is expected to be the single source of information and where possible the single source of government issued identification documents. As a digitized database that holds foundational personal data, it is set up to be the place for government agencies rendering services or carrying out other government functions can verify and authenticate identification information.

Although the government launched NIIMS in 2018 and started issuing digital identification numbers, in 2019 its constitutionality was challenged in the Nubian Rights Forum Case which was decided by the High Court in January 2020. The case brought to the fore the constitutional pitfalls of NIIMS, namely, whether as designed and implemented it had sufficient privacy, security and anti-discrimination safeguards for individuals, minority groups and even children, and whether sufficient public participation preceded amendments to the Registration of Persons Act that established it.

The Petitioners in this case were a minority group that has historically suffered discrimination accessing national ID cards and government services. The group was apprehensive that NIIMS would only exacerbate their exclusion from mainstream Kenyan society because their national ID cards were a precondition for enrollment in NIIMS and members of the group did not have these documents due to government inaction or deliberate exclusion or otherwise. Their petition further challenged NIIMS for introducing a regime of digital identification that authorised the Principal Registrar to collect citizens’ personal data, including sensitive data such as biometric data including DNA data and GPS data.

The High Court hearing the petition for interim orders in 2019 allowed the government to proceed with establishing the NIIMS and to collect data from citizens on voluntary non-mandatory basis, but it halted the collection of DNA information and GPS Coordinates, pending the final determination of the petition. The court also barred the government from transferring outside Kenya, any data it held until a comprehensive data protection and security law was passed. The Court rendered its final judgment on 30th January 2020. In the intervening period, the government launched a nationwide registration exercise that officially ended in June 2019. In November 2019, the Data Protection Act came into operation, meeting one of the conditions set by the Court was met.

In summary, the legal validity of digital identification programme launched as NIIMS rests on the following important conditions laid down by the Court:



### **1. Cessation of Collection of DNA and GPS Coordinates Data on Right to Privacy Grounds**

Collection of DNA and GPS coordinates from citizens and registered foreign residents for purposes of enrollment in NIIMS was declared unconstitutional. This means that these two data points will no longer be collected by the government. It is important to note that the government had not yet commenced collection of these two data types as it had not installed the facilities that would have enabled it to do so. The court disallowed collection of DNA and GPS coordinates on right to privacy grounds and gave the following reasons.



First, these two types of personal information data comprised sensitive information and collecting was intrusive.



Second, collecting DNA and GPS data was unnecessary to meet the purposes for which the government needed NIIMS and Huduma Namba.



Third, the collection of this sensitive personal data was not anchored on protective legislation.

Consequently, these three problems rendered the provisions of the Registration of Persons Act allowing the collection of these two types of personal data unconstitutional for being in violation of the right to privacy guaranteed under Article 31 of the Constitution. The Constitution at Article 2 provides that it is the supreme law of the land and therefore any legislation that is inconsistent with or that violates the Constitution must be declared null and void by courts.



### **2. Establishment of a Data Protection and Data Security Legislative and Implementation Framework as a Pre-Condition to Further NIIMS Enrollments**

The Court also found that the government launched NIIMS without an appropriate and comprehensive regulatory framework. This posed a risk to the security of data collected. To proceed, the government was directed to put in place a legislative framework that adequately protected the right to privacy guaranteed under Article 31 of the Constitution. The court found that the Data Protection Act that was enacted in November 2019 as the lawsuit was going on was still not adequate and there was still risk of unauthorized access to NIIMS data and therefore an ongoing risk to the right to privacy. For one, the Data Protection Act was not accompanied by statutory regulations to guide its implementation. Lacking an implementation framework, it purported to operate in a legislative and administrative vacuum.

The Data Protection Act also lacked adequate protections for children in that it failed to define who a child was for purposes of the NIIMS and also failed to provide adequate regulations for how biometric data of children would be collected, processed and stored in NIIMS.

The court pointed out that the Act provided that the Data Commissioner may exempt the operation of the Act and may issue data sharing codes to enable exchange of

personal data between government departments but without regulations to guide the Data Commissioner on this, there lacked an implementation framework for data security and protection. Furthermore, In addition to lacking regulations, the Data Commissioner had not yet been appointed. The registration of data controllers and processors had not been done. The Act was not enough as it needed operationalization, the court noted. Therefore, it did not matter whether NIIMS design was centralized or decentralized. What mattered was whether it had a “strong security policy and detailed procedures on its protection and security which comply with international standards”. The court asked the government to actualize in regulations the principles and standards for the operationalization of the system that would provide sufficient safeguards to protect fundamental rights. An adequate legal regulatory framework was necessary even if the government could demonstrate that it already had installed design measures such as encryption of and restricted access to data.



### ***3. Establishment of a Legislative and Implementation Framework to Ensure Inclusion and Non-Discrimination as a Pre-Condition to Further NIIMS Enrollments***

The court held that the government could make enrollment in NIIMS mandatory because digital data is indisputably the way of the future. However, the court noted that some may be excluded from enrollment and from receiving government services if they do not have national identity cards, which are a prerequisite to enrollment in NIIMS. Others may be excluded if they don't have good biometrics for instance if they don't have fingers or clear fingerprints. If NIIMS enrollment was mandatory and possessing Huduma Namba the means to obtain government services, the government should first establish a regulatory framework to ensure inclusivity and non-discrimination. This would require passing laws and regulations that cater to those who do not have national ID cards or those who have faulty biometrics. They should not suffer exclusion from NIIMS because of their documentary or physiological circumstances.

This then is the current state of play - NIIMS enrollment is on hold until the government establishes adequate legislative, regulatory and implementation frameworks for data protection and security covering adults and children alike in order to guarantee the right to privacy as required by the Constitution. The government is also to address any barriers to NIIMS inclusivity including by providing requisite registration documents to those who have experienced processing challenges before. It is worth noting that the government has recently circulated for public engagement, draft Regulations for the two statutes, the Data Protection Act and the Registration of Persons Act, in preparation for resumption of NIIMS enrollment. DNA and GPS Coordinates will no longer form the data points to be collected as doing so was declared unconstitutional. The Registration of Persons Act will have to be amended accordingly to comply with the court's order. When NIIMS enrollment resumes, it will be governed by these regulations and the Data Protection Act. The government has also recently scheduled interviews for recruitment of the Data Commissioner. It is expected that registration of data processors will also begin.

The long term effects of the partial launch of NIIMS will need to be considered from a point of view of costs, penetration, effectiveness and adoption of the system by the populace. The government should ensure compliance with the directives given by the court to avoid a second wave of litigation that might precipitate further delay.



# Policy Environment

D



NIIMS was designed by the ICT Ministry following the policy prescriptions of the draft National ICT Policy, 2016. Its design policy is centred on data centralization to promote efficiency in government service delivery. NIIMS as a centralized database was designed to be a single source of truth regarding identification information on citizens and registered foreign residents. In place of data protection and privacy, the design focused on risk mitigation. It failed for instance to differentiate between regular personal information and sensitive personal information such as DNA biometric data. It also did not have sufficient safeguards for children. This failure to give constitutional privacy rights upfront consideration led to the Nubian Rights Forum Case whose judgment in January 2020 put NIIMS enrollment on hold and now the government scrambles to put in place adequate data protection and security legislative framework as directed by the court. The court re-oriented NIIMS to a firmer and more explicit privacy policy framework as required by Article 31 of the Constitution which protects the right to privacy. Yet to be confirmed is whether NIIMS enrollment is going to be mandatory as the government has given contradictory communications and the Court did not direct that enrollment could not be made mandatory.

Efficiency and centralization are achieved in a number of ways. In place of the physical form national ID, citizens and foreign residents enrolled in NIIMS get a unique digital identification number (Huduma Namba) and a digital identity card (Huduma Card). The unique number and other prescribed personal information data are embossed on the card. National IDs have historically been issued under the Registration of Persons Act.



---

*Prior to NIIMS the government operated an Integrated National Population Register with everyone's biographical information. The government conceptualized NIIMS as a development of the pre-existing regime rather than a wholly new regime.*

---



---

As such it introduced NIIMS via amendments to the Registration of Persons Act and it is run under the same ministry, namely the Ministry of Interior and Coordination of National Government. However, the difference between NIIMS and the previous regime is that NIIMS will integrate the issuing of multiple identification documents that were hitherto issued by different government agencies and governed by different statutes, for instance birth certificates were issued under the Births and Death Registration Act and not under the Registration of Persons Act. NIIMS is poised to be an informational and administrative juggernaut. Huge bureaucracies tend to be inefficient and expensive. This is a policy challenge quite separate from the legal challenges discussed above. It can only be addressed at the policy level.

The newness of the system presents unique challenges, given the nature of the system, permanency, and its long term effects which may be difficult to undo once the system is in place. On the one hand, it may be argued that digital identification is not new since the government has been registering persons and issuing identification documents and what is changing is the form legal identification is taking. On the other hand, while it is true that the government has always been a registration and identification provider, digital identification changes the nature of state-citizen relationship. There is an undeniable shift of the balance of power that radically favours the government over the citizens. The old is new in that respect. The government's policy to see NIIMS as a mere continuation of its registration of persons programmes failed to appreciate that governance effects were new. Collecting biometric personal information may appear to the government as an efficiency and cost improvement, but to the citizen it is a new layer of power that the state acquires over the citizen.

Furthermore, path dependence and contextual givens might mean context will influence implementation of Huduma Namba. This raises questions as to whether context should not be taken into account by designers and re-designers of the system to take into account existential risks such as corruption, old dictatorial regime tendencies, wastage and so on. Reason being, there is a need to preempt challenges that may arise as a result of problems already entrenched in society that will undoubtedly infiltrate the system and negatively affect its performance. Conversely, a system that is not cognizant of contextual complexity will no doubt suffer a legitimacy and uptake crisis. For instance, Kenya has heightened rights awareness among citizens coupled with deep suspicion of the government. This is bound to make adoption of digital identification in Kenya different from that in any other country. Accordingly, choice of identity authentication and verification models and institutional frameworks put in place to implement the system should be context informed. It is not advisable to follow foreign models blindly.

