The Right to Privacy in Kenya

Stakeholder Report
Universal Periodic Review
49th[th] Session – Kenya

Submitted by the Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), ICJ-Kenya, Haki Na Sheria Initiative, STOPAIDS, and Privacy International

October 2024

INTRODUCTION

1. This stakeholder report is a submission by **Privacy International** (PI), the **Kenya Legal & Ethical Issues Network on HIV and AIDS** (KELIN), **ICJ-Kenya**, **Haki Na Sheria Initiative**, **STOPAIDS**.
2. **Privacy International (PI)** is a non-governmental, non-profit organisation that researches and advocates globally against government and corporate abuses of data and technology. **KELIN** is an independent Kenyan Civil Society Organization working to protect and promote health related human rights in Kenya by advocating for integration of human rights principles in laws, policies and administrative frameworks; facilitating access to justice in respect to violations of health-related rights; training professionals and communities on rights-based approaches and initiating and participating in strategic partnerships to realize the right to health nationally, regionally and globally. **ICJ-Kenya** (Kenyan Section of the International Commission of Jurists) is a non-governmental membership organization constituting a body of jurists drawn from members of the Bench and Bar in Kenya and the region. It is Africa's only autonomous national section of the International Commission of Jurists. ICJ Kenya has been working in Kenya and around Africa since 1959, and its mission is to promote human rights, democratic governance, justice, and the rule of law in Africa. **Haki na Sheria Initiative (HSI)** is a non-governmental organization based in Garissa, Kenya dedicated to ending the discrimination and promoting the rights of marginalized communities in Northern Kenya. Some of the leading programmes of HSI include the citizenship programme which advocates for equal access to ID for all; digital rights that promotes digital literacy and focuses on bridging the digital divide and access to justice which is key in enforcement of all other human rights through community engagement, capacity buildings & trainings, research, advocacy, legal aid and public interest litigation**. STOPAIDS** is a UK-based membership network with a distinguished thirty-five year history of engagement on international development and HIV and AIDS.

3. KELIN, ICJ-KENYA, HIS, STOPAIDS, and PI wish to bring their concerns about the protection and promotion of the right to privacy, and other rights and freedoms that privacy supports, for consideration in Kenya's upcoming review at the 49th session of the Working Group on the Universal Periodic Review.

The right to privacy

4. Privacy is a fundamental right recognised in numerous international human rights instruments, including in Article 17 of the International Covenant on Civil and Political Rights. The right to privacy enables the exercise of other rights such as the right to freedom of expression, freedom of association, and access to information, and it is essential for the dignity of people and the viability of democratic systems.

5. Interferences with the right to privacy can only be justified when they are established by law, necessary to achieve a legitimate goal, and proportional to the objective pursued.

6. Based on the development of information technologies that have enabled the mass collection, retention and processing of data, protection of the right to privacy has expanded to the processing of personal data. Several international and regional instruments include personal data protection principles.

Follow up to the previous UPR

7. In Kenya's previous review under the UPR Third Cycle[1], the Kenya government received two recommendations explicitly on protecting and respecting the right to privacy with respect to adoption a national data protection law in line with the international standards on the right to privacy, and ensuring that surveillance and profiling of citizens respect the right to privacy including by providing judicial oversight.

8. Furthermore, the government of Kenya received various recommendations on the need to address various policies and practices which criminalised and stigmatised people based on their sexual orientation, as well as on ensuring access to health services and information, and reviewing relevant laws and policies in order to ensure a rights-based legal framework sexual and reproductive health and rights for all in particular young people.

International obligations related to privacy

9. Kenya has ratified the **International Covenant on Civil and Political Rights (ICCPR)**,[2] which uphold the right to privacy.

10. The **Human Rights Committee** has noted that state parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against [arbitrary or unlawful interferences with the right to privacy]," regardless of "whether they emanate from State authorities or from natural or legal persons," and to protect the right to privacy itself.[3]

Domestic laws related to privacy

11. The **Constitution of Kenya** protects the right to privacy by enshrining international law in domestic law and explicitly protecting privacy as a fundamental right. Article 2 § 5

[1] The full list of recommendations are accessible in the report of the UPR Working groups, A/HRC/44/9, https://www.ohchr.org/en/hr-bodies/upr/ke-index

[2] Article 17 of the ICCPR provides, "[n]o one shall be subjected to arbitrary of unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and that "[e]veryone has the right to the protection of the law against such interference or attacks."

[3] General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (1988), para 1.

provides that "general rules of international law shall form part of the law of Kenya," and Article 2 § 6 provides "[a]ny treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution," which includes the UDHR and the ICCPR. Article 31 provides "[e]very person has the right to privacy, which includes the right not to have— (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed."

12. The **Data Protection Act, 2019**, is now the primary law on regulating the processing of personal data in Kenya. Various regulations have been developed to implement the Act including the Data Protection (Compliance & Enforcement) Regulation, 2021, Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021, and the Data Protection (General) Regulations, 2021

13. The **Kenya Information and Communications Act, 1998 (subsequently amended)** regulates the interception and disclosure of communications. Section 31 penalises the unlawful interception and disclosure of communications by telecommunication providers.[4] Section 83W criminalises unauthorized access to, and interception of, a computer service by an individual to "secure access to any computer system for the purpose of obtaining, directly or indirectly, any computer service," or to "intercept or cause to be intercepted, directly or indirectly, any function of, or any data within a computer system."[5]

14. The **Kenya Information and Communications (Consumer Protection) Regulations (2010)** protect subscribers from interception of their communications. Section 15(1) provides, "[s]ubject to the provisions of the Act or any other written law, a licensee shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data."[6]

15. Despite the domestic protections outlined above, the Kenyan government has passed legislation to expand the interception powers of intelligence and law enforcement agencies in ways that could lead to unlawful interference with the right to privacy.

16. The **National Intelligence Service (NIS) Act (2012)** limits the right to privacy and allows the NIS to investigate, monitor or interfere with the communications of people under investigation by the NIS or suspected of committing of an offense.[7] The NIS is meant

[4] Kenya Information and Communications Act, 1998, Section 31.
[5] Kenya Information and Communications Act, 1998, Section 83W.
[6] Kenya Information and Communications (Consumer Protection) Regulations, 2010, Section 15(1).
[7] *See* National Intelligence Service Act, 2012, Section 36 ("(1) The right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person who is subject to investigation by the Service or suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with. (2) The Service shall, prior to taking any action under this section, obtain a warrant under Part V."); *See also* and National Intelligence Service Act, 2012, Section 42(3) (a written authorisation from the Director General of the NIS, to allow the NIS to investigate or respond to a threat to national security, "may authorize any member of the Service to obtain

to be subjected by parliamentary oversight, presumably by the Intelligence and Security Committee, although this is not clear based on the wording of the NIS Act. The Act establishes an Intelligence Service Complaints Board, but very little information is publicly available about the Board and its investigations, if it has engaged in any.

