POLICY BRIEF
DATA PROTECTION & DIGITAL IDENTITY IN KENYA

Authored by KICTANet and commissioned by UK DAP
(United Kingdom's Digital Access Programme)

KICTANet
The Power of Communities
www.kictanet.or.ke

UKaid
from the British people

Imprint

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.orke
Web: www.kictanet.or.ke
Twitter: @kictanet

Programme:
UK DAP (UK government Digital Access Programme)

Project title:
Enhanced digital inclusion through capacity building, advocacy, awareness creation, action research, open and inclusive multiple stakeholder engagement in Kenya.

Sponsor:
United Kingdom's Digital Access Program

Authors:
Prof. Sylvia Wairimu Kang'ara

Editor:
John Walubengo

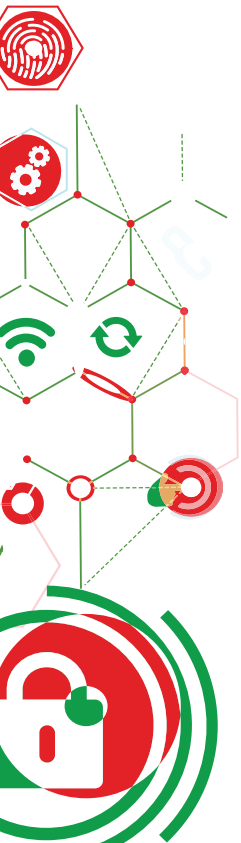
Design & Layout:
Stanley K. Murage (stanmuus@gmail.com, Cell:+254 720316292)

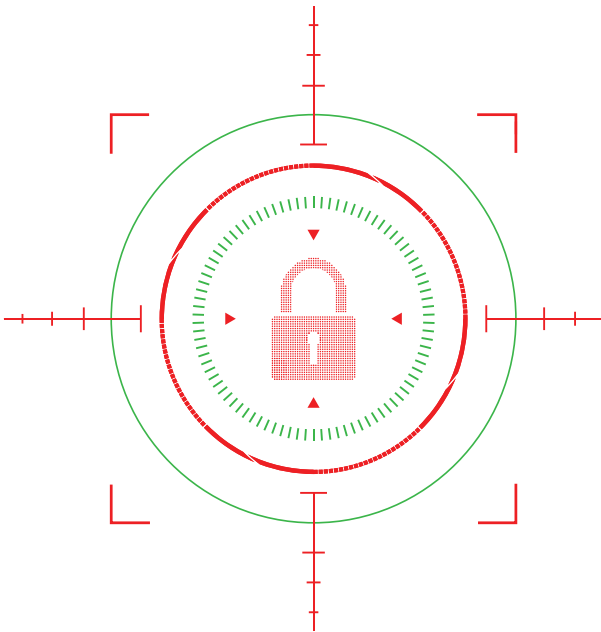
Photo (Title):
Cyber security and digital data protection concept Photo / www.freepik.com

Location:
Nairobi 2022

Year of publication:
Policy Brief No.10, May 2022

Table of Contents





Executive Summary

Kenya's Data Protection Act came into effect in November 2019 but soon thereafter, in January 2020, the High Court, in the Nubian Rights Forum Case, declared that the legislation was, in the absence of regulations and institutions necessary for its implementation, still deficient in providing adequate safeguards for the protection of personal data. [1]

At the heart of this pivotal litigation was the collection by the state of personal data for purposes of establishing an integrated identity system and issuing digital identity cards. The High Court excluded DNA and GPS information from the data that could be legitimately collected from citizens, saying it was too invasive to privacy and unnecessary for the intended purpose of civil registration and issuance of identity documents. In addition, the court directed the state to put in place adequate measures for safeguarding personal data legitimately collected to advance the policy objectives of the state.

It has been a colourful and eventful two years since these legislative and judicial postulations, which were discussed in an earlier KICTANet policy brief.[2] This policy brief evaluates what has happened since then in the legal, institutional and social contexts. It reviews and analyzes institutional policies, legislative developments and recent court decisions which, taken together with political and social trends, give a picture of the flashpoints in data protection and identity issues in Kenya. The writing of this Policy Brief has also benefited from comments and feedback given in a stakeholders webinar organized by **KICTANet** in February this year. The webinar featured presentations by the Data Protection Commissioner, Ms Immaculate Kassait, and experts drawn from various sectors including the telecoms sector and academic research institutions.