Timing is an important design and implementation policy question. For example, how long will it take to create and implement the digital identification system from beginning to end? How long does it take to get to the point where assurances can be given regarding its efficacy and safety of the system? What timing considerations should be given to political headwinds and contextual challenges, and how much preparation should there be pre-launch? Given that Kenya has experienced these challenges, one detects defects in the governments design and implementation policy for NIIMS. This is attributable to the fact that the government did not from the outset have a comprehensive policy document on NIIMS. Instead, it tucked NIIMS in existing ICT Policy and population register policies not seeing NIIMS as a far reaching intervention requiring its own comprehensive policy. The government issued a short



Huduma Brochure in 2018, which is hardly a comprehensive policy.<sup>15</sup>

Necessity is a strong argument for the introduction of digital identification. The idea that we live in a digital age and that the global economy is increasingly a digital economy based on digital societies seems to leave little or no room for choice as to whether Kenya or any other country should or should not adopt a national digital identification system. All that is left is room to determine the depth, scope, purposes and design of the system. This is in spite of the financial cost involved in its set up, implementation, maintenance and management.

It would be foolhardy to think that the digital identification system will not have challenges and will not need to be adjusted and refined through the course of time. Digital technology is in a constant state of change; the challenges of newness will never go away. And this means that there never can be a perfect system. The baseline characteristics of NIIMS should be reasonable functionality, adaptability and flexibility rather than perfection. A policy gap at the moment is that given this uncertainty inherent in rapidly changing technology and contexts, effective and continuous communication to stakeholders and the public has not been embraced as a critical success factor of the digital identification system at all its stages, from formation to implementation to adjustment to inevitable replacement in future. Witness testimony in the Nubian Rights Forum Case reveals that NIIMS is to assist the government in certain law enforcement agenda. Does the combination of registration and law enforcement functions cause anxiety in the public's perception of NIIMS? An effective communication policy seems necessary to promote appreciation and lessen apprehension of the government's intentions for a multipurpose system such as this one.

Digital identification in Kenya is based on the National ICT Policy of 2016<sup>16</sup> developed by the Ministry of ICT. Digitization is an important policy objective of the government. Digital identification is but a segment of the overall policy. A broader objective is to further economic development by encouraging the development of digital economies and electronic commerce. An e-government platform is expected to make government more efficient, result oriented, cost efficient and citizen centred. Efficiency in service delivery is a centerpiece of the government's digitization policy. Government services have been automated. Huduma Centres have been established throughout the 47 counties as one stop centres for citizen access to all government information and services.<sup>17</sup> According to evidence adduced by the government at the Nubian Rights Forum Case hearing, citizens who have been registered in the NIIMS and received a Huduma Numba will receive government services at Huduma Centres more efficiently than those who do not. The initial plan was to make digital identification mandatory but the government seems to have backed off from that following the court order in the Nubian rights case.

The National ICT policy also emphasizes establishment of a National Addressing System. The plan to collect individual GPS coordinates was said to advance this policy. GPS data was however not collected and will now not be collected following the court's directive. Alternative data will need to be used to create an addressing

---

<sup>15</sup> Huduma Brochure (see brochure footnote below).

<sup>16</sup> National Information and Communications Technology (ICT) Policy, issued by the Ministry of Information Communications and Technology in June 2017.

<sup>17</sup> In 2014 the government established the governance structure for Huduma Kenya Service Delivery Programme. Gazette Notice No. 2177, 4 April 2014 ([http://kenyalaw.org/kenya\\_gazette/gazette/notice/143142/](http://kenyalaw.org/kenya_gazette/gazette/notice/143142/)).

---

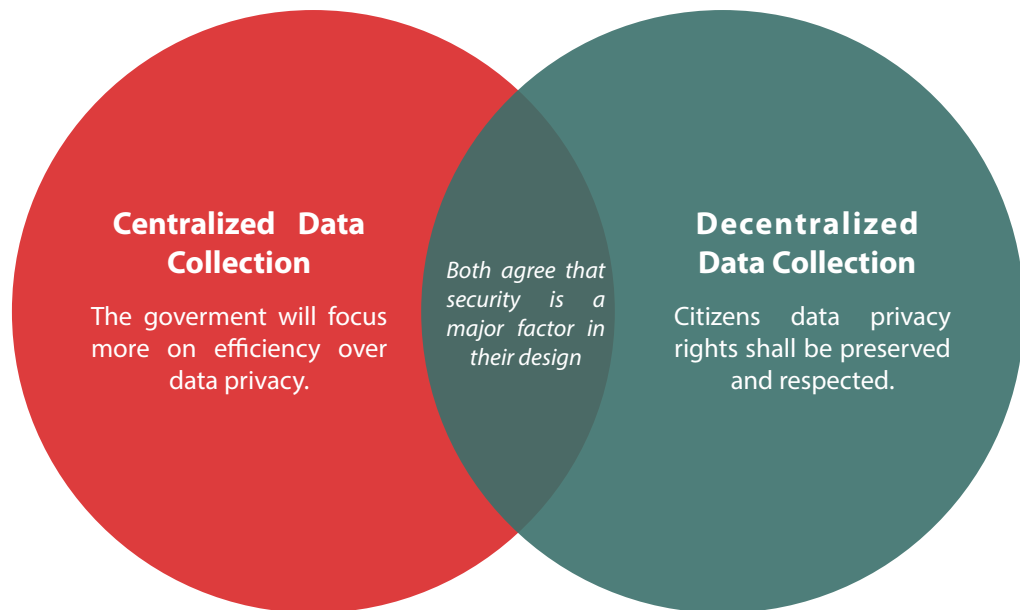
system. The multiple functions NIIMS was conceived to play beyond identification will need to be reviewed for compatibility and their legality reassessed.

In addition to efficiency in service delivery through E-Government, the national ICT Policy focuses on Big Data, E-Services, Electronic Commerce, Security including Cyber Security, National Security, Network Security and Information Security, and these relate to digital identification according to the evidence rendered in the Nubian Rights Forum Case.

The ICT Ministry is a service ministry in that it provides digital infrastructure to the Ministry of Interior and Coordination of National Government to carry out registration and issuance of digital identification and make the linkages necessary for digital verification and authentication of identity across government departments. Digital infrastructure also makes it possible for identification information to be collated, processed, distributed, and used in various ways. Identity information collected may be processed to assist decision making of various types, for instance, regarding allocation of resources and provision of social and economic services such as health and education, and therefore supports further implementation of government policy as charged to the various ministries.

Two design policies stand in contention among computing experts. The one adopted by the government favoured centralization of data, meaning that NIIMS was designed to be a centralized database that would be the single source of truth on personal information of citizens and resident foreigners. Government departments will be linked to the central database to extract only the information they require to deliver services to citizens. Information on NIIMS will be collected at birth registration and children linked to their parents on the system, however the biometric data of children such as digital fingerprinting will begin at age six. Efficiency is the key policy reason for the government's preference for data centralization. The efficiency benefits justifying this are that NIIMS information is reliable compared to when personal information is carried in different government registries. There are also cost efficiencies in addition to national security benefits, related to crime prevention and anti-terrorism strategies, gained from having a dependable, retrievable and collatable registration system.

The data centralization approach taken in design of NIIMS shows the government's almost exclusive focus on efficiency over data privacy concerns of citizens in its design policy. The alternative to data centralization is decentralization. Proponents of decentralization argue from a policy position of minimizing harm that may arise should there be a security breach in the system. Both camps agree that security threats cannot be entirely prevented no matter the design chosen but the possibility of them occurring and their effects if they occur can be minimized. When all data is in a central database, the central database will attract data heists because big data is especially attractive to criminals. Advocates for the right to privacy are concerned about surveillance by the state or state agents, and this is all the more a threat with centralized databases.



*Proposed Design policies for computing the data for NIIMS by Computer experts*

The government's data collection programme under NIIMS was conceived to be broad in scope of data that is collected. The Data Protection Act was enacted after NIIMS had been designed and launched. It has added missing scope limitations, for instance, that data collected had to be limited to a specified purpose. Without restrictions on what data the government can collect and how it can use it, citizens are left vulnerable to not just administrative failure and data leakage but also to state surveillance.

Finally, the government holds a policy against involving foreign entities in the design of critical infrastructure. This was followed in the design of NIIMS. Registration kits were however supplied by a foreign supplier but were checked for compliance with the government's digital security policy.



MILIMANI LAW COURTS





Kenya's digital identification legal framework sits in a number of legislation and judicial decisions. The provisions of the Bill of Rights of Constitution<sup>18</sup> provide robust protections for the right to privacy, right to information, right to fair administration, right to citizenship and right to equal protection of the laws and anti-discrimination. Parliament has enacted legislation to implement these constitutional provisions. NIIMS was introduced as an amendment to the the Registration of Persons Act, an old statute that preceded the new Constitution of 2010, but which must now be read and implemented within a new constitutional framework that has rights implementing statutes. Consequently, this regulatory context imposes new demands on how the state carries out its mandate of registration of persons be it in the design of registration programmes or digitizing fingerprints or introducing new identification technology such as face recognition which could happen in future as has happened in some countries such as China. The Constitution overrides any provisions of any legislation that conflict or are inconsistent with it.



## 1. Right to Privacy

The right to privacy under Article 31 of the Constitution protects citizens from suffering the indignity of unlawful exposure or disclosure of intimate details about them or their families. Personal information collected during NIIMS enrollment is therefore protected by the right to privacy which empowers citizens to exclude the government and others from their private lives and affairs, and from obtaining details about their private life and their person. Article 31 therefore places legal obligations on state officers such as registrars and others charged with operating the NIIMS

<sup>18</sup> Constitution of Kenya, 2010 (26 June 2020, [18](http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Con-2010;Constitution of Kenya; Protection of Rights and Fundamental Freedoms) Practice and Procedure Rules, 2013,</a></p></div><div data-bbox=)

system to obtain consent or lawful authority to collect and process information about persons, their family, and private affairs. The information should not be unnecessarily required or revealed. The privacy of their communications should not be infringed. The state should not use information contained in such communication except with their consent or under lawful authority.