17. The **Prevention of Terrorism Act (2012)** allows the government to limit fundamental rights, including the "the privacy of a person's communication to be investigated, intercepted or otherwise interfered with."[8]

18. The **Security Laws (Amendment) Act (2014)** allows for "the right to privacy . . . [to] be limited . . . for the purpose of intercepting communication directly relevant in the detecting, deterring, and disrupting [sic] terrorism."[9] This Act entrusts the executive to issue regulations to govern interception of communications. This Act also introduced a new amendment to the Prevention of Terrorism Act: a Cabinet Secretary was tasked with making new regulations to govern communications interception by the "national security organs" when related to terrorism investigations. It is unclear if these rules, which have yet to be articulated, would still require the National Security Organs to obtain warrants to intercept communications, as set out in previous laws."[10]

19. The **Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations (2013)** require that each telecommunication provider give the **Kenyan Communications Authority (CA)** access to "its systems, premises, facilities, files, records and other data" for inspection.[11]

20. The **Kenya Information and Communications (Amendment) Act (2013)** requires that telecommunication providers register a person's full name, identity card number, date of birth, gender, and physical and postal addresses before selling a SIM card or other telecommunication services to that person, and provides that such information may be disclosed to the government for the purposes of investigating any criminal offense.[12]

---

any information, material, record, document or thing and for that purpose —(i) enter any place or obtain access to anything; (ii) search for or remove or return, examine, take extracts from, make copies of or record in any manner the information, material, record, documents or thing; (iii) monitor communication;
(iv) install, maintain or remove anything; or (v) take all necessary action, within the law, to preserve national security," and such a written authorisation must also be accompanied by a warrant when it includes monitoring communication.)

[8] Prevention of Terrorism Act, 2012, Section 35.

[9] Security Laws (Amendment) Act, 2014, Section 69.

[10] Privacy International, 'Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya', 15 March 2027, https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya

[11] The Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations, 2013, Regulation 13.

[12] Kenya Information and Communications (Amendment) Act, 2013, Section 12.

21. The **Kenya Information and Communications (Registration of SIM-Cards) Regulations (2015)** requires telecommunication providers to transmit SIM-card registration information to the Communications Authority.[13]

22. The **Computer Misuse and Cybercrimes Act (2018)** provides the government sweeping powers to prosecute vaguely formulated and broadly defined crimes related to computers, and to search computers including by ordering people to decrypt encrypted data. For example, the Act creates content-related offenses for communications that are false[14] or "detrimentally affects"[15] a person, which could give the government unbridled discretion in monitoring communications and prosecuting certain people for certain types of communications, such as government whistle blowers or other individuals acting in the public interest.

AREAS OF CONCERN

23. In the Third Cycle of the UPR, we had highlighted concerns around communications surveillance and in particular the targeting of human rights defenders and journalist.[16] We continue to be concerned by the different invasive surveillance measures and practices deployed by the Kenyan government which undermine the right to privacy which continued to be reported by CSOs.[17] For example, in June 2024 around the mass protests which took place concerns were raised by CSOs of alleged online surveillance including reports that security agencies were using location data from telecommunication operators to locate and then abduct protesters.[18]

I. Elections and the Right to Privacy

24. During Kenya's 2022 elections, the entry into force of the Data Protection Act in November 2019 meant that for the first time the people of Kenya enjoyed specific protections around their personal data in an election cycle. This means that the supported recommendation 142.28 from the previous cycle was at least partially implemented.[19] Equally, however, the 2022 electoral process saw a number of serious concerns related to the right to privacy and data protection of Kenyan citizens arise,

[13] Kenya Information and Communications (Registration of SIM-cards) Regulations, 2015, Regulation 3.
[14] Computer Misuse and Cybercrimes Act, No 5 of 2018, Section 12.
[15] Ibid, Section 16.
[16] Privacy International (PI), the National Coalition of Human Rights Defenders Kenya (NCHRD-K), The Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), and Paradigm Initiative, 'The Right to Privacy in Kenya', Shadow joint stakeholder report, 35th session of the UPR Working Group, July 2019, https://privacyinternational.org/advocacy/3299/right-privacy-kenya
[17] Freedom House, 'Freedom on the Net 2023: Kenya', https://freedomhouse.org/country/kenya/freedom-net/2023
[18] Article 19, 'Kenya: Guarantee internet access and stop surveillance of protesters', 28 June 2024. https://www.article19.org/resources/kenya-guarantee-internet-access-and-stop-surveillance-of-protesters/
[19] A/HRC/44/9, Recommendation 142.28, https://www.ohchr.org/en/hr-bodies/upr/ke-index

concerns which PI assessed in collaboration with the Carter Centre as part of in-country pre-election assessment.[20]

A. Data-sharing of voters' data

25. There are concerns that the access to the voter register is not being effectively regulated, leading to voters' data being erroneously shared. In June 2021 for example, many Kenyans discovered they were registered as members of political parties without their knowledge and possibly without their consent. Over 200 complaints were made to the Office of the Data Protection Commissioner (OPDC) by individuals, and these were acknowledged by the OPDC which stated to work in consultation with the Office of the Registrar of Political Parties.[21]

26. However, information about any steps related to the alleged data violations was too often not relayed to local civil society organizations, and civil society organizations raised concerns that there seemed to be no investigation of what happened, no determination of who was responsible, and that there was no enforcement action taken nor penalties imposed.[22]

B. Challenges to voter registration

27. A further series of concerns arose around electronic voter registration prior to the elections themselves, including those regarding access to voter registration and reliability of electronic devices used to enact this process.

