Amnesty International Submission to the Office of the United Nations High Commissioner for Human Rights on the Impact of Digital Technologies on Social Protection and Human Rights

Amnesty International (Amnesty) welcomes the important initiative taken by the United Nations Special Rapporteur on extreme poverty and human rights, Philip Alston, to prepare a thematic report to the UN General Assembly examining the human rights impacts, especially on those living in poverty, of the introduction of digital technologies in the implementation of national social protection systems.

Following the invitation by the Special Rapporteur to prepare written input to aid the preparation of the report, Amnesty is pleased to submit feedback and recommendations for consideration focusing on questions 1, 3 and 5. We have also included in the annex Amnesty's report *Trapped in the Matrix: Secrecy, Stigma and Bias in the Met's Gangs Database* and Amnesty International and Access Now's Toronto Declaration on protecting the rights to equality and non-discrimination in machine learning systems. The organization welcomes and appreciates the opportunity to provide this submission.

1. **Are there specific case studies involving the introduction of digital technologies in national social protection systems?**

In January 2019, President Uhuru Kenyatta passed into law an amendment to section 9A of the Registration of Persons Act to include a national ID registration system as a "single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya." [1] The National Integrated Identity Management System (NIIMS), also known as Huduma Namba (Swahili for "service number"), was rolled out nationally on 2 April 2019.

NIIMS requires all Kenyan citizens and diaspora living abroad, as well as foreign nationals and refugees within Kenya's borders from the age of six to provide biometric data to the government in order to obtain a card which will be the only form of ID recognised in the country, and in order to access services.

The term 'biometric' has been defined in the Registration of Persons Act to include "fingerprints, hand geometry, earlobe geometry, retina and iris patters, voice waves and Deoxyribonucleic Acid (DNA) in digital form."[2] Collection of GPS coordinates of a person's place of residence are provided for under the Amended Reg of Persons Act. NIIMS allows the government to collect a huge range of biometric data on an unprecedented scale; no other state has created such a privacy-invasive national ID database.

The system was initially mandatory, however, a legal challenge filed by the Kenya Human Rights Commission (KHRC), the Nubian Rights Forum, and the Kenya National Commission on Human Rights (KNHCR) at the Kenyan High Court in February argued that the NIIMS was in breach of the constitution as it violates the right to privacy (Article 31), the right to equality, and the right to non-discrimination in the bill of rights, as well as the right to public participation.

As a result of the legal challenge, the Kenyan Hight Court delivered an interim ruling on 1 April, pending the full hearing of the case brought by the KHRC, the Nubian Rights Forum and the KNHCR due to take place on 19-21 and 24-25 June. The interim ruling permits the government to proceed with the collection of personal information under NIIMS, but directed that it shall not:

[1] Kenya: Statute Law (Miscellaneous Amendments) No. 18 of 2018

[2] Registration of Persons Act No.33 of 1947 (as amended to 2012), section 3.

a) Compel any member of the public to participate in the collection of personal information and data in NIIMS.

b) Set any time restrictions or deadlines as regards the collection of the said personal information and data in NIIMS.

c) Set the collection of personal information and data in NIIMS as a condition precedent for the provision of any Government or public services, or access to any government or public facilities.

d) Share or disseminate any of the personal information or data collected in NIIMS with any other national or international government or non-governmental agencies or any person.

Therefore, registration is not compulsory and the government cannot compel any person to register, set deadlines for registration or deny access to government or public services to unregistered persons.

Despite this, national media sources have reported that registration stations have been set up in multiple areas with 35,000 Morpho Tablet 2 data capture kits in use across the country.[3] National media also reported that Communications Authority Director General Francis Wangusi had warned that punitive measures, including blocking unregistered persons from using their mobile phones and accessing other services, would be enacted on those who fail to register.[4] Some government employees reportedly received a memo warning their salaries would not be paid unless they registered for NIIMS.[5]

Despite the High Court interim ruling, Kenyan authorities have been persistently calling on people to register and have been widely publicising a registration deadline, including on official government social media accounts, without making clear that registration is not mandatory. Authorities set an initial deadline of 18 May, but on that date President Uhuru Kenyatta directed the National Inter-Ministerial Committee for Implementation of Huduma Namba to extend the registration deadline by one week until 25 May. According to government figures, more than 31 million people (61% of the population) had registered as of 13 May. In addition, registration for the Kenyan diaspora opened on 6 May and a deadline has been set for 19 June.[6]

The NIIMS raises serious human rights concerns, including the right to privacy as enshrined in Article 31 of the Kenyan Constitution and Article 17 of the International Covenant on Civil and Political Rights. By law, any limitation to fundamental rights including privacy must be clear and concise; necessary and proportionate; and, pursue a legitimate aim. The generation, collection, and processing of information of all citizens and registered foreigners appears to be unnecessary and disproportionate even if the legitimate aim is to enhance service delivery and national security.