The Registrar can only require information about a person when it is necessary to meet the requirements of the Registration of Persons Act. It would be unlawful to require more information than prescribed by the Act. Only designated agents authorized by the registrar should collect the information and they too have an obligation not to reveal it or share it with others unless it is necessary and authorized in the course of their duties.

Article 31 does not impose an absolute ban on the state obtaining personal information or sharing it across state departments and agencies. It however sets a bar of necessity and an obligation of data protection on the state. NIIMS is designed for information collection, permanent storage and sharing within a linked government network. This shift to digital collection, use and sharing of personal information increases the state's data privacy and protection obligations. These obligations are now contained in the Data Protection Act of 2019.<sup>19</sup> Even though NIIMS was designed and launched before this statute was enacted, the system must now be operated in compliance with this statute. Furthermore a draft bill on data protection regulations relating to civil registration<sup>20</sup> is now in circulation for purposes of public engagement and eventual consideration and enactment by Parliament. Once it becomes law, compliance by NIIMS administrators will be required.



## 2. Right of Access to Information

The Constitution at Article 35 further guarantees the right of access to information. This constitutional right has been subsequently reinforced in various statutes including the Access to Information Act No. 31 of 2016,<sup>21</sup> enacted precisely to implement Article 35, and the Data Protection Act 24 of 2019. To comply with Article 35 and related statutory provisions, state officers in charge of digital identification services must allow citizens to have access to information held by the State as well as information

<sup>19</sup> Data Protection Act No. 24 of 2019 (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019>).

<sup>20</sup> Data Protection Act (Civil Registration) Regulations, 2020 (draft) (<https://www.interior.go.ke/wp-content/uploads/2020/02/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-2020.pdf>).

<sup>21</sup> Access to Information Act No. 31 of 2016 (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016>).

that the officers have allowed another person to possess, such as a contracted data processor, so long as the information is “required for the exercise or protection of any right or fundamental freedom”. Article 35 further provides that “every person has the right to the correction or deletion of untrue or misleading information that affects the person”. Since NIIMS is a personal information database, the ministry in which it is housed will need to develop regulations on how right to information requests will be handled when the requests are made by someone other than the owner of the information. Right to information requests that concern sensitive personal information will need special processing protocols.

The Access to Information Act No. 31 of 2016<sup>22</sup> requires public entities, and the NIIMS administration is such one, to keep and maintain accurate records in a manner that makes it possible for citizens to exercise the right to access information. Records may be kept electronically as is envisaged under NIIMS. Limitations to the right to access information abound however. The Data Protection Act only covers personal data and grants the right to access and to control its use. The Access to Information Act, on the other hand, covers all information held by public entities and private bodies whether personal or not. A citizen seeking access to information from the Principal Registrar or data processor or other related entity may face limitations if seeking access to information has nothing to do with personal data at all. An example of such information could be business records of the Principal Registrar’s office sought by a citizen who has sued to challenge an adverse automated administrative decision by the office or its agents.

The Access to Information Act defines personal information in broad terms. Worth noting is that the definition includes information that would be collected for digital identity purposes: “any identifying number, symbol or other particular assigned to the individual;” and the fingerprints, blood type, address, telephone or other contact details of the individual”; in addition to information regarding a person’s natural biological attributes such as race and gender. The legislative purpose of this statute is to promote disclosure and transparency institutional practices. This orientation is not in conflict with the other discussed namely, data protection and security. The Access to Information Act does not permit disclosure that involves “the unwarranted invasion of the privacy of an individual, other than the applicant or the person on whose behalf an application has, with proper authority, been made.”

Furthermore, like the Data Protection Act, this statute requires public entities and private bodies to correct, update or annotate personal information they hold once an application is lodged with them. In a sense, such corrective applications may be about protecting privacy or may be about encouraging disclosure of only accurate information in line with legislative intent.

---

<sup>22</sup> Access to Information Act No. 31 of 2016. (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016>).



### **3. Right to Equal Protection & Anti-Discrimination**

While legal pitfalls abound for digital identification programmes that lack sufficient privacy and security safeguards, the government must not refuse to issue legal identification documents on equal terms to all eligible persons. The Constitution under Article 12 provides that every citizen is entitled to “a Kenyan passport and any document of registration or identification issued by the State to citizens”. The Constitution also requires Parliament to pass legislation for the registration and documentation of eligible non-citizens, which it has done by passing the Kenya Citizenship and Immigration Act No. 12 of 2011<sup>23</sup> and the Kenya Citizens and Foreign Nationals Management Service Act No. 31 of 2011. The Constitution at Article 27 prohibits discrimination by the state and private persons. The significance of a non-discriminatory national digital identification document is clear when one considers that it could soon become the only document for accessing services, information, opportunities, social and economic rights under Article 43, disability rights under Article 54, minority rights under Article 56, elder rights under Article 57 and youth rights under Article 55, and may be even voting rights guaranteed by Article 38.

Consequently, sufficient thought must be given to strategies for enhancing adoption of digital identification to ensure digital inclusiveness across the 47 counties. The Constitution at Article 6 provides for devolution and access to services. It requires state organs to ensure reasonable access to services in all parts of the Republic “so far as it is appropriate to do so having regard to the nature of the service”. In the same vein, Article 10 binds all state organs, state officers, public officers and all persons to the national values and principles of governance which include inclusiveness, equality, human rights, non-discrimination, transparency, accountability and sustainable development.

---

<sup>23</sup> Kenya Citizenship and Immigration Act, 2011 (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2012%20of%202011&term=birth>) and Kenya Citizenship and Immigration Regulations, 2012. (<http://kenyalaw.org:8181/exist/kenyal-ex/sublegview.xql?subleg=No.%2012%20of%202011>)





#### **4. Right to Fair Administrative Action**

The Fair Administrative Action Act No. 4 of 2015,<sup>24</sup> implements Article 47 of the Constitution which guarantees the right to fair administrative action. To comply with the Constitution, an agency or department making administrative decisions regarding digital identification must provide written reasons to a citizen whose rights or fundamental freedoms are affected by its decisions. Moreover, the decision making process must be conducted in an expeditious, efficient, lawful, reasonable and procedurally fair manner. An example of an adverse administrative decision that would require communication of reasons in writing is a decision to deny or cancel a digital identity document so making it impossible for the citizen or eligible person to access services or opportunities, for instance employment or monetary payment. The Constitution provides that administrative actions are reviewable by a court or a tribunal, and therefore provides a rights enforcement mechanism in addition to others discussed here provided by other statutes.

The Act's definition of administrative action fits the type of work done and decisions undertaken by various offices charged with the mandate of providing digital identification. This work involves registration and data processing, for example the Principal Registrar under the Registration of Persons Act and the Data Commissioner under the Data Protection Act. The Act defines administrative action as "the powers, functions and duties exercised by authorities or quasi-judicial tribunals; or any act, omission or decision of any person, body or authority that affects the legal rights or interests of any person to whom such action relates." The definition is broad enough to include private data processors that might be contracted by the Principal Registrar to carry out data processing under the NIIMS. Upon successful petition for judicial review of administrative actions, a court or a tribunal may revoke decisions made or order the Principal Registrar to act in a particular manner, for instance, issue a digital identification card to make it possible for the aggrieved person to access services or opportunities.

---

<sup>24</sup> Fair Administrative Action Act No. 4 of 2015 (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%204%20of%202015>).



## 5. Data Protection and Data Security

The Data Protection Act No. 24 of 2019<sup>25</sup> is a general statute regulating the handling of all personal data. Data collected for purposes of issuing Huduma Namba will typically be personal data and in some cases will also be sensitive personal data, and therefore will be governed by the Act. This new law significantly affects the legal validity of digital identity under the NIIMS/Huduma Namba registration system introduced by the government in 2018. The provisions of the Act affect the long term implementation and development of NIIMS in a number of ways.

To start with, the Act brings the administration and management of registration of persons under the oversight of the Data Protection Commissioner. Under the Registration of Persons Act, the Principal Registrar has the mandate to maintain a register containing personal information details prescribed by the statute. In the statutory scheme of the Data Protection Act, the Registrar would qualify for the designation of a Data Controller, defined by the Act as a “natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data”.

Then it defines personal data as “any information relating to an identified or identifiable natural person” and further defines biometric data as a type of personal data “resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.” The Act also recognises and defines health data and “sensitive personal data”, defining the latter as “data revealing the natural person’s race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of person’s children, parents, spouse or spouses, sex or the sexual orientation of the data subject.”

The Act regulates the processing of personal data that is “entered in a record, by or for a data controller or processor, by making use of automated or non-automated means.” This accurately describes the work of the Principal Registrar under the Registration of Persons Act. As data controller, the Principal Registrar may engage a data processor, defined by the Act as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.” The data controller and data processor cannot operate unless registered by the Data Commissioner upon meeting the registration requirements of the Act.

<sup>25</sup> Data Protection Act, No. 24 of 2019 (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019>).

---

The Act requires data controllers and data processors to abide by principles and obligations of personal data protection, failing which their certificate of registration may be varied or cancelled by the Data Commissioner. To comply with the Act, the Principal Registrar and her data processors are required to handle personal data in a manner consistent with the principles of data protection enumerated in the Act.