This Policy Brief aims to review the progress that has been made in Kenya's data protection and privacy law and policy in light of the government's attempt to roll out a national digital legal identity programme. It also aims to show how legal identity issues have played out in day to day activities of citizens and high stakes national events such as voting in national elections. Ultimately, the democratic principles of nationhood, citizenship and legal identity are presented as the baseline for executive and legislative action that seeks to resolve mounting anxiety about data sovereignty and self-ownership.

Some provisions of the Data Protection Act, including, notably, the provisions for the establishment of the Office of the Data Protection Commissioner and appointment of the Data Protection Commissioner have been implemented. This policy brief discusses the status of other statutory requirements, including those directing the establishment of the data controllers and data processors register, complaints mechanisms, and data breach reporting procedures.

1. Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR. Sylvia Kangara, Digital Identification Law in Kenya: The State of Play, KICTANet Policy Brief No. 5, August 2020. 23 March 2022, https://www.kictanet.or.ke/policy-briefs/.
2. Sylvia Kangara, Digital Identification Law in Kenya, ibid.

It is noteworthy that a second challenge was successfully lodged at the High Court against the government's plan to roll out the Huduma Namba post the Nubian Rights Forum Case.[3]

This time, the Office of the Data Protection Commissioner joined the litigation as an interested party. What has emerged from the High Court's decision in this subsequent case is that there are still huge gaps in following through with the provisions of the Data Protection Act that are to ensure that personal data collected with the provisions of the Data Protection Act that are to ensure that personal data collected by the state is protected adequately.

Having failed to carry out the personal data impact assessment, required by the Act, the government's plan to jumpstart Huduma Namba registration stalled again. This is how critical investments in data protection have become to the success of government programmes. The Huduma Bill,[4] pending in Parliament, has proven controversial, this being an election year haunted by prior electoral mishaps and disputes.

This Policy Brief notes that it is critical that government initiatives are conceived and carried out only after data protection institutions are sufficiently funded and kitted. Put differently, the design of state operations should have data protection designed into them from inception because working backwards has enormous costs and a high risk of total derailment.

The Kenyan public has shown it is wary about data protection and privacy. As data protection and privacy institutions are getting off the ground, it is important that they are allowed to be demonstrably independent and autonomous in the interest of inspiring the public's confidence before, during and after any incidences of data breach arise.

Kenya is often touted to be a digital economy, even a Silicon Savannah. To live to this billing, the international dimension of data questions and problems also needs to be addressed without prevarication.

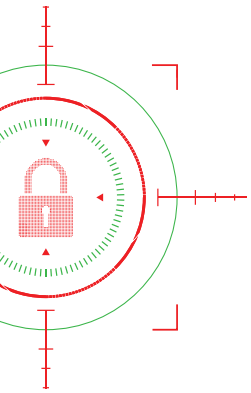
The progress achieved and the progress envisioned requires resources to be channelled to the adequate and sustained training of data protection and privacy professionals across disciplines and sectors so as to eliminate any weak links.

3. See note 16, infra.
4. Huduma Bill, http://www.parliament.go.ke/sites/default/files/2021-12/Huduma%20Bill%2C%202021.pdf. 23 March 2022.

Introduction

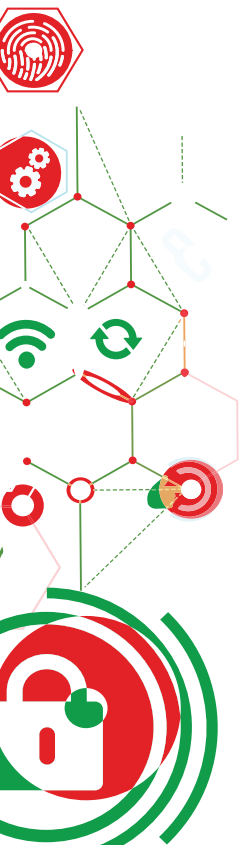
The relationship individuals have with the state is cemented by identity and citizenship.