28. Moreover, it was only after a successful legal challenge was brought by a number of organisations, including the Kenyan Human Rights Commission,[23]that the Independent Elections and Boundaries Commission (IEBC) was ordered by the High Court to distribute a manual register to each polling station to allow for voters to be manually verified, with the caveat that it should only be used in instances where

[20] The Carter Center, 'Carter Center Election Expert Mission to Kenya 2022 Final Report', 2023, https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/kenya-2022-elections-final-report.pdf

[21] Kenyan Office of the Data Protection Commissioner, Statement on Alleged Use of Personal Data in Registration to Political Parties without Consent, 25 June 2021, https://www.odpc.go.ke/wp-content/uploads/2024/03/POLITICAL-PARTIES-STATEMENT.pdf

[22] Privacy International, 'Our final report on Kenya's 2022 election in collaboration with The Carter Center Election Expert Mission', 2023, https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

[23] IEBC, "Printed Register of Voters", 5 August 2024, Media Release, https://www.iebc.or.ke/uploads/resources/ZmpeSxiDjm.pdf

electronic kits used for electors to vote, known as KIEMS kits, [24] completely failed and that there was no possibility of repair or replacement.[25]

29. The inclusion of the manual register turned out to be essential since on election day, the IEBC reported that KIEMS kits failures necessitated resort to the manual register in 238 polling stations (of more than 46,000 in total) on election day.[26] Without the alternative of the manual registers, many individuals would have been prevented from voting.[27]

C. Involvement of the private sector in electoral process

30. Furthermore, issues arose with regards to Public-Private Partnerships related to the use of personal data entered into by the Kenyan government with private corporations. These agreements should be drafted to explicitly ensure and take into consideration the respect of the right to privacy and data protection principles, including by laying out safeguards, where personal data is implicated.[28]

31. For example, in the run up to the election, it was reported that the former elections technology provider in Kenya, the company OT Morpho (now known as IDEMIA), withheld Kenyan biometric voter data based on outstanding payments owed by the IEBC and refused to allow the transfer of that data to Smartmatic, who had won the tender process run by the Kenyan government to provide the technology solutions for the 2022 elections.[29] In effect, IDEMIA laid claim to the voter roll and all the information contained therein. The issue was resolved outside of the courts, but it indicates a grey area in relation to the ownership of data produced by electronic information gathering systems.

[24] The Kenyan Integrated Elections Management System (*KIEMS*) and cover all stages of the electoral process except casting ballots and counting, which are still a manual exercise. The electronic kits have a biometric voter registration system that is used to take voters' personal biometric data including facial data, fingerprints and civil data. They also enabled results transmission. See: Citizen Digital, "Elections 2022: What you need to know about IEBC KIEMS kits", 2022, https://www.citizen.digital/news/elections-2022-what-you-need-to-know-about-iebc-kiems-kit-n303613

[25] Citizen Digital, "Elections 2022: What you need to know about IEBC KIEMS kits", 2022, https://www.citizen.digital/news/elections-2022-what-you-need-to-know-about-iebc-kiems-kit-n303613

[26] Privacy International, 'Our final report on Kenya's 2022 election in collaboration with The Carter Center Election Expert Mission', 2023, https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert; Carter Centre (2023) "Carter Centre Election Expert Mission to Kenya Final Report", https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/kenya-2022-elections-final-report.pdf

[27] *ibid*

[28] See Privacy International, 'Safeguards for Public-Private Surveillance Partnerships', 2021, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

[29] Wangeci Thuo, "Squabble over Sh800 million debt could prevent IEBC register", 16 February 2022, *The Informer*, https://theinformer.co.ke/41617/squabble-over-sh800-million-debt-could-prevent-iebc-register/

32. In July 2022, the Chairman of the IEBC announced[30] in a keynote address during the National Election Conference that the voter register would be "available to stakeholders for a minimal fee". The legal basis for the distribution of the voter register, as well as the extent to which it would be modified – if at all – to limit the disclosure of sensitive personal data such as biometric data remains unclear. It also remains unclear whether the IEBC acted on this stated intention.

D. Abnormal vote transfers

33. Many voters raised concerns that the electoral areas in which they had registered had been changed without their knowledge and approval. These issues were brought to the attention of KPMG as it was carrying out its audit of the voter register, as commissioned by the IEBC.[31] KPMG confirmed in its audit report that it had identified a trend of "abnormal" vote transfers[32] between the 2017 general election and May 2022. This phenomenon is inconsistent with the Elections Act of 2011, which states that only a registered voter can transfer their own registration to a different electoral area. The IEBC later announced that three IEBC officials had been arrested for involvement in illegal transfer of voters. On July 7, the Chair of the IEBC announced that those officials were suspended and referred to the director of public prosecutions.[33]

34. Uncertainty around this issue regarding personal data triggered by the transfer of data in the voter register underscored the need for increased transparency and effective public communications around data protection as provided for under the Data Protection Act, 2019.

II. The Right to Health and the Use of New Technologies

35. Although new technologies can help transform and improve access to health[34], the process of digitizing the healthcare sector can expose users and the wider health ecosystem to new risks, which in part stem from decisions that are made when implementing digital health systems.[35] There are increasing concerns regarding privacy and security of personal data arising from the use of new technologies and

[30] IEBC, "Chairman's Keynote Address During The National Election Conference 2022, Held On The 11th And 12th July 2022 At The Kenyatta National Conference Centre Nairobi", July 2022, https://www.iebc.or.ke/uploads/resources/6KLXraSE7u.pdf
[31] KPMG, "Independent Audit of the Register of Voters: Final Audit Report, 16 June 2022, https://www.iebc.or.ke/uploads/resources/0CpUTC8Q5a.pdf
[32] IEBC, "Audit Report on the Registration of Voters", 20 June 2022, Media Briefing, https://www.iebc.or.ke/uploads/resources/JqmDO7vRL0.pdf
[33] IEBC in *The Nation* [Youtube], "Chebukati on illegal transfer of voters", 7 July 2022, https://www.youtube.com/watch?v=hMdoJimxpd0
[34] See: WHO (2021) Global strategy on digital health 2020-2025, available at https://www.who.int/publications/i/item/9789240020924
[35] A/HRC/53/65; Privacy International, 'Why we need to talk about digital health', 27 November 2021, https://privacyinternational.org/long-read/4674/why-we-need-talk-about-digital-health; Privacy International, 'Digital Health: what does it mean for your rights and freedoms', July 2024, https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms

innovation in the health sector.[36] As well as concerns relating to the negative impacts that digitizing can have on specific communities including young people, people from marginalised or criminalised communities such as people living with HIV/AIDS, migrants and women and girls as has been the case in Kenya.[37] Frequently, these communities are excluded from the process to develop public policies for implementing new technologies that impact them.[38]

36. Kenya, like many other countries, has seen an uptake in the use and implementation of digital health technologies from patient administration and hospital billing functions, to management of clinical services to outpatients and wider electronic health (e-health) and mobile(m-health) initiatives.[39] Some of the main initiatives which have been rolled out include the District Health Information System (DHIS2)[40] for centralised population data collection, the OpenMRS for managing TB and HIV programmes in smaller clinics, and the Kenya Master Health Facility List (KMHFL), which is an application that covers all health facilities and community units in Kenya.[41] As well as various e-health initiatives such as mTiba, a health wallet manged by Safaricom to send, save and spend funds for medical treatment and medication at M-TIBA-registered clinics and hospitals;[42] myDawa which is an online registered pharmacy;[43] and Maisha Meds, a network of online pharmacies and clinics across East Africa, who are funded by US-based academic institutions like the Bill and Melinda Gates Foundation, global agencies such as USAID, and private pharmaceutical companies like Pfizer.[44]

37. In the following sections we outline some of the key concerns which PI, KELIN, and other NGOs have observed in Kenya.