Data subjects under the Registration of Persons Act are the persons eligible for registration and identification documents. The Act accords them data subject rights which the Registrar, staff of the Registrar, and data processors contracted must respect by taking affirmative steps, such as informing the citizen of the use to which their personal data is to be put, or by refraining from doing something such as processing all or part of personal data if the citizen objects. In addition data controllers and data processors must collect data directly from a person unless it is permissible to collect data indirectly. They also must adhere to the “duty to notify”, which is a requirement to inform the person that personal data is being collected and for what purpose, as well as their rights to data protection. As such the point of contact and interaction with citizens and other persons eligible for registration is regulated by statutory collection protocols protecting the data subject.

After data collection protocols are observed, the data controller and processors must observe regulations about lawful processing of personal data (processing protocols, we might label them). They must establish consent to process, carry out impact assessment if necessary in high risk cases, and then determine that the processing is necessary and if so, ensure it is done for the purpose for which the data was collected. Furthermore, the Act allows the data subject to place restrictions on the processing of their data if the data is inaccurate, contested, unnecessary, or if the data subject has objected to the processing. The data subject may request that the data held be rectified or erased and not processed. Additional processing protocols must be observed for sensitive data and health data. Finally, the Principal Registrar is exempt from the Act’s restrictions where processing of personal data is necessary for national security, public interest or authorised by written law or court order. There are also exemptions related to journalistic, literary, artistic use and uses related to research, history and statistics.

A third set of regulations, we might call them use protocols, regulate how data controllers and processors use and store data they have collected or processed. The Act prohibits automated decision making and profiling that “produces legal effects” concerning or significantly affecting the data subject that would be impermissible under the Act. The Act also prohibits commercial use of data without express consent or written legal authority, and even where allowed, data for commercial use is to be anonymised. How the government uses NIIMS data is going to be affected by these rules. For example using the data to profile citizens may advance a policy objective of service delivery but it should not be done in a way that violates the protections given by the Act.

A fourth set of regulations, we might call them data control and ownership protocols, allow the data subject to continue to have a say on how the data controller and processor handles their data well into the future. The Act grants data subjects a right to data portability. This is the right to receive the information collected in a readable format and the right to transmit or to have it transmitted. In addition, the Act limits

the retention of personal data by data controllers and processors beyond the period of its purpose. In our case, the Principal Registrar bears an obligation to delete, erase, anonymise or pseudonymise personal data that is not necessary to retain. Data subjects have a right to request the Principal Registrar to rectify, erase, or destroy data in their possession.

The Act imposes conditions for transfer of data out of Kenya. The Principal Registrar would need the approval of the Data Commissioner to do so after establishing that sufficient data protection safeguards exist. Alternatively, the Principal Registrar may transfer personal data out of Kenya if necessary, and the Act prescribes on such necessity. Sensitive data may not be transferred without the consent of the data subject. The Act imposes limits on commercialisation of data alongside the limitations on transfer of data out of Kenya. Law has long considered information and news to be property, albeit of shifting value with the passage of time. With the advent of Big Data, data has also come to be commercialised and arguments abound that data is now a form of property. The salient question is who owns it? Does the data subject own their data? Whatever the case as each situation might present different circumstances and conclusions, the Constitution at Article 40 provides that “every person has the right, either individually or in association with others, to acquire and own property”. Some countries have introduced digital identification cards that are machine readable just like credit cards while others have adopted mobile phone devices as a form of digital identification that citizens use to verify and authenticate their identity in order to access government services and complete transactions with non-governmental service providers. Canada’s digital identification key was developed from data already given to banks by citizens. These examples show a trend towards merging legal identity and commercial activities, making urgent the question whether exclusive property rights over personal data remain with the citizen or are taken over by other participants in their digital village.

A fifth set of provisions under the Act, we might call them enforcement protocols, stipulates what is to happen in the event of personal data breaches and also stipulates remedial measures. In the event of breach, the Principal Registrar will be required to notify the data subject and the Data Commissioner of the breach within prescribed timelines. The written notification must provide sufficient information to enable the data subject to take protective measures. The Data Protection Act prescribes data protection by design or by default, which is the requirement that the data controllers and processors should implement appropriate technical and organisational data protection measures.

On data security, the Computer Misuse and Cybercrimes Act No. 5 of 2018<sup>26</sup> prescribes criminal penalties for actions including or culminating in theft of data that also lead to physical, economic or emotional harm against the data subject because of harmful use of the data stolen. This Act therefore complements the enforcement provisions of the Data Protection Act and other statutes discussed here. The Data Protection Act for instance, requires data controllers and processors to report data breaches, which would in turn trigger prosecution under the Computer Misuse and Cybercrimes Act if criminal culpability was established. The Act imposes criminal penalty for the crime of identity theft and impersonation by providing at Section 29 that “a person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and is

<sup>26</sup> Computer Misuse and Cybercrimes Act No. 5 of 2018 (<http://kenyalaw.org/8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018>).

liable, on conviction, to a fine not exceeding two hundred thousand shillings or to imprisonment for a term not exceeding three years or both.”

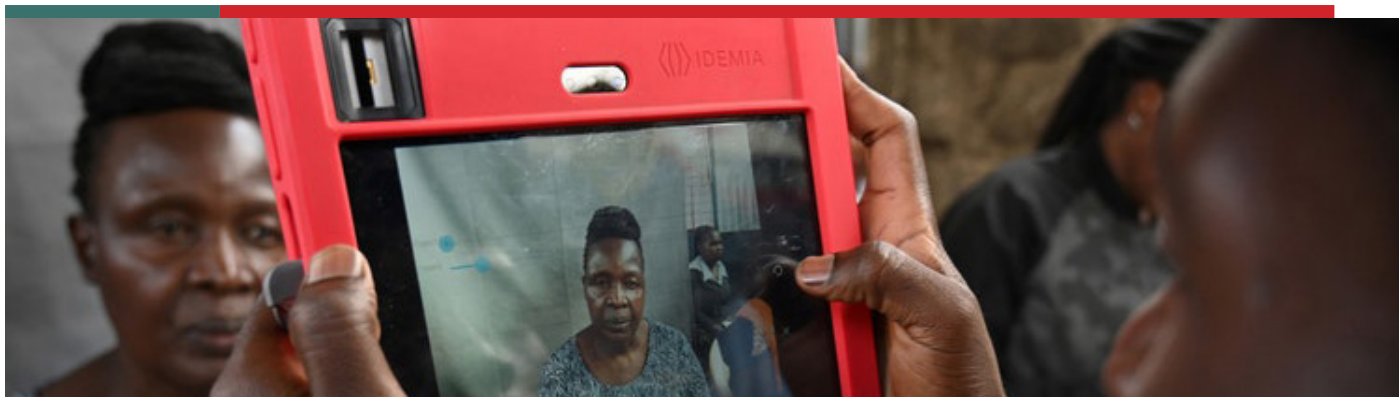
This Act protects the integrity of computer systems, programs and data, and the rights to privacy and access to information guaranteed in the Constitution, in addition to facilitating international cooperation on matters of cybersecurity. Besides criminalizing identity theft and impersonation, the Act further protects digital identification data systems such as NIIMS by establishing the following as crimes punishable through criminal penalties: computer forgery, computer fraud, fraudulent use of electronic data and cyber espionage.

The Kenya Information & Communications Act<sup>27</sup> establishes the Communication Authority which among other functions licenses and regulates providers of information and telecommunication services in line with government policy. At Section 27D the Act lays down the requirement for regulations on SIM-card registration, confidentiality and disclosure of subscriber information, deactivation of SIM-Cards, among other regulatory considerations. The Act also provides for the regulation of electronic transactions and certification of digital signatures. Coupled with provisions of law regulating banks and other financial institutions, these provisions on telecom regulation are critical to the growth, expansion and inclusiveness of digital identification systems, of course depending on the method of authentication chosen for the country now or in future.

Contract law and the use of digital identification in contracting. Public digital identification is the kind used by the government under the Registration of Persons Act. Private identification is the kind used by private parties to provide contractual or proprietary rights, for instance rights to access a building or transfer money or conclude an electronic transaction using a digital signature. Private digital identification, being based on contract, which is considered naturally consensual as well as commercial, has not attracted as much controversy as the public digital identification regime which relies on state fiat. Contractual digital identification however raises questions of non-consensual data mining and commercialisation without the consent of data subjects. The Data Protection Act covers both public and private digital identification questions.

---

<sup>27</sup> Kenya Information & Communications Act (<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%201998>); Kenya Information & Communications Act Subsidiary Legislation (<http://kenyalaw.org:8181/exist/kenyalex/sublegview.xql?subleg=No.%202%20of%201998>).



## 6. Registration of Persons Act and the New Draft Regulations

The Registration of Persons Act,<sup>28</sup> creates the office of the Principal Registrar who is mandated to create a national population register containing prescribed identity and profile markers of all persons eligible for registration. Citizens have a right to registration documents as do legally eligible foreign residents. The government has an interest in knowing who is within its borders for reasons of planning for service delivery, national security, crime management and prevention, taxation, voting, among other governmental functions. At the same time citizens not only have a right to registration documents but to government services typically accessed after production and verification of documents showing status and eligibility to receive the service sought. In addition, the government has special specific duties it owes citizens that it may not owe non-citizens. The only way individuals can enjoy rights conferred by nationality and citizenship is through national identity cards and passports. The Registration of Persons Act governs and regulates the issuance of national identification cards. There are other registration statutes discussed below but they serve other documentation purposes not provision of national IDs. Under NIIMS, these other documents will be issued from the same database.

Kenya is in the process of transitioning from physical form identification cards to digital identification cards. Up and until 2018 when this Act was amended to introduce the NIIMS/Huduma Namba digital identification regime, physical form registration and identification cards was the regime used by the government as established in the Act. Digital identification has been hailed as more efficient, critical to development of digital economies and societies, good for the ends of governance such as security and taxation, the gateway to a single document legal identity; but also vilified as lacking adequate privacy and data security protections.