Citizenship is the source of an individual's legal identity because it affirms that the individual is a subject of and under the protection of a sovereign nation.



However, citizenship is not the only identity people have. Identities are also derived from ethnicity, race, creed, gender, family, marital status, tribe, and origin among other attributes that are the basis for the anti-discrimination constitutional protections found in Article 27 of the Constitution.

The benefits flowing from legal identities are limited because resources are finite, and one might say that legal identities are created to drive decisions on who should or should not access these benefits, as much as they are created in order to assign legal responsibilities, such as who pays taxes to what nation.



Legal identities are created by the state when it collects biographical and biometric information on each individual. Biographical and biometric data is further used to authenticate legal identity.

The state, institutions, individuals and even machines will not take your word for it! In addition to the protections under Article 27, that these attributes of legal identity should not be used to discriminate since all citizens are to receive equal treatment before the law, the Constitution at Article 31 confers on individuals the right to privacy of their personal information and information about their family.

The right to privacy confers dignity to citizens. The government also exists to provide services to citizens, services that are also dignity enhancing. The right to privacy and the right to government services are at the heart of current disputes about data protection and legal identity in Kenya.

It is emerging that these conflicts and concerns will be quelled only if legal identity is developed and deployed by the state in ways that preserve and even promote the right to privacy. Leadership on this issue must emerge from the state if the state is to also effectively regulate the private sector's use of personal data and protection of consumer privacy interests.

Kenya's governance and development agenda does not start and end with assuring access to government services, although this is the often-cited reason for the collection of personal data used to create legal identity documents.

In addition to government services, legal identity, specifically digital identity, is expected to catapult Kenya to economic powerhouse status because digital commerce depends on identities that can be authenticated by e-commerce platforms, payment systems, and by machines.

With diminishing face to face marketplace interaction, digital identities are critical to economic growth. Furthermore, workplaces and other places where daily interactions occur are today powered by electronic communication, making digital identity indispensable to economic and social survival.

Kenya's current data protection and identity policy, and legal and institutional framework, must resolve these tensions and conflicts, reservations and aspirations.

It is still under development as the discussion below illustrates. The Office of the Data Protection Commissioner (ODPC) associates data protection with advancing the ambition to turn Kenya into a Silicon Savanna. However, whereas the uptake of mobile banking and communication was almost organic, at least believed to have been so, the uptake of digital legal identity has been an uphill task.

Government programmes have not manifested the same level of trustworthiness as the private sector. We observe that privacy has been the selling point for the private sector, therefore organically trusted by citizens, while the opposite is true for the government, which promotes the common good by exposing, controlling and disciplining the behaviour and activities of citizens.

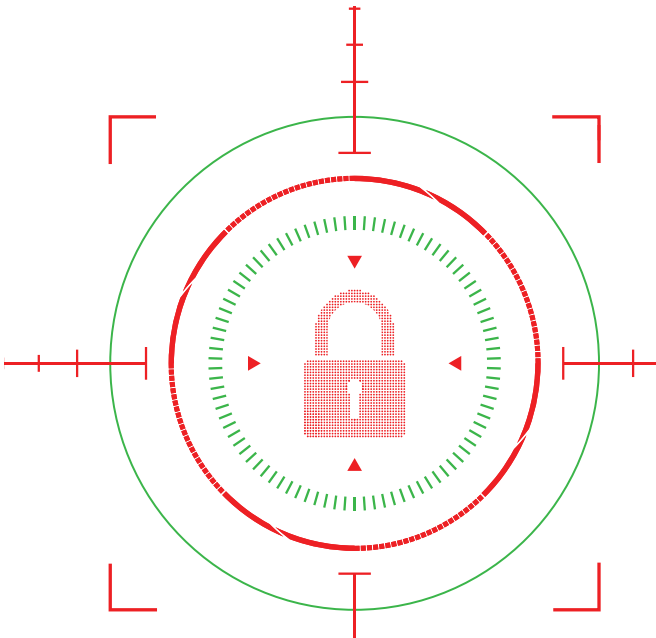
It is no wonder that citizens' uptake of government-controlled and issued digital legal identity has been fraught with resistance in our courts. The fears of citizens are that the information comprising their legal identity could be used in ways that undermine their legitimate rights and interests.