A. The lack of effective regulation of health data and increasing innovation and technology in the health sector

38. As noted above whilst various digital health initiatives have already been rolled out by the Kenyan government[45] as well by other third parties, including the private sector.

[36] Privacy International, 'Digital Health: what does it mean for your rights and freedoms', July 2024, https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms
[37] See: A/HRC/53/65, para 62
[38] See: A/HRC/53/65, para 9 and Section B "Participation"; For further on this issue see: https://www.graduateinstitute.ch/DigitalHealth-Rights
[39] Government of Kenya, Third Medium Term Plan 2018 – 2022, https://vision2030.go.ke/publication/third-medium-term-plan-2018-2022/ ; TransformHealth Kenya, 'Landscape Analysis of Digital Health & Universal Health Coverage in Kenya', April 2022, https://www.kelinkenya.org/wp-content/uploads/2023/01/Landscape-Analysis-of-Digital-Health-Universal-Health-Coverage-in-Kenya-00000003.pdf
[40] More information: https://dhis2.org/
[41] Kenya Master Health Facility Registry, https://kmhfr.health.go.ke/
[42] Vodafone, Safaricom's M-TIBA, 28 August 2020, https://www.vodafone.com/digital-society/safaricoms-m-tiba
[43] More information: https://mydawa.com/
[44] More information: https://maishameds.org/
[45] TransformHealth Kenya, 'Landscape Analysis of Digital Health & Universal Health Coverage in Kenya', April 2022, https://www.kelinkenya.org/wp-content/uploads/2023/01/Landscape-Analysis-of-Digital-Health-Universal-Health-Coverage-in-Kenya-00000003.pdf

These have been deployed in an ineffective and fragmented regulatory and legislative void with no specific legislation on digital health and reports of weak enforcement of the existing Data Protection Act, 2019, in relations to regulating the processing of personal data, including health data.[46] As a result, CSOs in Kenya have called for the urgent need to effectively regulate the digital health sector to ensure people and their data are protected.[47]

39. Prior to the adoption of the Digital Health Act (2023), there were five specific policies and standards that guided digital health initiatives in Kenya: (i) Kenya National eHealth Strategy (2011); (ii) Kenya National eHealth Policy (2016-2030); (iii) Kenya Standards and Guidelines for mHealth Systems (2017); (iv) Health Information Policy (2014-2030) and; (v) Health Sector ICT Standards and Guidelines (2013) and; the Health Act (2017). These policies were complemented by core legal frameworks such as: (i) the Data Protection Act (2019); (ii) Kenya Information and Communications Act (1998); the Science, Technology, and Innovation Act (2013); the Computer Misuse and Cybercrimes Act (2018); and the ICT Policy (2019).

40. Considering this previously fragmented approach, despite concerns with the process by which the Act was adopted and shortcomings in the adopted text, the Digital Health Act was welcomed by CSOs advocating for the regulation of digital health in Kenya as it provided a comprehensive framework for the regulation of the provision of digital health services. It also established a comprehensive integrated digital health information system and the creation of a new institution, the Digital Health Agency (DHA).[48]

41. However, in July 2024 the Act was deemed unconstitutional by the Kenyan High Court for lack of adequate public participation in the law-making process and for violation of constitutional provisions that it has not complied with constitutional requirement on public participation, and it ordered Parliament to undertake an adequate, reasonable, sufficient and inclusive public participation as well as undertake a wider sensitization on the law itself before enacting it.[49] This has meant that Kenya is back to being in a situation where the regulation of digital health innovation and technology remains fragmented and insufficient. Furthermore, given issues with lack of implementation of the Data Protection Act (2019) by actors deploying digital health

[46] Digital Health and Rights Project Consortium (2022) Digital health and rights of young adults in Ghana, Vietnam, Kenya: final project report, page 3 and 19, https://repository.graduateinstitute.ch/record/300591?_ga=2.99187678.1735834843.1682602161-345088509.1672743223&v=pdf

[47] KELIN, 'Harnessing the Power of Digital Health Technologies to Transform Healthcare Delivery in Kenya', 9 August 2023, https://www.kelinkenya.org/harnessing-the-power-of-digital-health-technologies-to-transform-healthcare-delivery-in-kenya/

[48] See: CIPESA, 'Does Kenya's Digital Health Act Mark A New Era for Data Governance and Regulation?', 3 May 2024, https://cipesa.org/2024/05/does-kenyas-digital-health-act-mark-a-new-era-for-data-governance-and-regulation/; KICTANET, 'Kenya's Digital Health Act: A Leap Forward in Data Governance', 24 October 2023, https://www.kictanet.or.ke/kenyas-digital-health-act-a-leap-forward-in-data-governance/

[49] ICJ Kenya, 'Case Summary – Unconstitutionality of Social Health Insurance Act, Primary Health Care Act, Digital Health Act', 2024, https://icj-kenya.org/news/sdm_downloads/case-summary-unconstitutionality-of-social-health-insurance-act-primary-health-care-act-digital-health-act/

initiatives, including the private sector, the lack of specific regulation on digital health is raising concerns.[50] It is essential that the governance and regulatory gaps are addressed given the "unprecedented risks to the right to be free from arbitrary or unlawful interference with one's privacy" posed by the use of digital health innovation and technologies, as recognise by the UN Special Rapporteur on the right to health.[51]