These issues were litigated in the Nubian Rights Forum Case which found that the government had not put in place an adequate data protection legal framework and for that reason the amendments to the Registration of Persons Act that introduced digital identification derived from the NIIMS population register containing personal and sensitive information was pronounced unconstitutional. In response and in order to comply with this adverse decision, the government has recently published Draft Regulations to Registration of Persons Act and the Data Protection Act, namely, the Registration of Persons Act (National Integrated Identity Management System)

<sup>28</sup> Registration of Persons Act, Cap 107 of the Laws of Kenya (26 June 2020 <http://kenyalaw.org:8181/exist/kenyalex/act-view.xql?actid=CAP%20107>). Registration of Persons Act, Cap 107, Subsidiary Legislation (26 June 2020 <http://kenyalaw.org:8181/exist/kenyalex/sublegview.xql?subleg=CAP%20107>).

Regulations of 2020<sup>29</sup> and the Data Protection (Civil Registration) Regulations, 2020.<sup>30</sup>

The draft regulations on registration of persons under NIIMS provide that “enrolment” means the process of collecting specified particulars from an individual for the purpose of assigning them Huduma Namba. The question here is what are the “specified particulars”? The Court in the Nubian Rights Forum Case prohibited the government from collecting DNA and GPS coordinates. Government witnesses appearing in the case testified that the government had no intention of collecting DNA and GPS information even though the provision introducing NIIMS into the Registration of Persons Act made provision for the two.

To comply with the decision, the statute will have to be amended. The remaining particulars are enumerated in Section 5 of the Act: registration number, full name, country of birth, country of residence, date of birth or apparent age, place of birth, occupation, profession, trade or employment, place of residence and postal address, Land Reference Number, Plot number or house number, finger and thumb impressions or palm or toe or palm impressions if fingers and thumbs are missing, biometric data defined to include digital fingerprints and digital photographs, date of registration, and any particulars that may be prescribed.

The draft regulations define the “Huduma Card” as “a digital multipurpose identity card issued to an individual under the Act”. “Huduma Namba” is defined as a “unique identification number issued to an individual under the Act.” The regulations therefore operationalize the provisions of the Act that mandated that those registered in NIIMS are issued both a card and a unique number.

The regulations distinguish between foundational and functional data. This is an important distinction from a data minimization point of view. When an individual requests a service from a government agency, functional data, that is data necessary to process that request, is used, and not the foundational data which is entire data relevant to the individual held by the government in NIIMS including biometric data and biographical data. This distinction dovetails with the distinction in the Data Protection Act, which distinguishes between personal information and sensitive information and mandates higher protection for the latter.

NIIMS is the population register containing foundational data. Depending on the service sought, functional data relevant to the service will be retrieved from NIIMS by the agency as it is linked to the data system. The Huduma Number and Huduma Card when presented at a service point are verified against data in the system. NIIMS is also to be used to issue passports and electronically generated copies of identity documents. The range of documents that may be accessed from the system is enumerated in the Act, the idea being that issuance of identity documents will be centralized under NIIMS and cease to be in disparate registries and agencies as has been the case.

The Huduma Namba and Huduma Card are to be issued only to eligible residents,

---

<sup>29</sup> Registration of Persons Act (National Integrated Identity Management System) Regulations of 2020 (26 June 2020, <http://www.hudumanamba.go.ke/wp-content/uploads/2020/02/THE-REGISTRATION-OF-PERSONS-NATIONAL-INTEGRATED-IDENTITY-MANAGEMENT-SYSTEM-REGULATIONS-2020.pdf>)

<sup>30</sup> Data Protection (Civil Registration) Regulations, 2020 (26 June 2020, <https://www.interior.go.ke/wp-content/uploads/2020/02/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-2020.pdf>)

that is citizens and resident foreigners. The unique identifier is a random not predetermined number. The Huduma Card will have the Huduma Namba embossed on it as well as Section 9(2) particulars, namely, a photograph and fingerprint. The regulations provide that there will be four types of Huduma Cards - for minors aged six and above, adult citizens, foreign nations and refugees. Draft Regulation 9 establishes the primacy and supremacy of the Huduma Card and Huduma Namba by providing that they shall constitute sufficient proof of identity when presented and authenticated by biometrics. Card authentication will be done using card readers to be distributed to all service centres across the country.

Draft Regulation 15 makes provision for updating of the NIIMS register with new particulars at the instance of the resident individual who wishes to do so. This is consistent with the Data Protection Act whose provisions give individuals the right to seek correction and erasure of their personal information. Draft Regulation 16 provides that production of identification documents shall rely on foundational data under the NIIMS database. This will be a measure to prevent errors in documents by using NIIMS as the single source of truth for personal information, identification, verification and authentication. Draft Regulation 18 allows government agencies to be linked to the NIIMS database but only if they rely on foundational data to deliver a public service.

By being linked, such agencies may authenticate personal data in their possession with the NIIMS database. As such NIIMS will play a crucial role as the go to database for delivery of government services. In addition, the linked agency authorized to transmit, access or retrieve foundational data when necessary for the proper discharge of the agency's functions.

Draft Regulation 17 makes the processing of personal data under NIIMS subject to the provisions of the Data Protection Act. The recently published Data Protection Act Draft Regulations specific to civil registration also apply. These regulations have four substantive parts that cover protections for the data subject, enumerate the obligations of the civil registration entities and prescribe data security safeguards and protocols for the entities and external service providers engaged by the entities and granted access to personal data held by the entity.

Draft Regulation 2 defines "civil registration" as the "continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events to the population including registration of births, adoption, marriage and death". The Regulation identifies 7 "civil registration entities", the seventh being the Principal Secretary responsible for the NIIMS database. Importantly, the same draft Regulation identifies the Principal Secretary in the Ministry of Interior and Coordination of National Government as the data controller for purposes of civil registration. The data controller plays a critical role in the data protection regime of the Data Protection Act and would be a critical player in the protection of the foundational data held by the NIIMS database. Draft Regulation 5 places the duties of compliance with the Data Protection Act on the "civil registration entity", which is a "public agency responsible for administering laws" concerned with registration, including NIIMS. The duties of such an entity include the duty to protect data, the duty to seek consent to collect personal information, the duty to inform the data subject what data is being collected, for what purpose and to be shared with whom.

Draft Regulation 8 requires the civil registration entity to ensure that if personal data is used for a new purpose, the new purpose is compatible with the old one. Draft



---

Regulation 9 embraces the principle of data control by the data subject as it allows the data subject to ask the civil registration entity to restrict the processing of their personal data. Other provisions allowing the data subject control over the data held by NIIMS provide the right to access personal data, right to request rectification of personal data albeit a limited right because the entity must determine whether the rectification is necessary and may decline the request in writing. Under Draft Regulation 13, a data subject is entitled to request and to receive their data in a machine readable format.

Under draft Regulation 14 a person duly authorized by a data subject may exercise the rights of the data subject on their behalf and may be allowed access to information. The civil registration entity is entitled under this regulation to presume that the person is authorized to access the data unless evidence to the contrary is provided. This regulation places the burden of ascertaining third party data access rights on the data subject rather than on the entity. Draft Regulation 15 imposes a burden of protecting data collected from children on the civil registration entity.

NIIMS data is to be retained in perpetuity except if the data is collected for a specified purpose, in which case it may be deleted, anonymized or pseudonymised. The Data Protection Act requires institutions and entities to hold data only for as long as is necessary for the purpose for which it was collected. This limitation helps limit the risk of data loss or unlawful exposure and transmission. Since NIIMS is a population register, it makes sense that draft Regulation 17 allows for data retention in perpetuity. It is the obligation of the entity to determine personal data to be deleted, erased, anonymised or pseudonymised.

Draft Regulation 18 imposes on the civil registration entity the duty to report a data breach to the Data Commissioner. The entity is also in charge of carrying out data impact assessment when required under Section 31 of the Act.

Under draft Regulation 20, the Data Protection Officer for NIIMS is to keep written records of the processing activities of the civil registration entity including information on transfer of data to a foreign country and data protection impact assessment measures taken. Draft Regulation 21 is important because it allows a civil registration entity to share with a public agency personal data it has collected. The regulation does not define what a public agency is but it says its authorized officer may request the data in writing and the writing should state the purpose for the data, duration the data will be held and the data protection safeguards in place. The public agency has an obligation to protect the data so obtained and restrict it to purpose.

Draft Regulation 22 regulates an entity that employs automated decision making. It does not ban or unduly limit automated decision making. Instead it provides that a data subject about whom automated decisions are made should be informed and given explanations about the logic, significance and consequences of automated processing. The entity using automated decision making is to ensure that the data is secured and it is also to ensure that the data subject can obtain human intervention and express their point of view. The data subject is accorded the right to register complaints with the entity orally or in writing, and the entity is to conduct investigations and notify the complainant within 7 days of any action taken. Appeals lie with the Data Commissioner.

---

Although NIIMS was designed and launched before data protection legislation had been enacted, draft Regulation 24 prescribes that a civil registration entity shall embed data privacy measures directly into the design of its database to ensure protection of personal data. It is yet to be seen whether NIIMS design and administration complies with this provision. The operational and technical systems of a civil registration entity are to incorporate data privacy and protection principles and mechanisms such as de-identification measures and cyber and physical security measures.

Three types of security safeguards are to be used - technical, personnel and procedural. It is also the obligation of the entity to ensure its infrastructure and systems are not attacked and that the database is continuously backed up. In addition to that, the Data Commissioner is mandated to conduct periodic monitoring and evaluation of security safeguards of the civil registration entity. The civil registration entity is to formulate a written data security procedure binding upon users within its entity and guiding them on data protection, privacy, security and use protocols including the manner of dealing with information incidents when they happen and the protocols for authorizing access to the database of the entity.

Draft Regulation 34 requires an entity to document security incidents involving the breach of personal data. The entity is also to prescribe how the incidents are to be handled and resolved. Appropriate safeguards should be in place before an entity connects database systems to or transfers data through the internet or other public network. Periodic security audits are to be done by data security experts and reports acted upon by the entity every 24 months. Draft Regulation 38 prohibits a civil registration entity from transferring personal data it has collected out of Kenya, except with the approval of the National Security Council. This restriction on transfer of data out of Kenya is more stringent than what is provided for under the Data Protection Act but it does not list consent of data subject as a condition for transferring data out of Kenya.