Personal data, which is protected by the Data Protection Act, is intricately linked to a person's identity. The right to privacy assures an individual's dignity by allowing them to reserve certain aspects of their lives from public glare and commercial exploitation. Self-ownership, which includes control over personal data, is a component of a person's identity. Legal identity is a small but important part of self-identity.

In a democratic regime, the constitutional protections of the individual must rise in tandem with the policy goals of the state and the aspirations of society. The individual and society are mutually constitutive. In furtherance of these legal objectives and policy objectives, a search for the appropriate balance between competing values and aspirations has continued after the passage of the Data Protection Act in 2019.

Subsequent landmark cases decided by Kenyan courts have directed the state to spare no effort in putting in place adequate measures for data protection.

As the country heads to another highly contested presidential election, the demands for data protection laws are beginning to bite and areas needing urgent attention are becoming clearer



1. Overview of current data protection policy, legal and institutional landscape

An earlier policy brief issued by KICTANET in 2020[5] discussed the Data Protection Act, 2019 and other relevant legislation. It also reviewed domestic and international practice in addition to reviewing judicial decisions influencing policy at the time.

This policy brief looks at policy, legal and institutional changes that have occurred since then, noting milestones that have been achieved and problems yet to be resolved.

1. Three Data Protection Regulations were passed in 2021 to implement the provisions of the Data Protection Act following the High Court's decision in the Nubian Rights Forum Case:

   (i). The Data Protection (General) Regulations), 2021. [6]
   (ii). The Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021. [7]
   (iii). The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021.[8]

2. In addition, two important bills currently pending in Parliament will have a far-reaching effect on data protection and the identity landscape if passed:

   (i). Huduma Bill, 2021[9]. This Bill is dated 3rd December 2021. It provides for the National Integrated Identity Management System (NIIMS). It provides for the enrolment of adults and children into the System as well as for the issuance of the Huduma Card and identity documents such as passports. In addition, Part VI stipulates data protection safeguards. Part VII stipulates offences and penalties. In its First Schedule, the Bill provides for NIIMS "foundational data".

   (ii). Computer Misuse and Cybercrimes (Amendment) Bill, 2021.[10] "The Bill also seeks to provide an additional function of the National Computer and Cybercrimes Coordination Committee which is to recommend websites that may be rendered inaccessible within the country." Could this be used to respond to a data leak or could it be used to suppress online speech? The Bill underwent the First Reading in Parliament in June 2021.

5. Sylvia Kangara, Digital Identification Law in Kenya, supra 1.6. http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN263_2021.pdf
7. http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN265_2021.pdf.
8. http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN264_2021.pdf
9. http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2021/TheHudumaBill_2021.pdf. Accessed on 10 February 2022.
10. http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2021/TheComputerMisuseandCybercrimes_Amendment_Bill_2021.pdf. Accessed on 10 February2022.

The Office of the Data Protection Commissioner is up and running.[11] It is established under the Data Protection Act to implement the provisions of the Act. The Data Protection Commissioner was appointed on 16 November 2020,[12] a year after the Data Protection Act came into effect. In addition to the Commissioner, the administrative structure of the ODPC comprises four directorates.[13] The directorates are statutory creatures of the DPA and each is designed to carry out specific statutory mandates.

This institutional setup makes the assessment of the ODPC's formal and procedural compliance with statutory prescriptions critical to personal data protection possible. The ODPC has already established some features of its modus operandi by issuing Guidance Notes on three important areas. In addition, the ODPC has an interactive website through which it communicates with stakeholders regarding statutory actions, for instance, the creation of a register of data controllers and data processors, establishment of a complaints procedure for personal data rights violations, and reporting data breaches, among others.