Amnesty is concerned that Kenya has undertaken this unprecedented exercise while it lacks even a basic legal framework for data protection, including safeguards around data storage and security, or independent oversight of the system.

---

[3] Coda, *Kenya's Controversial Biometric Project is Shrouded in Secrecy*, 3 May 2019, https://codastory.com/authoritarian-tech/kenya-biometric-project-shrouded-in-secrecy/

[4] Standard Digital, *Government to block sim cards whose owners fail to beat Huduma Namba deadline*, 18 April 2019, https://www.standardmedia.co.ke/business/article/2001321603/huduma-namba-government-to-block-sim-cards

[5] Citizen Digital, *Machakos County Gov't won't pay staff without Huduma Namba*, 3 April 2019, https://citizentv.co.ke/news/machakos-county-govt-says-wont-pay-staff-without-huduma-namba-239075/

[6] See, for example, Kenyan High Commission in London http://kenyahighcom.org.uk/huduma-namba-registration/, Kenya High Commission in Ottowa http://kenyahighcommission.ca/wp-content/uploads/2019/05/HUDUMA-NAMBApdf.pdf and Kenya Embassy in Washington DC http://www.kenyaembassydc.org/pdfs/Huduma_Namba.pdf

NIIMS could have particularly damaging effects on marginalised groups such as refugees and ethnic minority groups, who already face excessive scrutiny from Kenyan authorities and are required to provide additional information when registering for ID cards. Without clarity on how such data will be used and protected, who is authorized to access it and for what purposes, whether it will be shared with other governments and third parties.

It is also concerning that in the past, Kenya has brazenly flouted the binding international principle of *non-refoulement* by forcibly returning refugees and asylum seekers who have sought safety in the country. Upon their return, some refugees have been arrested and detained without charge.

There are close to 500,000 registered refugees in Kenya, and others who have been waiting to be registered since 2015. If other governments or third parties are granted access to this information – or if the data is vulnerable to being stolen by them – refugees could be exposed to a grave risk of further abuse when they return home, or even while in Kenya.

The amended law was passed without public consultation despite Kenya's constitution requiring public input before any new law can be adopted. This has caused public outcry amongst some Kenyans and human rights organisations. On 28 February, the Senate's security committee called for the Huduma Namba roll-out to be suspended, due to concerns about the legal framework.[7]

It appears that NIIMS is the latest in a global trend towards governing through big data, as plans for similar nationwide biometric registers are underway in India[8], Malaysia[9] and Jamaica[10] and another is planned in several African states, including Zimbabwe.[11] It is therefore essential that the rights to privacy, equality and non-discrimination are guaranteed if such systems are going to be implemented, and that robust safeguards are put in place for the secure and responsible collection, storage and use of personal information. In this regard, comprehensive data protection legislation must be in place before any such system is considered. In addition, independent oversight mechanisms should ensure transparency of and accountability for the use of such systems.

3. What human rights concerns might arise in connection with the introduction of digital technologies in social protection systems?

It is crucial to note at the outset the importance and applicability of the international human rights legal framework in the field of digital technologies, including AI. This framework is universal, binding and actionable, and provides a tangible means to protect individuals from human rights violations. Ethics initiatives generally fall short on substance, concrete standards, transparency and accountability. For this reason, Amnesty International has advocated for companies, policy-makers and other key stakeholders to adopt an approach based on the international human rights framework.