Draft Regulation 40 concerns outsourcing agreements between the civil registration entity and an external service provider. If the external service provider is to be granted access to personal data held by the entity then the entity must make an assessment of data security risk. The entity must also enter into an express agreement with the external service provider defining the data and its purposes, the data systems the external service provider may access, types of permissible processing activities, plus the duration for holding the data and eventual disposition.

Persons engaged by the external service provider to handle the data made accessible by the entity shall be bound by similar obligations as will any other external service provider engaged by the entity. The external service provider has a reporting obligation to the civil registration entity. The civil registration entity on its part has a supervisory role over the external service provider to ensure compliance with the agreements and statutory obligations in the Act and regulations.



## **7. Kenya Citizenship and Immigration Act**

The Kenya Citizenship and Immigration Act No. 12 of 2011 provides for registration of qualifying persons as citizens and residents. A person newly registered as a citizen receives a certificate of registration. This then qualifies the person to receive a digital national ID under the Registration of Persons Act. This Act also provides for the issuance of various types of passports and other travel documents.

The Act enumerates that citizens are entitled to receive documents of registration or identification including: birth certificate, certificate of registration, passport, national ID card and voter's card. The form and content of these documents is to be determined by the Cabinet Secretary. The single identity document envisaged by NIIMS will reduce the number of documents to be issued to a citizen by the government. The Act provides that a passport is prima facie evidence of citizenship. Citizenship and immigration is a data intensive area involving collection of information from citizens, verification, authentication and issuance of identification documents by the government whose effect is to establish legal identity. It is no wonder that it is fast becoming automated and digitized across and within countries to create linkages and harmonization of travel and trading documents.



## **8. International and Regional Laws**

The Constitution makes international law, including regional law, part of Kenyan law. Article 2(5) states that "the general rules of international law shall form part of the law of Kenya" and Article 2(6) states that "any treaty or convention ratified by Kenya shall form part of the law of Kenya...." Article 6 of the Universal Declaration on Human Rights (UDHR) and Article 16 of the International Covenant on Civil and Political Rights articulate the right to be recognized as a person before the law. The ICCPR<sup>31</sup> at Article 17 guarantees the right to privacy, at Article 19 the right to information, at

<sup>31</sup> International Covenant on Civil and Political Rights, ratified by Kenya on 1 May 1972. <http://kenyalaw.org/treaties/treaties/159/International-Covenant-on-Civil-and-Political-Rights>

Article 24 the right to nationality and birth registration, and at Article 25 citizenship rights which include the right to take part in public affairs and have access to public services of one's country without discrimination or unreasonable restrictions. Article 11 protects freedom of movement which includes the right to move freely within territory, the right to leave and the right not to be deprived of the right to enter one's own country.

These clusters of rights are important for digital identification because identity authentication will often be required before the rights can be enjoyed, demanded or enforced. Similar provisions are present in other human rights treaties Kenya has ratified, including, the Convention on the Rights of Persons with Disabilities.<sup>32</sup> Kenya has also ratified the International Covenant on Economic, Social and Cultural Rights (ICESCR) 1966,<sup>33</sup> which guarantees among other rights the rights to work and social security, to access which citizens often must produce identification documents. Article 7 of the Convention on the Rights of the Child and Article 24(2) of the International Covenant on Civil and Political Rights also recognize a right to birth registration.

Kenya has ratified several regional treaties that have a bearing on digital identification. The Treaty Establishing the East African Community, 1999,<sup>34</sup> requires Partner States at Article 104 to "maintain common standard travel documents for their citizens" as one of the listed measures of regional cooperation. It defines a common standard travel document as a "passport or any other valid travel document establishing the identity of the holder, issued by or on behalf of the Partner State of which he or she is a citizen and shall also include inter-state passes."

The Treaty Establishing the Common Market for Eastern and Southern Africa (COMESA), 1993,<sup>35</sup> provides at Article 164 that as a measure of cooperation, Member States shall progressively adopt measures to promote free movement of persons, labour and services and the rights of establishment of residence of citizens of Member States. The treaty states that a valid travel document means a "passport or any other valid travel document establishing the identity of the holder, issued by on behalf of the Member State of which he is a citizen and shall also include a laissez passer issued by the Common Market to its officials." The details of these benefits are to be developed in the Protocol on the Free Movement of Persons, Labour, Services, Right of Establishment and Right of Residence.

Kenya has ratified the African (Banjul) Charter on Human and Peoples' Rights, 1981.<sup>36</sup> It guarantees the right to information, right to access public services and freedom of movement. Curiously, the Banjul Charter does not provide for the right to privacy but it recognizes the right to integrity of the person.

---

32 Ratified by Kenya on 18 June 2008. <http://kenyalaw.org/treaties/treaties/278/Convention-on-the-Rights-of-Persons-with-Disabilities>

33 Ratified by Kenya on 1 May 1972. <http://kenyalaw.org/treaties/treaties/873/International-Covenant-on-Economic-Social-and-Cultural>

34 Ratified by Kenya on 31 May 2000. <http://kenyalaw.org/treaties/treaties/60/Treaty-Establishing-East-African-Community>

35 Ratified by Kenya on 8 December 1994. <http://kenyalaw.org/treaties/treaties/42/Treaty-Establishing-Common-Market-for-Eastern-and>

36 Ratified by Kenya on 23 January 1992. <http://kenyalaw.org/treaties/treaties/11/African-Banjul-Charter-on-Human-and-Peoples-Rights>

---

Worth considering is whether regional treaties of European Union (EU) and other countries might have an impact in Kenya or for Kenya. For instance the EU's General Data Protection Regulation (GDPR) which has affected a number of foreign corporations with commercial interests in Europe such as Facebook, Google and Apple. These companies have faced high level litigation and endured hefty fines imposed by courts in the EU as a result.

Uwazi



Towards Service Excellence

Utility Bills Payments

37

5

36

4

PRISA



hudu  
KENYA

a



The Registration of Persons Act, Cap 107, Revised 2018, is the principal law for the issuance of national identity cards. The national identity card is the primary form of personal identification in Kenya. It is mandatory for Kenyan citizens who have attained the age of majority to obtain a national identity card. Even though a passport is a recognized form of identification under the Kenya Citizen and Immigration Act it is however not mandatory.

The institutional framework for the issuance of paper and digital national identification documents is provided for under the Registration of Persons Act. Provisions regarding the new digital identification card were grafted onto the old regime through the new Section 9A introduced into the Act. According to the draft NIIMS Regulations released by the government in February 2020 following the decision in the Nubian Rights Forum Case, digital identification is to replace non-digital when the new system is implemented fully. We are in a transition period prone to adjustments and changes.

The registration of persons falls under the State Department of Interior and Citizens Service within the Ministry of Interior and Coordination of National Government. The Ministry is headed by a Cabinet Secretary who is appointed by the President with the approval of the National Assembly as required by Article 152 of the Constitution. The Department, on the other hand, is administered by a Principal Secretary, who is also appointed by the President in accordance with Article 155 of the Constitution, after nomination by the Public Service Commission and upon approval by the National Assembly.

The Registration of Persons Act provides for a number of key offices the fore most being those of the Principal Registrar and the Deputy Principal Registrar, both appointed by the Cabinet Secretary. The Principal Registrar in turn appoints the personnel of the department starting with the Provincial Registrar and the District Registrar as well as Senior Registrars, Registrars, Assistant Registrars, Senior Assistant Registrars, Assistant Principal Registrars. Further, the Act provides for fingerprint officers of various cadres - Chief Fingerprint Officer, Deputy Chief Fingerprint Officer, Senior Fingerprint Officer, Fingerprint Officer and Senior Fingerprint Assistant. Officers appointed under the Act are collectively referred to as Registration officers. Rule 12 of the Act requires the Department to issue a Certificate of Appointment

to all Registration Officers. Citizens may lawfully ask to see an officer's Certificate of Appointment. In an era of heightened public concern about privacy and security of personal information and data, coupled with suspicion and litigation regarding digital identification/Huduma Namba, Rule 12 promotes the principle of data privacy.

The statutory mandate of the Principal Registrar is to keep a national register of all persons in Kenya. The national register must have the personal data prescribed by the statute and is open to inspection by an authorized officer. The national identification card issuance procedure involves the collection of fingerprints, photographs and personal data collected through a prescribed statutory form that is filled by the applicant at the designated place of issue. The Principal Registrar issues a national identity card to all persons registered in the national register in accordance with the Act.

The Act also establishes the office of Director of National Registration who is appointed by the Public Service Commission. The Director may set up an information authentication committee or appoint an authentication agent to authenticate information contained in the register whenever demands for information are made. The Director has power under Section 18A to cancel and revoke identity cards. Under Section 17, the Cabinet Secretary may by Gazette Notice declare an identity card issued invalid. Under Section 17A any authorized officer may arrest without a warrant a person suspected of committing an offence under the Act. Under Rule 7(1), loss of an identity card is to be reported to the police or an administrative office. A police abstract is required when a person applies for a replacement card at the office of the designated registration office. As such registration of persons is administered and regulated through a mix of administrative, policing and prosecutorial measures. A legitimate concern is whether these regulatory and enforcement mechanisms do not expose citizens to layers of bureaucracy and extortion, weakening identification rights, protections and privileges.