THE DIRECTORATES

Directorate of data protection compliance

Roles

- Registration and certification of data controllers and processors
- Register maintenance
- Oversight over data processing operations in the country
- Data processing verification
- Periodic audits and compliance review
- Data Protection Impact assessments
- Inspections
- Data transfer compliance review

Directorate of Complaints, Investigations and Enforcements

Roles

- Receiving, handling and investigating complaints
- Developing, implementing and reviewing policies, strategies and guidelines
- Summon witnesses
- Implement administrative fines for failure to comply with the DPA

11. See its website: https://www.odpc.go.ke.
12. See report filed by the office on the commemoration of 100 days since the establishment of the office: https://www.odpc.go.ke/office-of-the-data-protection-commissioner-commemorates-its-100th-day/. 10 February 2022.
13. See link: https://www.odpc.go.ke/mandate-of-the-office/directorates/. Accessed on 10 February

Directorate of Research, Policy and Quality Assurance

Roles

- Review and updating of regulations and guidelines set out under the DPA
- Promote self regulation among data controllers and data processors
- Research development in processing of personal data and mitigate risk of adverse
- effects on the privacy of individuals
- Publicize the provisions of the DPA.
- Promote international cooperation in matters relating to data protection
- Ensure Kenya is in compliance with data protection obligations under international conventions and agreements
- Promote collaboration with other bodies or organizations within and outside the country
- Coordinate the development of guidelines on codes of practice for the data controllers, data processors and data protection officers
- Coordinate the development of data protection registration and certification standards and data protection seals and marks

Directorate of Corporate Services

Roles

carries out administration functions spread out across four divisions: Receiving, handling and investigating complaints.

- Human resource management and administration
- Finance and accounting
- Information communication technology
- Corporate communication

The ODPC has so far issued the following Guidance Notes:

- Guidance Note on Electoral Purposes
- Guidance Note on Data Protection Impact Assessment
- Guidance Note on Consent

In addition to information regarding the administrative components of the ODPC discussed above, the ODPC's interactive website is advancing the implementation of the DPA in the following ways:

- Whatsapp helpline.
- Procedure for Filing a Complaint (online complaint form provided which is to be filled by one who wishes to file a complaint. Submission of the complaint is also done online).[14] The ODPC has in addition developed a Complaints Manual.[15]
- Procedure for Reporting a Data Breach (online form that one reporting the breach is required to fill. The submission is also done online). [16]
- Register of Data Controllers (not yet operational but noted to be coming soon).
- Register of Data Processors (not yet operational but noted to be coming soon).
- Link to Twitter handle.

14. See link: https://www.odpc.go.ke/file-a-complaint/. Accessed 10 February 2022.
15. See reference: https://www.odpc.go.ke/office-of-the-data-protection-commissioner-commemorates-its-100th-day/.
16. See link: https://www.odpc.go.ke/report-a-data-breach/.

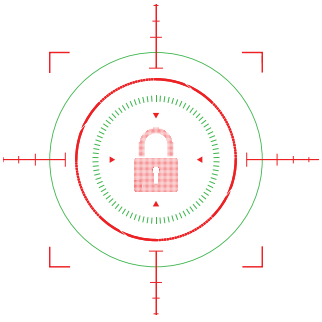
2. Recent Developments and Emerging Issues Relating to Privacy and Identity in Kenya Over The Last Three Years (2019-2022)

1. Office of the Data Protection Commissioner:Huduma Namba Roll Out Stopped by the High Court because Personal Data Impact Assessment Not Done

The government's decision to jumpstart the rollout of Huduma Namba was quashed on 14 October 2021 by the High Court.[17] The Data Protection Commissioner joined this suit as an interested party, taking the position that the application to stop the rollout should be dismissed because the Data Protection Act provided for alternative mechanisms for dispute resolution that had not been exhausted before the filing of the judicial review application.

The court agreed with the Commissioner's argument that data subjects could not seek judicial redress before either exhausting the DPA's alternative mechanisms; or seeking an exemption from internal mechanisms under the Fair Administrative Action Act. However since one of the applicants was a constitutional public interest defence institute, it was not a data subject and therefore could not pursue recourse in the DPA's internal redress mechanisms reserved for data subjects. Consequently, the court quashed the government's decision to roll out the Huduma Namba Card because a data impact assessment had not been conducted as required by the DPA.