---

[7] Daily Nation, *Senators want digital listing stopped as CSs snub summons*, 28 February 2019, https://www.nation.co.ke/news/Huduma-Nambab-CSs-snub-senate-summons/1056-5003226-35no4l/index.html; Business Daily Africa, *Senate orders suspension of biometric listing*, 28 February 2019, https://www.businessdailyafrica.com/economy/Senate-orders-suspension-of-biometric-listing/3946234-5004220-3lmg8j/index.html

[8] For example, India's Aadhaar programme. Time*, India Has Been Collecting Eye Scans and Fingerprint Records From Every Citizen. Here's What to Know*, 8 September 2018, http://time.com/5409604/india-aadhaar-supreme-court/

[9] Malaysia's national identification card is used for accessing government services and also functions as a driver's license, ATM card, contactless payment card, frequent traveller card, and health document containing basic medical information. See http://www.m2sys.com/

[10] National Identification System, or NIDS https://www.nidsfacts.com/faq/

[11] See Foreign Policy, *Beijing's Big Brother Tech Needs African Faces*, 24 July 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

Amnesty believes there are key issues with AI systems that urgently need to be addressed in order to respect human rights and protect them now and in future. Amnesty's key concerns with current AI systems are that:

- AI technology is predicted to fuel massive changes to employment, particularly through automation of jobs, which will require governmental action to protect workers' rights.
- AI systems collecting and processing vast amounts of personal data create new threats to rights, including the right to privacy.
- AI systems are contributing to discrimination – for example, in policing in the US and UK.
- A lack of transparency and accountability in current systems could deny victims of human rights abuses by AI-informed decisions adequate access to justice or remedy.
- Innovation in AI is for the most part being led by corporate actors, which could lead to limiting access to AI technology to a select few in future.

There are two major areas where states must place attention and invest resources to ensure that widespread use of AI benefits and does not erode human rights.

Impact of AI on employment and workers' rights

Advanced AI software will likely increase automation in the workplace, as systems become adept at more complex tasks. According to research by the McKinsey Global Institute, while automation could raise global productivity growth anually by an estimated 0.8%-1.4%, approximately half of the activities people are paid almost $15 trillion in wages to do could potentially be automated.[12] Technological advances and 'efficiency' savings will likely see machines replacing people in the workplace, as roles become part or fully automated.

States must ensure that people are able to access the right to work (Article 6(1) of the International Covenant on Economic, Social, and Cultural Rights) now and in the future, including through investing in training and re-skilling programmes to help those whose jobs could be at risk of automation to stay employable; considering new skills that will be in demand in a tech-driven economy; preparing for an employment landscape that is radically altered by mass unemployment and fully addressing the impact on state welfare and benefits systems. This may include exploring the viability and desirability of alternative income models like Universal Basic Income, as was explored in the 2017 report by the UN Special Rapporteur on Extreme Poverty and Human Rights.[13]

Privacy and racial profiling

Advancements in AI come hand-in-hand with the development of vast economies of personal data – raising concerns about privacy rights. AI systems are developed and trained using extremely large datasets. They are by and large designed to hone their function through continually processing new data – the larger quantities of relevant data that the system can access, the better.

There are numerous risks associated with networked systems storing and processing such large amounts of personal data. The use of advanced AI software will dramatically increase the points of personal data collection in terms of both volume and detail. For example, facial recognition and gait recognition technologies can easily capture and process detailed personal information on a previously unforeseen scale.

The networking of interconnected systems – from the internet and telecoms, to systems and sensors in travel, health, logistics, traffic, electricity networks – allows the possibility for cross-referencing

---

[12] Mckinsey Global Institute, *A Future that Works: Automation, Employment, and Productivity*, January 2017, https://www.mckinsey.com/featured-insights/digital-disruption/harnessing-automation-for-a-future-that-works

[13] For more on the human rights case for exploring Universal Basic Income, see report by Philip Alston, UN Special Rapporteur on Extreme Poverty and Human Rights, delivered to the UN Human Rights Council in June 2017: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/073/27/PDF/G1707327.pdf

data that, when collected previously, used to be held in silos. Networked big data may be used to create intimate and precise personal profiles of individuals, a tactic already widely used for commercial advertising and political marketing during elections.[14]

AI software also makes profiling on such an intimate individual level much more accessible – with the potential for companies and governments to influence people to a greater degree than ever before, using highly personalised messaging across a range of platforms. Personal data is increasingly being used by systems to inform decision-making processes in all areas of our lives. There is potential for discrimination where information from one aspect of someone's life or previous behaviour is used to inform a decision or access to a service elsewhere. For example, insurance providers may use social media data to evaluate an insurance claim without the claimant's knowledge.[15]

To ensure personal data collection and use by AI systems does not impact negatively on the rights of people, states must:

- Ensure that the rights of individuals, including privacy rights, are strengthened and upheld through the General Data Protection Regulation and other relevant data protection laws.
- Invest in public education to make people more data literate and aware of their rights. This means ensuring that individuals know not only what their rights are, but how to make a complaint or seek redress where they feel their data has been misused.
- Give greater powers to regulatory bodies that provide oversight and accountability on the use of AI and big data, particularly where AI systems could adversely affect rights.
- Ensure adequate regulation of private companies, including, for example, by mandating independent audits of AI systems where their use case means they have the potential to significantly impact human rights.
- Ensure that AI systems in public service use are designed in a manner compatible with human rights standards, such as being non-discriminatory and providing means to pursue effective remedy.
- Require that all AI systems used in public services and other services that directly impact on human rights are clearly identified as AI systems. Companies and public bodies should always disclose when such a system is used to deliver services or make decisions that impact people's rights.

Rights to Equality and Non-Discrimination

The adoption of AI and data-driven processes to aid governance and decision-making across many sectors of society has the potential to facilitate discrimination if proper oversights are not put in place.

Getting approval for a loan or mortgage or purchasing health or home insurance in the future will increasingly be determined by personal data run through an unaccountable algorithm. As argued by data scientist Cathy O'Neil, such systems are capable of reinforcing and entrenching existing discrimination based on profile data such as income, home address, ethnicity, gender or religion.[16] At the same time, the algorithm's decision is frequently beyond scrutiny. An individual who is charged a higher premium for their insurance or denied a mortgage has no means of challenging this decision and interrogating the data upon which it is based.

There is already worrying evidence that the use of AI and big data in policing can perpetuate discrimination and identity bias. As predictive policing systems advance rapidly and are deployed

---

[14] https://www.bbc.co.uk/news/uk-39171324

[15] Car insurance company Admiral last year attempted to use Facebook data to gather information that would inform insurance decisions: https://www.theverge.com/2016/11/2/13496316/facebook-blocks-car-insurerfrom-using-user-data-to-set-insurance-rate

[16] See O'Neil, Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2016)

across the law enforcement and security spheres, there is an urgent need to put safeguards in place to minimise the risk of human rights abuses and guarantee accountability when errors are made. Scrutiny of such systems and how they work as 'decision support' tools in the police is difficult, given that these systems are usually proprietary.

One research study from the Human Rights Data and Analysis Group (HRDAG)[17] developed a replica of a predictive policing algorithmic programme that is used by police forces in numerous US states, and ran it as a simulation on crime data in Oakland. It concluded that the programme reinforced existing racial discrimination within the police. This was because the system was built using already biased data that recorded higher crime rates in parts of the city with a higher concentration of black residents. The algorithm therefore predicted more crime in those areas, dispatching more frontline police officers, who unsurprisingly made more arrests. The new data was fed back into the algorithm, reinforcing its decision-making process and creating a pernicious feedback loop that would contribute to over-policing of black neighbourhoods in Oakland.

In 2014, the Metropolitan Police Service (MPS) announced it would introduce an automated system to assign risk scores to individual suspected of being 'gang members' in London.[18] The pilot reportedly used data gathered from social media along with police crime reports to generate offending risk scores for all individuals associated with London gangs.

Amnesty International's research into the MPS's Gangs Databases demonstrated that the current manual system used by the police to flag individuals as 'gang associated' is arbitrary, lacks adequate oversight and contributes to the overrepresentation of BAME young people in the criminal justice system. In this context, the introduction of automated risk-scoring on top of an already deeply flawed data collection policy with no effective oversight and safeguards in place raises significant human rights concerns.

As a result of Amnesty's research, UK regulatory body the Information Commissioner's Office took enforcement action against the Metropolitan Police, confirming many of our findings and requiring that the police overhaul the database. Mayor of London Sadiq Khan has also published detailed recommendations to the MPS in response to Amnesty's report to ensure future data collection on gangs is human rights compliant.

5. **Would you have specific recommendations about addressing both the human rights risks involved in the introduction of digital technologies in social protection systems as well as maximizing positive human rights outcomes?**

Please refer to the Toronto Declaration, which highlights the risk of human rights harms associated with AI and machine learning systems and contains recommendations for states and companies to address discrimination resulting from the use of such systems.

---

[17] Lum, Kristian and Isaac, William Isaac, *To predict and serve?*, 7 October 2016, https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x

[18] BBC News, *London police trial gang violence 'predicting' software*, 29 October 2014, http://www.bbc.co.uk/news/technology-29824854