B. Proliferation of private sector health apps

42. Kenya has seen significant uptake and deployment of health apps. In 2023 it was reported that at least 180 health apps were operating in Kenya.[52] However, concerns have been raised as to how these are being deployed by startups and other private sector actors and the implications for users and their rights given the weak enforcement of the Data Protection Act, 2019, and the regulatory and legal void highlighted above when it comes specifically to digital health.[53]

43. These apps are developed by private sector actors and recommended by government health agencies. For example, the m-mama programme is being brought to Kenya through a partnership between the Government of Kenya, USAID, the Vodafone Foundation, Safaricom, and the M-Pesa Foundation[54] and it raises concerns how the data will be processed by these different actors.[55] These types of public-private partnerships in the digital healthcare sector are proliferating, but opportunities for scrutiny and transparency of such partnerships is limited. This 'government-industry complex' has largely evolved in a weak regulatory framework. States have obligations to effectively regulate the role that industry should play in the health sector and the level of accountability and scrutiny they should be subject to.[56]

44. There are also concerns about how the processing of personal data, including health data by these apps is being managed given well-documented risks about apps sharing health data with third parties to generate profit.[57] Research by DHPR in Kenya has

[50] KELIN, 'Harnessing the Power of Digital Health Technologies to Transform Healthcare Delivery in Kenya', 9 August 2023, https://www.kelinkenya.org/harnessing-the-power-of-digital-health-technologies-to-transform-healthcare-delivery-in-kenya/
[51] See: A/HRC/53/65, para 59.
[52] Kabui Mwangi, Number of Kenyans seeking digital health treatment rises, study shows, 2 May 2024, *Business Daily*, https://www.businessdailyafrica.com/bd/corporate/health/number-of-kenyans-seeking-digital-health-treatment-rises--4611174
[53] See: A/HRC/53/65, para 59.
[54] Kenyan Ministry of Health, $18 Million Public-Private Partnership To Save Lives Of Mothers And Babies In Kenya, 21 June 2023, 21 June 2023, MOH News, https://www.health.go.ke/18-million-public-private-partnership-save-lives-mothers-and-babies-kenya
[55] Privacy International, 'How digital health apps can exploit users' data', 4 March 2022, https://privacyinternational.org/long-read/4804/how-digital-health-apps-can-exploit-users-data
[56] Privacy International, 'Safeguards for Public-Private Surveillance Partnerships', available at: https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships
[57] Privacy International, 'An unhealthy diet of targeted ads: an investigation into how the diet industry exploits our data', 4 August 2021, https://privacyinternational.org/long-read/4603/unhealthy-diet-targeted-ads-investigation-how-diet-industry-exploits-our-data

shown that these are concerns for young people in Kenya about "hostile actors" having access to information about them.[58]

C. Use of social media to access and provide health information and services

45. Social media is increasingly becoming a space for young people to seek and share information on health issues, in particular sexual and reproductive health and sexuality.[59] Research undertaken by the Digital Health and Rights Projects (DHRP), a participatory action research project,[60] revealed that young adults in Kenya reported predominantly using Google, social media, and social chat groups for seeking health information.[61] For example, Love Matters Kenya is a Facebook group with 1.8 million followers, which provides a space for advice and debate on sexuality and sexual and reproductive health information that is both accurate and provides a positive approach to sex for its followers. Another example is the use of Facebook and WhatsApp groups by HIV peer support outreach workers during the Covid-19 pandemic, to provide psychosocial support, treatment adherence advice, and coordinate medical and financial aid during Covid-19 restrictions. [62]

46. Therefore, social media has filled a gap for some marginalised groups who may otherwise lack access to vital health information, and has empowered other communities such as women and young people to self-manage their healthcare.[63] They have reported that it gives them anonymous access to HIV, Covid-19 and sexual and reproductive health information they urgently need, which they feel unsafe seeking elsewhere, including public run health centres, for fear of stigma and violence. Persons living with HIV, young men and women also reported being subject to harassment by a health care professional, and therefore these tools are safer and more accessible compared to attending healthcare facilities.[64]
47. However, there are concerns about the accuracy of information provided and safety when using social media and other applications. Participants in the research conducted by DHRP, which included young adults, also disclosed harms linked to seeking health information online including data mining, cyberbullying, and anxiety of

[58] Digital Health and Rights Project Consortium (2022) Digital health and rights of young adults in Ghana, Vietnam, Kenya: final project report, page 19, https://repository.graduateinstitute.ch/record/300591?_ga=2.99187678.1735834843.1682602161-345088509.1672743223&v=pdf
[59] See: A/HRC/53/65, para 5 and 54
[60] For more information: Digital Health and Rights Project, https://warwick.ac.uk/fac/cross_fac/cim/research/digital-health-rights/
[61] Digital Health and Rights Project, 'Digitalisation, Health and Participation: a Brief on Kenya', page 4, https://warwick.ac.uk/fac/cross_fac/cim/research/digital-health-rights/publications/dhrp_-_kenya_final_version.pdf
[62] Digital Health and Rights Project Consortium (2022) Digital health and rights of young adults in Ghana, Vietnam, Kenya: final project report, page 13 and 15, https://repository.graduateinstitute.ch/record/300591?_ga=2.99187678.1735834843.1682602161-345088509.1672743223&v=pdf
[63] *ibid*, page 14
[64] *ibid*, page 13-14

surveillance, especially for young people living with HIV, key populations[65], and young women seeking information on SRH or access to safe medical abortion.[66]

48. Furthermore, they are concerns about accessibility and digital exclusion as not everyone owns a smartphone or device to access this information. Therefore, sharing devices within a family remains very common practice and decreases the privacy and autonomy of users. Furthermore, the ability to afford increasing costs of data effects accessibility as well as language barriers as most social media and online platforms provide services in English only.[67]

D. Surveillance of women and girls living with HIV

49. In 2023, KELIN carried out a study on the impact of HIV index testing[68] on access to sexual and reproductive (S&R) health services among young women and girls in four sub-counties in Kisumu County.[69] Study participants indicated that health care providers lacked training in data privacy and data security issues, and a need for more robust privacy and confidentiality protections of services, for example through encryption.[70] These comments followed instances where there had been involuntary disclosure of service users' HIV status during partner notification processes, as well as incidences where healthcare workers had breached confidentiality either involuntarily or voluntarily.[71] As well as general concerns regarding who had access to their electronic medical record systems (EMR)[72].