The upshot of this case is that only data subjects are required to exhaust alternative mechanisms provided by the ODPC before taking a grievance to court. Second, the court issued an order that the government should carry out the personal data impact assessment before jumpstarting the Huduma Namba roll even though there had been an initial rollout before the DPA came into effect. Third, therefore, the DPA has a retroactive effect and cannot simply be ignored because an initiative began before it was passed.



17. Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested party) (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14Â OctoberÂ 2021) (Judgment). http://kenyalaw.org/caselaw/cases/view/220495/. Accessed 10 February 2022.

2. Fintech and the Right to Accurate Personal Data

The High Court on 15 October 2020 awarded Kenya Shillings 10 million in damages to a litigant who had been erroneously characterised as a credit defaulter by the Higher Educations Loans Board.[18] This case was litigated under the statutory regime that existed before the passage of the DPA.

Under Regulation 35 of the Credit Reference Bureau Regulations, 2013 (CRB Regulations) "a customer who believed that the information contained in the database was inaccurate, erroneous or outdated" was required to notify the bureau, in writing, of the information dispute."

Despite receiving an email from the petitioner to the effect that she had been listed as a loan defaulter even though she had never taken any loan with HELB, no action was taken to rectify the error and this affected her standing with lenders.

3. Employees and the Right to Accurate Personal Data

The right to correct personal data was also successfully asserted in a case involving the date of birth of a senior retired judge.

Justice Evans Githinji a Court of Appeal judge, objected to an erroneous assertion made by the Judicial Service Commission regarding his date of birth. The error was used to require him to proceed on retirement six months early. [19]

4. Limitations on Disclosure of Information under the Access to Information Act

The High Court on 26 November 2021 declined a petition seeking disclosure of information held by security agencies regarding the terrorist attack at Garissa University.[20] The access to information request, if granted, would have led to the release of personal data of victims, noted the court, although the prevailing reason for denying the petition was that releasing the information would have jeopardised national security and was therefore not in the public interest.

We surmise from this case that the Data Protection Act is not the only legislation limiting access to personal data held by the state. We might in future see courts resolving conflicts emanating from the various regimes governing data protection and identity.

Should we be concerned about the state using data protection arguments to prevent access to information in ways that are inconsistent with democratic governance and transparency?

5. Legal Identity, Technology & Elections

Section 44 of the Elections Act, No. 24 of 2011 [21] regulates the use of technology in elections. It establishes an Integrated Electronic Electoral System that "enables biometric voter registration, electronic voter identification and electronic transmission of results."

The Section requires the Independent Electoral and Boundaries Commission to develop "a policy on the progressive use of technology in the electoral process." In addition to requiring the Commission to verify its electronic records, the section requires the Commission to work in consultation with relevant agencies, institutions and stakeholders to make regulations for the better carrying into effect its provisions.

18. Eunice Nganga v Higher Education Loans Board & 2 others [2020] eKLR.
19. Republic v Judicial Service Commissions & 2 others Exparte Erastus M Githinji [2019] eKLR. http://kenyalaw.org/caselaw/cases/view/176738/. accessed 10 February 2022.
20. Legal Advice Centre t/a Kituo Cha Sheria & 33 others v Cabinet Secretary, Ministry of Education & 7 others (Petition 104 of 2019) [2021] KEHC 390 (KLR) (Constitutional and Human Rights) (26 November 2021) (Ruling). accessed 10 February 2022.
21. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202011. Accessed 10 February 2022.

Section 44A requires the Commission to have "complementary mechanisms" for the identification of voters that is "simple, accurate, verifiable, secure, accountable and transparent".

The Data Protection Act in a similar fashion requires the Data Protection Commissioner to work in collaboration with other agencies. The changes proposed in the Huduma Bill would require the IEBC to rely on the NIIMS and to be linked for purposes of voter identification and verification during elections.

The Bill anticipates this by bringing the management of the IEBC onboard into the membership of an administrative committee, to be established if the Huduma Bill becomes law, comprising senior officials of various government ministries.