The new NIIMS provisions will introduce new functions to the office of the Principal Registrar who is to oversee the collection of biometric data and other new types of data besides the traditional forms of data - fingerprinting, photographs and details of birth, parentage, residence. Following the High Court's decision in the Nubian Rights Forum Case rendered in January 2020, the government published the *Draft Registration of Persons Act (National Integrated Identity Management System) Regulations, 2020*.<sup>37</sup>

The draft regulations assign to the Registration Officer the task of enrolling resident individuals into the NIIMS database. The draft regulations do not have a definition for "registration officer" and so we assume that the definition in the Act applies to digital identification as they apply to the old. The applicant for the identity documentation must appear in person before the Registration Officer for enrollment and is to provide an application and the statutorily prescribed particulars including biometric data. The Registration Officer is mandated to issue each a resident individual applying with one type of card from the four types provided for: Minors' Card, Adults' Card, Foreign Residents' Card and Refugees' Card - and of course these means that the applicant in making the application must provide documentary proof of their particular status matching their eligibility for one of the cards. The Registration Officer is also in charge

---

<sup>37</sup> Published at the Ministry of Interior website - <https://www.interior.go.ke/wp-content/uploads/2020/02/THE-REGISTRATION-OF-PERSONS-NATIONAL-INTEGRATED-IDENTITY-MANAGEMENT-SYSTEM-REGULATIONS-2020.pdf>



of effecting updates to the personal data held in the system upon notification by a resident individual.

The draft Regulations provide that the Principal Secretary is the one to issue the Huduma Namba and is also the one to communicate with applicants regarding the success or otherwise of their application.

There are special draft provisions on processing children worth noting. Newborns are to be enrolled in the NIIMS at the point of birth registration however only minors of six years and above may provide biometric data and be issued the Huduma Card. Such minors are to appear in person and are enrolled upon the consent of their parent or guardian.

The Act at Section 14 provides for offences related to identification, one of which is failure to apply to be registered in accordance with the provisions of the Act. There are other offences related to the identity card. Offences are triable in subordinate courts.

*The Births and Deaths Registration Act (Cap. 149)*<sup>38</sup> provides for the office of the Principal Registrar of Births and Deaths. It also provides for the offices of Registrar and Deputy Registrar both appointed by the Minister. The Registrar is mandated to register births and deaths occurring in the registration areas designated by the Minister. The Register is to be completed with statutorily prescribed particulars in the Register Books and Forms provided to the Registrars by the Principal Registrar. Also involved in the registration of births and deaths are medical officers who must issue documents containing information required to effect registration.

The birth of a person occurring after the expiration of the 28th week of pregnancy whether alive or dead is eligible for registration under the Act. Section 26 of the Act provides for the issuance of a certificate of birth once a birth has been registered. As noted above the proposed NIIMS Regulations provide that a newborn is to be enrolled into the NIIMS database at the time of birth registration although one must be at least 6 years of age to be issued with a Huduma Card. The birth registration and the Certificate of Birth issued thereafter, besides being important for proof of citizenship, are therefore important sources of foundational data for the NIIMS enrollment process and the eventual issuance of digital identification encapsulated in the Huduma Namba and Huduma Card.

The Kenya Citizenship and Immigration Act 12 of 2011<sup>39</sup> puts the “Director of the Service” appointed under Section 16 of the Kenya Citizens and Foreign Nationals Management Service Act, 2011,<sup>40</sup> in charge of citizenship and immigration matters. The Director issues passports and other travel documents and is also mandated to conduct research, collect and analyze data and manage records. The Service also appoints immigration officers recognized under the Act. In addition to passports, several documents are recognized under the Act which are relevant to application of the digital identification under the NIIMS regime. These include the foreign nationals

---

<sup>38</sup> The Births and Deaths Registration Act (Cap. 149). <http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20149>

<sup>39</sup> Kenya Citizenship and Immigration Act 12 of 2011 <http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2012%20of%202011>

<sup>40</sup> Kenya Citizens and Foreign Nationals Management Service Act, 2011 <http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202011>

registration certificate under Section 56, the permanent residency status document under Section 37, the pass under Section 36, the permit under Section 40, and the Visa. Rule 46 under the Regulations states that a passport or other travel document presented by foreigners establishes identity and nationality.

Section 22 also sets out the right of citizens to receive any document of registration or identification that is issued by the state, namely, birth certificate, certificate of registration, passport, the national identity card and voter's card. These documents are required for enrollment into NIIMS when a resident individual seeks to obtain one of the four types of digital identification depending on their residency status as discussed above.



*Section 3A of the Act provides that personal data obtained under the Act shall be held and maintained in accordance with the principles of the Data Protection Act.*



It is worth noting that Kenya now requires her citizens to have digital passports in place of the non-digital ones which are being phased out. The digital passport is significant for another reason discussed above in the "legal framework" section. In line with the requirements of the Treaty for the Establishment of the East African Community, Kenya now issues a digital East African passport. Section 32 confirms that a passport provides "prima facie evidence of the citizenship or domicile of the holder, as the case may be, and of their entitlement to state protection." The Regulations to the Act show a declaration made by Cabinet Secretary in 2014 that declared the Kenyan identity card a recognized travel document for travel to Rwanda and Uganda.

Section 48 of the Act states that an "immigration or other authorised officer of the Service shall capture biometrics in the course of the discharge of the mandate of the service." This provision means that the government collects biometric data to complement data that is in passports and other travel documents. Section 54 provides for offences relating to documents. One might argue that digital identification will minimize incidents of these offenses since forgeries and alterations as well as the incidences of providing false information will be reduced since the government can verify and authenticate information from its own database.

The Act establishes the Border Control and Operations Coordination Committee to, among other functions, co-ordinate the exchange of information between the agencies responsible for the security and management of the borders at the designated entry and exit points. The Committee has eleven members and is chaired by the Principal Secretary of the Immigration Ministry. This Committee submits a report to the National Security Council at the end of every year detailing its activities and operations.


---

The Kenya Citizenship and Foreign Nationals Management Service Act No. 31 of 2011 establishes a state corporation (the Service) by the same name and provides for the creation and maintenance of a national population register and the administration of the laws relating to births and deaths, identification and registration of citizens, immigration and refugees. The Act establishes the following offices: under Section 5 the Board of the Service whose chairperson is appointed by the President. Second, the Director General of the Service and Directors of the Service. Third, the Kenya Citizenship and Immigration Service Appeals Tribunal. Appeals from the decisions of this Tribunal lie at the High Court.

The Service has an all encompassing implementation role for policies and laws relating to citizenship and immigration, births and deaths, identification and registration of persons, issuance of identification and travel documents, foreign nationals management and the creation and maintenance of a comprehensive national population register. In this regard, the Service is mandated to administer the four statutes: the Registration of Persons Act (Cap. 107), Births and Deaths Registration Act (Cap. 149), the Citizenship and Immigration Act, 201 and the Refugees Act, 2006 (No. 13 of 2006).

The Service is to collect and compile information on the distribution and composition of the population, among other functions. Its primary functions involve receiving personal information from the primary registration agencies and to store and update it. It is also to generate appropriate unique identifiers for individuals and groups. Further, it is to regulate the sharing of information by various registration agencies and users and undertake data collection and dissemination in a manner that ensures consistency and accuracy in accordance with set national standards and guidelines. It is also to facilitate access to information and data to national population registration information. The challenge here of course is that these functions are very similar to those given to the Principal Registrar as the person in charge of NIIMS under the Registration of Persons Act. Subject to confirmation, one may conclude that these functions might have been superseded by the NIIMS regime and will need to be amended or deleted to avoid duplication and conflict of roles.

The Data Protection Act No. 24 of 2019 establishes the Office of the Data Commissioner (ODC). The Data Commissioner is to be appointed by the President to serve for a single term of 6 years following a recruitment exercise undertaken by the Public Service Commission. One of the mandates of the ODC is to register data controllers and data processors. Data Controllers may contract Data Processors but the later remain answerable to the former with regards to compliance with the provisions of the Act. The model Kenya has chosen is centralization of personal data collection and processing under NIIMS with an overarching regulator under the Data Protection Act. This model allows multiple private sector players to be involved in processing data under the supervision of data controllers who may be private or public entities. These sectoral players are regulated by a statutory Data Commissioner. The Registrar of Persons would be a public agency under and regulated by the DPA. The Registrar of Persons would be at liberty to in-house data collection and processing or to out-source those functions while remaining answerable to the Data Commissioner regarding compliance with the



statute. The Data Commissioner can receive complaints regarding breach of the Act's provisions, and has investigative and enforcement powers. Appeals against decisions of the Data Commissioner lie at the High Court. The Data Commissioner may also seek a preservation order from the High Court to prevent loss or modification of personal data.

The Commission on Administrative Justice is the administrative body charged with the enforcement of the Access to Information Act No. 31 of 2016. The Chief Executive Officer of a public entity is designated the access to information officer for purposes of the Act. The Commission has oversight, investigatory and enforcement powers of compliance with the Act and is the entity that reviews decisions of public entities and private bodies that have denied citizens access to information.

The Fair Administrative Action Act No. 4 of 2015 provides for its enforcement in courts and tribunals. A person aggrieved by an administrative action or decision made by a state or non-state agency may seek judicial review of the action or decision by filing an application in court or in a tribunal.

The Kenya Information and Communications Act No. 2 of 2018 establishes the Communication Authority. The Commission's mandate is to regulate, licence and facilitate the development of the information communications sector. It carries out this mandate through a Board as the governing body and a Director General as the Chief Executive Office. The Act establishes the Communications and Multimedia Appeals Tribunal. Aggrieved parties may appeal the decision of this tribunal at the High Court.





**Legal Framework:** It remains to be seen whether the government will put in place an adequate legislative and implementation framework for NIIMS data protection and security that extends to all the government agencies having access to the foundational and functional data availed through the system. The government's initial orientation was to favour efficiency over privacy. In addition, the government designed NIIMS a centralized database, which experts have noted makes it more vulnerable to attacks and makes breach more consequential than would be the case with decentralized databases. The failure to have an adequate legislative framework in place and to make critical appointments such as the appointment of the Data Commissioner point at weaknesses in end-to-end conceptualisation of the digital identification programme. It points to challenges within the government and suggests a need to return to the drawing board to think through each step and put in place resources and personnel required to run the system effectively. These omissions undermine the government's stated embrace of efficiency and cost effectiveness.