50. The study highlighted concerns around HIV Index testing, including documented practices of disclosure infractions undermining efforts to ensure safe and secure access to S&R health. A key recommendation of the study was to raise awareness about privacy and data protection responsibilities of healthcare providers, including their obligations under the Data Protection Act 2019 as well as the need to develop further regulation and guidance to protect people and their data in a healthcare context.[73]

---

[65] Key populations refer to groups who that are particularly vulnerable to HIV and frequently lack adequate access to services. These included but are not limited to: gay men and other men who have sex with men, sex workers, transgender people, people who inject drugs and prisoners and other incarcerated people. For more details: https://www.unaids.org/en/topic/key-populations

[66] Digital Health and Rights Project Consortium (2022) Digital health and rights of young adults in Ghana, Vietnam, Kenya: final project report, page 17, https://repository.graduateinstitute.ch/record/300591?_ga=2.99187678.1735834843.1682602161-345088509.1672743223&v=pdf

[67] Ibid, page 16

[68] Also known as Assisted Partner Notification Services (APS)

[69] Kisumu was selected because it is among the 4 counties with the highest HIV prevalence rates in the country and is regarded as one of the key counties in need of intensified focus to prevent new HIV infections.

[70] KELIN (2023) Impact of HIV index testing on access to sexual and reproductive health (SRH) services for young women and girls in Kenya: A participatory action research study, Research report, https://www.kelinkenya.org/wp-content/uploads/2023/04/HIV-Index-Testing-Research.pdf

[71] *ibid*, page 35-36

[72] *ibid*, page 39

[73] KELIN (2023). Impact of HIV index testing on access to sexual and reproductive health (SRH) services for young women and girls in Kenya: A participatory action research study. Research report, page 47-48. https://www.kelinkenya.org/wp-content/uploads/2023/04/HIV-Index-Testing-Research.pdf

E. Safe access to accurate sexual and reproductive health

51. Despite many users, in particular young people, accessing sexual and reproductive (S&R) health information and services online[74] which was also reported in a case-study produced by PI and KELIN that technology-based tools facilitating access to sexual and reproductive rights are gradually emerging in Kenya.[75]

52. However, research by DHRP has reported instances where people seeking information on S&R healthcare online in Kenya are experiencing concerns around accuracy of the information being shared as well as privacy and confidentiality[76] when such tools and the those processing personal data do provide data protection policies to provide assurance to people as to how their data will be processed and measures to protect their data and their rights.[77]

53. Furthermore, expansive data processing activities resulting from the use of such tools can lead to heightened risks to users' privacy, which in a context where we have criminalisation of S&R healthcare such as access to safe abortion the risk is further heightened.[78]

III. Digitalisation of essential services and social protection programmes

54. Over the years and across many jurisdictions, there has been a growing reliance on digital technologies for accessing and delivering public services and social protection programs.[79] These technologies are frequently used to identify beneficiaries, assess eligibility, distribute assistance, and purportedly combat fraud.[80] While we recognise that certain technologies may enhance access to public services and social protection, the associated risks must not be underestimated.

55. The increasing dependence on digital platforms has made digital access a prerequisite for participation in society, excluding many and creating new barriers that

---

[74] Macharia P, Pérez-Navarro A, Inwani I, Nduati R, Carrion C. An Exploratory Study of Current Sources of Adolescent Sexual and Reproductive Health Information in Kenya and Their Limitations: Are Mobile Phone Technologies the Answer? International Journal of Sex Health, 16 May 2021, 33(3):357-370, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10929578/

[75] Privacy International, 'Country case-study: sexual and reproductive rights in Kenya', 4 June 2020, https://privacyinternational.org/long-read/3859/country-case-study-sexual-and-reproductive-rights-kenya

[76] Digital Health and Rights Project Consortium (2022) Digital health and rights of young adults in Ghana, Vietnam, Kenya: final project report, https://repository.graduateinstitute.ch/record/300591?_ga=2.99187678.1735834843.1682602161-345088509.1672743223&v=pdf

[77] Privacy International, 'Country case-study: sexual and reproductive rights in Kenya', 4 June 2020, https://privacyinternational.org/long-read/3859/country-case-study-sexual-and-reproductive-rights-kenya

[78] See: A/HRC/53/65, para 55-56; Privacy International, 'Health Tech In Sexual and Reproductive Rights', https://privacyinternational.org/learn/health-tech-sexual-and-reproductive-rights

[79] A/74/493

[80] See: Privacy International, Social Protection Programmes', https://privacyinternational.org/learn/social-protection-programmes, Privacy International, 'Stage 3: The policing of social benefits: punishing poverty', 2019, https://privacyinternational.org/node/3114

disproportionately impact marginalised groups.[81] Also, it has been widely recognised that these practices have had discriminatory effects.[82] Additionally, this trend demands large-scale data processing, often forcing individuals to trade their right to privacy in exchange for essential services necessary for survival and dignity.[83]

56. In the following sections, we outline some of the key concerns related to these issues observed in Kenya.

A. Deployment of a national digital identity system

57. Over the years, we have raised specific concerns about the development of national digital identity systems.[84] These systems have been recognised to raise significant implications for the right to privacy and data protection.[85] Furthermore, the effects of such systems can lead to exclusion,[86] an issue that has been also highlighted by the Secretary-General of the United Nations in his report on the role of new technologies in the realisation of economic, social, and cultural rights.[87]

58. Kenya, like many countries, has been advancing its digital agenda by attempting to introduce a national digital ID system.[88] In 2018, the Kenyan government tried to introduce the Huduma Namba project. The promulgation in January 2019 of the Statute Law (Miscellaneous Amendment) Act, 2018 (SLMAA) amended the Registration of Persons Act to enable the government to collect extensive personal data on Kenyans and registered foreigners in a national database including: land and

[81] See: A/74/493; A/HRC/48/31; Privacy International, 'Exclusion and identity: Life without ID', 14 December 2018, https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id, Privacy International, 'When ID leaves you without identity: the case of double registration in Kenya', 20 December 2021, https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya

[82] A/74/493; A/74/493

[83] Privacy International, 'Digital National ID systems: Ways, shapes and forms', 26 October 2021, https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms

[84] See: ICJ-Kenya, 'What State should Do To Successfully Roll Out New Digital ID System', 10 November 2023, https://icj-kenya.org/news/what-state-should-do-to-successfully-roll-out-new-digital-id-system/; Haki Na Sheria Initiative, 'Crafting a Democratic Blueprint: Designing Digital Identity Systems for the People', https://drive.google.com/file/d/1MwPqQNWMqK-tAdXU3bsN1FqYAsEJvji5/view; Haki Na Sheria Initiative (2021) 'Biometric Purgatory: How the Double Registration of Vulnerable Kenyan Citizens in the UNHCR Database Left Them at Risk of Stateless', https://drive.google.com/file/d/1ziw6aEqHdAL5Ly7Ct51TA_CN-ZaX-XAp/view; Privacy International, 'The 'Identity Crisis' around the world', 16 September 2023, https://privacyinternational.org/explainer/5126/identity-crisis-around-world; Privacy International, Demanding identity systems on our terms, https://privacyinternational.org/campaigns/demanding-identity-systems-our-terms

[85] Privacy International (2020) A Guide to Litigating Identity Systems, https://privacyinternational.org/learning-resources/guide-litigating-identity-systems.