A number of issues arise from Kenya's ongoing transition to the digitisation of legal identity and the use of technology in elections. The first is whether inter-agency collaboration mandated by law offends the independence of the IEBC and the ODPC, both of which are required by law to act independently.

Second, the IEBC, like other data controllers, is expected to put in place data protection security measures commensurate with its important obligations in elections and constitutional referenda. Would electoral data security be assured where there is inter-agency dependence with regard to legal identity verification?

Section 17 of the Election Offences Act, No. 37 of 2016, provides for offences related to the use of technology in elections and provides that it is an offence to intentionally acquire, use, misuse, transfer, alter or delete another person's identification information.

Upon conviction, this offence attracts a fine not exceeding 10 million shillings or imprisonment for a term not exceeding 10 years or both.[22] While this would appear to be an effective protection for voter registers and electoral integrity, the keen observer will note that likely offenders are likely to be those with political clout to access electronic databases without repercussions. At least if one agency is in charge, it will be easier to track offenders than if multiple agencies controlled legal identity databases.

This then questions the policy favoured by the government, namely, to have one single source of personal data. A data breach would put that much more at stake in a single-source system that has at the same time embraced inter-agency collaboration.

6. Non-Consensual Use of Personal Data

There was a hue and cry in June 2021 when Kenyans realized that they had been listed as members of various political parties without their consent or knowledge.[23] The Registrar of Political Parties responded as follows:

"The Election Law requires that only party members would be allowed to participate in the party primaries. We have received numerous complaints from citizens to have been enlisted by political parties that they never subscribed to. Should you find yourself registered as a Member of a Political Party that you didn't apply for, follow the procedure below and we will remove your details:

(i). Write a letter of resignation, with your details to the party.
(ii). Attach a copy of ID to the letter.
(iii). Send a copy of your letter and ID to our office, or scan and forward to **info@orpp.or.ke**

22. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2037%20of%202016. Accessed 10 February 2022.
23. https://www.the-star.co.ke/news/2021-06-19-kenyans-protest-registration-as-party-members-without-consent/. Accessed 10 February 2022.

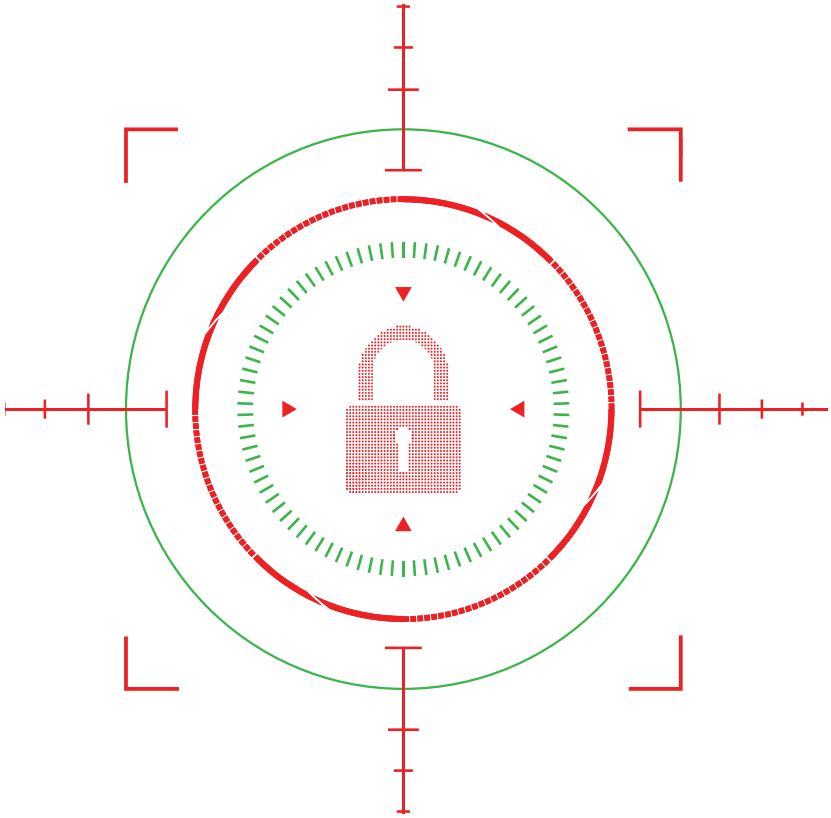
Please note that all resignation letters MUST be sent to a political party that recruited you." [24]