**Data Commissioner:** How effective, autonomous and independent will the Data Commissioner be? Will the recruitment process suffer headwinds as has been the case with recruitment of the Director General of the Communications Authority? Filing this position is critical to resuming NIIMS enrollment. The risk of delays occasioned by procedural or substantive failures in the recruitment process constitutes a challenge.



**Data Security:** Data security is a challenge facing even the most technologically sophisticated nations. There are no expert countries, so to speak, from which a country like Kenya can borrow a foolproof model. The technology landscape is also fluid and changes rapidly, keeping everyone learning and anticipating the next wave of changes. On the one hand, Kenya should learn from other countries, but on the other hand even those countries remain on a fluid learning curve. This will remain an ongoing challenge.



**Discrimination:** Digitization of government services should be inclusive. In a county of uneven distribution of wealth, opportunities, access, that at the same time has a robust people centred Constitution and laws, a mandatory digital ID may face legal hurdles. National identity cards comprise one of the most basic rights of citizenship. The government will have to provide a minimum threshold of facilities across the 47 counties to ensure inclusive NIIMS enrollment and access to government services. Important rights such as the right to vote will be unrealizable if this is not done, now that the government prefers a mandatory enrollment approach and the Court in the Nubian Rights Forum Case did not pronounce it an invalid. Every government

office processing identification documents will need to have working card readers and other related infrastructure, not to mention fully trained staff that can run NIIMS enrollment efficient and at the same time abide by privacy restrictions. The alternative will be to allow physical form IDs to continue being used, but this will also present dual track challenges and an urban-rural bias.



**Trust:** Clearly there are important political questions yet to be resolved before Kenyans can fully adopt national digital identification. Kenya is a highly politicized and litigious country. Many government initiatives are sometimes shrouded in secrecy and other times generate mistrust. NIIMS was introduced in such a context and will remain affected by it more so because the government intends to use digital identity in processes such as voting and census taking, which are inherently political in nature and tend to evoke political sentiments and contestation. Another area that raises political concerns is the suspicion that there will be foreign access to NIIMS data for political or commercial use.



**Data Protection:** Creating digital identification involves collecting personal information. If this is not done carefully and professionally, the information collected will not be accurate or useful for the purposes for which NIIMS was set up.



**Security:** Questions were raised by litigants and expert witnesses in the Nubian Rights Forum Case regarding the government's choice of a centralized database over a decentralized database. Centralized databases were said to be more prone to security breaches because they make for seizable data heists and are attractive cyberterrorism targets. The system is yet to be tested. On its resilience, we can only take the government's word for now.



**Coordination:** The existence of multiple statutes and institutions on registration, identification and other documentation was said to create inefficiency and duplication. NIIMS is supported by the argument that it solves this problem by centralizing personal information data in one centrally administered database and generating identification documents and authentication from this single source of truth. Still multiple government agencies will need to be harmonized and synchronized to ensure efficiency and cascade data protection and security across all government departments.



**Rights of Children:** There has been a failure by the government to prioritize seeing NIIMS from a citizen's experience perspective. The government sees it as just a minor development from what it has always done as the collector of personal information and issuer of identification documents. This is not the case because digitization allows the government to do so much more with personal information than before.



**Legality:** The government intends to use NIIMS as a single source of truth on identity that will enable the issuing of a single unique identification number and card. It has also expressed optimism that NIIMS will help with law enforcement and tracking of missing children, combating terrorism and human trafficking. NIIMS is not only going to be a bureaucratic juggernaut for registration and documentation but a law enforcement tool as well. This raises important questions whether the government will ensure the tool is used within boundaries of legality.



**Legal Identity:** Legal identity has recently been an area of litigation and may continue to be. A case in point is the Audrey Mbugua Case <sup>41</sup> where the petitioner, a transgender Kenyan, sought to have particulars of his identity changed on his high school certificates and the High Court in his favor and against the Ministry of Education which had refused to effect the changes. There is emerging the right to have a different identity than the one assigned at birth. The challenge lies in having a digital identification programme that can adapt to changes in legal identity, especially now that NIIMS enrollment starts at the early age of six.

---

<sup>41</sup> Republic v Kenya National Examinations Council & another Ex-Parte Audrey Mbugua Ithibu [2014] eKLR (26 June 2020, <http://kenyalaw.org/caselaw/cases/view/101979/>).





Kenya still has a long way to go before fully launching a secure national digital identification system. The government is in the process of developing a comprehensive digital identification policy, legal and implementation framework to enable a launch. The process of issuing Huduma Numba has stalled, compromising seamless end to end implementation, and exposing challenges in government implementation strategies and conceptual orientation to efficiency over privacy, and a worrying delay in making critical statutory appointments such as that of the Data Commissioner.

At stake in the government's quest to create digital bureaucracies and economies is the data privacy and data control interest of individuals whose information is collected into a national population register designed to be a single source of truth about personal identity. There is a certain inevitability that has attached to the introduction of digital identification by governments. Kenya is considered Africa's Silicon Savannah. It is not surprising that it is working its way towards establishing and entrenching digital identification. This pro-technology historical context gives momentum to the growing sense of inevitability of digital identification.

At the same time, Kenya is a democracy that is still in formation. Government programmes often invoke suspicion, a suspicion that is exacerbated by the intensity of inevitability of government involvement and control of people's affairs and choices. In addition, globalisation of economic activity has not benefited everyone. The argument that digital identification will help Kenya in the context of economic globalisation therefore has limitations and in fact does cause consternation that things are only going to get worse for the vast majority disproportionately resident in the developing countries.

Digital identification may or may not be the economic silver bullet it has been sold to be. It all depends on other economic indicators. To add to that, the country is yet to receive assurances about investments the government has made in data security, given that even more developed countries have been vulnerable to large scale attacks on their data infrastructure. Lastly, digital surveillance by governments and non-state actors who gain access to the NIIMS database is an important concern. People are asking whether after the introduction of digital identification, what is to stop the government from introducing face recognition technology for purposes of mass surveillance? The possibility and risk that innocuous and malevolent uses of technology might be blended invites us to continue improving the policies, laws, and institutional frameworks discussed above.

# Recommendations



1. Effective communication and transparency are critical to the adoption and legitimacy of digital identification programmes due to the natural suspicion citizens have of technology especially when used by the government. Given the cost of putting the programmes in place, an upfront and immediate investment in effective communication will cultivate public goodwill and promote enrollment uptake across the four corners of the country.

For instance, the government needs to clarify whether enrollment is mandatory or not, and if mandatory pass legislation directing that it is and stating the consequences of default. If it is optional, the government should communicate how services will be accessed by those unwilling or unable to enroll. If this clear communication is not provided, avenues for corruption and citizen intimidation by police might arise. The government could use community based organizations to disseminate information about NIIMS enrollment and its benefits. Even though registration of persons is a national government function, government services are issued at Huduma Centres in the 47 counties. County governments would play a critical role assisting the national government disseminate information about NIIMS to local communities.

2. The government should appreciate that NIIMS unlike the old physical form registration process has adjusted the citizen-state relationship fundamentally. NIIMS is not just a small development in registration of persons and issuing of identification documents, admittedly traditional state functions, which now impact citizens in new ways. It is recommended that the government should give NIIMS personnel special training on the rights of citizens under the Constitution and the statutes discussed above. Internal departmental processes should be streamlined with effective management and business procedures involving logs, forms, and data access protocols, breach communication protocols and so on. Internal and external auditors should be engaged to help keep officials accountable and ensure compliance with laws and timely production of statutory reports.

3. Academic experts should be engaged to provide cutting edge staff training and computing experts should be engaged to continuously service the digital identification security infrastructure.

---

4. Critical offices should be filled and succession planning done to avoid prolonged vacancies in future. Human and other resources should be provided to the NIIMS department and the department should have a clear administrative structure reflecting the regulatory protocols mandated by law. This should be done upfront in the interest of data protection and security.

5. The review given above of the legislative framework reveals that running the digital identification programme effectively within the country's legal framework involves a massive bureaucracy. It will be important to review the NIIMS institutional framework in order to eliminate role duplication. This will be an important cost saving measure. It will also harmonise operations and prevent turf wars among the various statutory heads. At the moment it is not clear, for example, how the Principal Registrar administering NIIMS will relate to the Director of the Service as the two have similar roles. This needs to be clarified through statutory amendments. The duty bearers under each statutory regime should be clarified and timeframes for taking specific actions, for instance providing reports on breach, obtaining data transfer consent, should be streamlined to eliminate confusion and role conflicts.

6. The government should invest in a professional cadre of registration officers to ensure that personal information is collected accurately. This will ensure that NIIMS becomes the single source of truth and it carries out its functions in a cost effective manner. It will also persuade citizens that the system works, which will improve its uptake, helping overcome the challenges of trust it has faced so far.

7. Harmonization and synchronization of the various laws and institutions involved in handling and processing personal information will need to be done. Rather than do it in a vacuum, perhaps a trial period could be launched to test whether recent changes ordered by the court and any other changes made to NIIMS will work per plan. After that, with the benefit of any revelations obtained from the trial period, a full scale launch will be on a sure footing. The trial period should involve vulnerable and marginalised communities, and minority groups.

8. Human rights organizations that work with vulnerable constituencies should be brought on board to advise on legal compliance status of the revised programme before it is fully launched. This will preempt lawsuits in future, will improve adaption and provide information critical to improving the user's experience. The trial period should be assessed by independent professionals.



The Kenya ICT Action Network (KICTANet) is a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. The Network is a thought leader and is dedicated to bringing evidence, expertise, and more voices into ICT policy decision-making. KICTANet promotes public interest and rights based approach in ICT policy making.

[www.kictanet.or.ke](http://www.kictanet.or.ke)