[86] Privacy International, 'Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations', 29 March 2021, https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible

[87] A/HRC/43/29

[88] Privacy International, 'The 'Identity Crisis' around the world', 16 September 2023, https://privacyinternational.org/explainer/5126/identity-crisis-around-world; Privacy International, Demanding identity systems on our terms, https://privacyinternational.org/campaigns/demanding-identity-systems-our-terms

house reference number, biometric data such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form. Amongst other initiatives, the Huduma Numba project established the National Identity Integrated Management System (NIIMS), a centralised database purposed to consolidate all government records about an individual into a single ID system.[89]

59. This system was developed without public consultation or adequate safeguards, and there were also concerns that this system could also lead to the exclusion of vulnerable communities, including the Kenyan Nubian and Somali communities.[90]

60. Towards the end of 2019, three petitions were filed at the Kenyan High Court challenging various aspects of the proposed NIIMS.[91] The Kenyan High Court ruled that the system needed to be halted until there is "an appropriate and comprehensive regulatory framework on the implementation of NIIMS". It also found that the processing of GPS co-coordinates and DNA was intrusive and unnecessary for identification purposes and so also concluded that the sections in the Registration of Persons Act requiring such collection conflict with Article 31 of the Constitution and are unconstitutional, null and void. Unfortunately, the Court failed to address the issue of exclusion despite recognising the risks, and overall the Court agreed that the processing of biometric data was necessary for the purpose of identification.[92] And ultimately, the Court missed an opportunity to question the system's overall purpose and structure.[93] Despite these shortcomings, the High Court's judgement led to the Huduma Numba system being halted,[94] and then ultimately dropped.

61. However, in early 2023 the government announced the implementation of a new third-generation ID system, the Maisha Namba, with a roll-out initially announced for October 2023.[95] The term "Maisha Namba" refers to an identity ecosystem comprising four interrelated aspects: Maisha Namba, Maisha Card, Digital ID, and the National Population Master Register. Maisha Namba specifically refers to the Unique Personal Identifier assigned at birth registration, which will remain in use until death

[89] Privacy International, 'Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba', 27 January 2022, https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

[90] Maureen Kakah, Nubian group opposes use of new ID system, 22 February 2019, *Nation*, https://www.nation.co.ke/news/Group-opposes-use-of-new-ID-system/1056-4994288-pt4cru/index.html

[91] Petition 56, 58 & 59 of 2019 (Consolidated), http://kenyalaw.org/caselaw/cases/view/189189/

[92] Privacy International, 'Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons', 24 February 2020, https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

[93] Privacy International, 'Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons', 24 February 2020, https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

[94] Namati, 'Press release: Huduma Numba Stopped!', 31 January 2020, https://namati.org/news-stories/press-release-huduma-namba-stopped/

[95] Derrick Okubasu, Govt Unveils Maisha Namba After Signing Deal With UN. 14 August 2023, *Kenyas.co.ke*, https://www.kenyans.co.ke/news/92093-maisha-namba-govt-unveils-new-name-digital-id-after-signing-deal-un

registration.[96] Similarly to its predecessor the Huduma Numba, the process of implementation of the Maisha Numba was flawed with a lack of meaningful participation, and a repetition of the concerns addressed by the High Court in its judgement about the need for effective regulation of the processing of personal data including biometric data, the need for safeguards to protect people and their data from misuse and abuse by the government but also the private sector, and concerns of exclusion and discrimination for those unable to easily register because of administrative barriers amongst others.[97] Since the onset the Maisha Numba ecosystem has been repeatedly challenged in court by CSOs which has led to the registration being halted on several occasions.[98]

62. In December 2023, our partner Haki Na Sheria Initiative field a petition against the Government challenging the roll out of the Maisha Nama Digital Identity Ecosystem.[99] Haki Na Sheria Initiative flagged potential constitutional violations, including of (i) the right to privacy given the vast processing activities the system would entail including extensive data sharing amongst government bodies and with the private sector, and (ii) discrimination against marginalised communities who have faced challenges to access citizenship rights including marginalized and minority communities, particularly in Northern Kenya, Coastal Kenya, and other rural areas that face regulatory and administrative challenges in the acquisition of national IDs including secondary vetting and the inaccessibility of registration offices. Further the children of people from these communities as well as around 40,000 double-registered individuals who were erroneously registered as refugees despite being Kenyans and who are now facing challenges to be able to be registered in the national identity system.[100]

---

[96] KICTANET, 'Understanding Maisha Namba: Kenya's New Digital Identity System', 10 November 2022, available at:https://www.kictanet.or.ke/understanding-maisha-namba-kenyas-new-digital-identity-system/

[97] ICJ-Kenya, 'What State should Do To Successfully Roll Out New Digital ID System', 10 November 2023, https://icj-kenya.org/news/what-state-should-do-to-successfully-roll-out-new-digital-id-system/; Kenya Human Rights Commission, 'Government shouldn't force flawed digital ID system on Kenya', 27 February 2024, Press release, https://khrc.or.ke/press-release/government-shouldnt-force-flawed-digital-id-system-on-kenya/; Rachel Achieng' and Joshua Kitili, 'An Overview of the Digital ID system and the Unique Personal Identifier in Kenya', 28 February 2023, CIPIT, https://cipit.strathmore.edu/an-overview-of-the-digital-id-system-and-the-unique-personal-identifier-in-kenya/