This public fiasco should help the ODPC to cut its teeth as the vanguard of the DPA. It was and remains an important test case for the effectiveness of the complaints and investigations mechanism of the newly established ODPC. Institutional efficiency and effectiveness are important because, as we have explained above, data subjects are obligated by the DPA to follow the internal complaints mechanism before pursuing judicial remedies.

7. Personal Data in Social Media Activism

Kenyan social media platforms are renowned for being vibrant virtual spaces for democratic engagement. However, with democratic fervour, there have been rampant revelations of personal data. Notably, revelations that have been prosecuted or have led to arrests are those that have involved high profile political figures. [25]

The arrests have been carried out under the Computer Misuse and Cybercrimes Act, contentious legislation for the reason that it can be used to advance political ends such as the silencing of free speech by political opponents. For the ordinary citizen, personal data is fair game in Kenyan social media.



24. https://www.orpp.or.ke/index.php/en/8-latest-news/99-procedure-to-de-list-and-join- another-party. Accessed 10 February 2022

25. https://www.standardmedia.co.ke/kenya/article/2001405369/no-more-tea-for-edgar-obare-following-arrest-by-dci. 10 February 2022.

CONCLUSION & RECOMMENDATIONS

1 The DPA establishes the Office of Data Protection Commissioner and confers on it wide-ranging but specific mandates. Our courts have been keen on upholding compliance with the Act. Without adequate funding for the office, data protection will not only remain a mirage but many important governance and development initiatives will also be defeated when challenged in court.

2 In addition to allocating the ODPC more funds, governance and development initiatives requiring massive personal data to implement, whether run by the state or private entities should not be started without a prior data impact assessment and other compliance review by independent experts. This will save time and resources in the long run.

3 Institutional collaboration across agencies is prescribed by the DPA and other statutes, however, the risk of loss of institutional independence is also very high. Greater effort should be put into assuring the Kenyan public and International participants in Kenya's economy that institutional independence is an important principle that will not be compromised.

4 There is a classist tendency by state actors such as investigators and prosecutors to act only when the personal data rights of high profile individuals are violated. It is important that all citizens enjoy equal protection of the laws and institutions, otherwise, the government will continue to struggle convincing citizens that it is in their interest to entrust their digital legal identity rights to state agencies.

5 Civic awareness gaps about personal data rights should be filled by independent organisations and enforcement, which is more difficult to do, should be carried out by state agencies.

6 Almost every state and corporate office will handle personal data. The country will need to step up the training of data privacy & data security professionals to assist the legal compliance departments of many institutions.

7 A culture of respecting personal data rights should be fostered across the country, especially on social media platforms. Kenyans have been leading the pack in digital technology uptake, but the downside is that unlawful posting of personal data has become rampant and in some instances harmful socially and morally.

8 International collaboration, such as was evident during the recent visit by Estonia's Prime Minister, should be embraced but with a caveat that homegrown solutions will always be superior to borrowed ones because each national context is different and faces different problems and risks.

Even though Kenya aims to be a regional if not a global trendsetter, digital Innovation and enterprise informed by context and carried out within the provisions of Kenyan laws will always be superior to indiscriminate copying from other countries.

9 State agencies and offices should be cognizant that despite having executive power, they have obligations under the DPA and other laws that require the state itself to protect data in its custody just like any private entity is required to do. Too often state agencies fail to comprehend that they are both the regulator as well as the regulated when it comes to data protection and privacy.

Beyond having powers, the state also has duties and obligations enforceable by citizens with regard to their personal data and legal identity.

10 As data protection and legal identity are new and evolving areas, stakeholders should remain engaged to assist in the formulation of superior policies, legal reform, development of new technologies and talent nurturing and development.

KICTANet

The Power of Communities

Email: info@kictanet.orke
Web: www.kictanet.or.ke
Twitter: @kictanet