[98] See: Sam Kilpagat, High Court puts the brakes on Kindiki's plan to introduce Maisha Namba, 5 December 2023, *Nation*, available at:https://nation.africa/kenya/news/high-court-puts-the-brakes-on-kindiki-s-plan-to-introduce-maisha-namba-4454474; Nixon Kanali, Kenya's High Court lifts injunction on new digital IDs issuance, 26 February 2024, *ITWeb*, https://itweb.africa/content/raYAyqorp3pMJ38N; Sam Kilpagat, High Court stops implementation of Maisha Card, 25 July 2024, *Nation,* https://nation.africa/kenya/news/high-court-stops-implementation-of-maisha-card-4702756; Emanuel Wanjala, Court rescinds earlier orders blocking maisha namba rollout, 12 August 2024, *The Star*, https://www.the-star.co.ke/news/2024-08-12-court-rescinds-earlier-orders-blocking-maisha-namba-rollout

[99] Haki na Sheria Initiative, 'Press Statement: Civil Society seeks reform of Kenya's Digital ID System', 20 December 2023, https://drive.google.com/file/d/1gROLgdLyJJLifgtjM39MPMEPtyT27yTE/view

[100] See: Haki Na Sheria Initiative (2021) Biometric Purgatory: How the Double Registration of Vulnerable Kenyan Citizens in the UNHCR Database Left Them at Risk of Stateless, https://drive.google.com/file/d/1ziw6aEqHdAL5Ly7Ct51TA_CN-ZaX-XAp/view; Privacy International, 'When ID leaves you without identity: the case of double registration in Kenya', 20 December 2021, https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya

63. These concerns raised by Haki Na Sheria Initiative and the other petitioners as well as PI[101] have been recognised by Courts around the world[102] and also highlighted by the Secretary-General of the United Nations in his report on the role of new technologies in the realisation of economic, social, and cultural rights.[103] The case is was due to be heard on 5th October 2024 but it was announced that the hearing has been adjourned until March 2025.

B. WorldCoin

64. Worldcoin[104] introduced its iris-scanning scheme in Kenya as part of a new identity and cryptocurrency system.[105] In August 2023, the government suspended its operations, citing concerns over data protection and the project's legality.[106] Similarly, the Office of the Data Protection Commissioner warned citizens against engaging with the system, noting Worldcoin's failure to comply with the Data Protection Act.[107] Moreover, a parliamentary committee recommended shutting down the company altogether, pointing to violations of the Computer Misuse and Cybercrimes Act and even labelling its activities as potential espionage.[108]

65. After a year of suspension, Worldcoin resumed operations in June 2024,[109] though it remains unclear whether the issues that led to the halt have been resolved. Notably, other countries are scrutinising Worldcoin's practices, particularly concerning data protection and biometric use.[110] Additionally, an MIT Review investigation published

[101] In June 2024, Privacy International filed expert witness testimony before the court to assist the adjudication of the case. PI highlighted concerns emerging from identity systems around the world and proposed measures to mitigate them, addressing issues such as biometrics, exclusion, unique identifiers, data breaches/security, function creep, data retention and the effective application of data protection law. The witness statement can be access on PI's website: https://privacyinternational.org/advocacy/5344/privacy-international-submits-expert-witness-testimony-haki-na-sherias-case

[102] Privacy International (2020) A Guide to Litigating Identity Systems, https://privacyinternational.org/learning-resources/guide-litigating-identity-systems

[103] A/HRC/43/29, para 33.

[104] See: https://worldcoin.org/

[105] Annie Njanji, Kenya suspends Worldcoin scans over security, privacy and financial concerns, 2 August 2023, *Tech Crunch*, https://techcrunch.com/2023/08/02/kenya-suspends-worldcoin-scans-over-security-privacy-and-financial-concerns/

[106] Natasha Kahungi, Kenya government suspends Worldcoin cryptosystem operations amidst investigations into privacy and legality, 2 August 2023, Jurists News, https://www.jurist.org/news/2023/08/kenya-government-suspends-worldcoin-operations-amidst-investigations-into-privacy-and-legality/

[107] Natasha Kahungi, Kenya High Court halts Worldcoin data processing amid privacy concerns, 28 August 2023, *Jurists news*, https://www.jurist.org/news/2023/08/kenya-high-court-halts-worldcoin-data-processing-amid-privacy-concerns/

[108] Digwatch, 'Worldcoin allowed to resume operations in Kenya after year-long probe', 20 June 2024, https://dig.watch/updates/worldcoin-allowed-to-resume-operations-in-kenya-after-year-long-probe

[109] Reuters, Worldcoin to resume Kenya operations after police drop investigation, 20 June 2024, https://www.reuters.com/world/africa/worldcoin-resume-kenya-operations-after-police-drop-investigation-2024-06-20/

[110] Natasha Lomas, Worldcoin's official launch triggers swift privacy scrutiny in Europe, 28 July 2023, *Tech Crunch*, https://techcrunch.com/2023/07/28/world-gdpr-concerns/

in 2023 revealed that Worldcoin "used deceptive marketing practices, collected more personal data than it disclosed, and failed to obtain meaningful informed consent."[111]

RECOMMENDATIONS

In light of the above considerations, KELIN, ICJ-Kenya, Haki Na Sheria Initiative, STOPAIDS, and PI make the following recommendations to government of Kenya:

1. Strengthen the implementation of Data Protection Act, 2019 and make clear in law and in relevant guidelines that personal data from the electoral register which has been made accessible is still subject to, and protected, by data protection law, including for onward processing.

2. Ensure that there is an effective legal and regulatory framework in place to guarantee a human rights-based approach in the design and deployment of digital health technologies by the government and non-state actors which provides for the meaningful participation of affected communities and protects people's right to health and privacy amongst other fundamental rights including non-discrimination and equality, by reinitiating a legislative process to enact a comprehensive digital health legislation that aligns with the Constitution.

3. Take steps to ensure that the necessary protections are in place for all, but in particular women and girls, persons living with HIV, and young people, to access sexual and reproductive health information and services safely and securely, and adopt a strong regulatory framework to protect the confidentiality and privacy of their data and health status including through the effective implementation of the Data Protection Act, 2019.

4. Review and redesign the proposed digital identity system, the Maisha Numba, to ensure it aligns with Kenya's national and international human rights obligations in its design and implementation, and adopts legal, policy and technical safeguards to prevent exclusion, unlawful surveillance and exploitation of the data processed for identification purposes.

5. Take measure to ensure that steps taken to adopting digital public infrastructures abide by Kenya's national and human rights obligations to protect people and their rights including the Data Protection Act, 2019, and in particular effectively regulate the involvement of the private sector in such initiatives.

[111] Eileen Guo and Adi Renaldi, Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users, 6 April 2022, *MIT Review*, https://www.technologyreview.com/2022/04/06/1048981/worldcoin-cryptocurrency-biometrics-web3/