EQUAL RIGHTS TRUST

The Equal Rights Trust

Submission to the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance on new information technologies, racial equality and non-discrimination

December 2019

Introduction

1. The Equal Rights Trust (the Trust) is grateful for this opportunity to respond to the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance in relation to the call for submissions on the acute and structural threats that new information technologies such as big data, machine learning, and artificial intelligence (AI) pose to the rights to non-discrimination and racial equality human rights principles and standards.

2. The Equal Rights Trust is an independent international organisation whose objective is to combat discrimination and advance equality as a fundamental human right and a basic principle of social justice. We pursue and promote the right to equality as a right to participate in all areas of life on an equal basis, which requires taking a holistic, comprehensive approach to different inequalities. We work in partnership with equality defenders – civil society organisations (CSOs), lawyers, government representatives and others committed to using law to create an equal world – providing them with the technical, strategic and practical support they need to work for the adoption and implementation of comprehensive equality laws. In connection with this work, we engage with UN bodies and procedures in order to increase knowledge and understanding of equality law and its role in the realisation of other rights and development.

3. The use of new information technologies such as big data, machine learning, and artificial intelligence (AI) is spreading, and it has been noted that such technologies "are rapidly becoming essential analytical, communicational, and even legal, infrastructure for our societies".[1] It is estimated that ""global GDP could be up to 14% higher in 2030 as a result of AI".[2] However, despite the global proliferation of AI, we are "only beginning to understand the flaws, limitations and boundaries of algorithmic decision-making",[3] especially in terms of discrimination.

[1] EPSC Strategic Notes, "The Age of Artificial Intelligence: Towards a European Strategy for Human-Centric Machines", European Commission, Issue 29, 27 March 2018, p.7, available at: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf.
[2] PwC, "*Sizing the Prize* – What's the Real Value of AI for Your Business and How Can You Capitalise?", 2017, available at: https://www.pwc.com.au/government/pwc-ai-analysis-sizing-the-prize-report.pdf.
[3] Committee of experts on internet intermediaries (MSI-NET), *Algorithms and Human Rights,* Council of Europe, DGI(2017), p.12, available at: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

4. There is a developing consensus for the need to develop international, regional and national law approaches to regulating new technologies and AI. In this short submission, we focus on providing evidence highlighting the actual and potential discriminatory impacts of new information technologies, including the risk that such technologies will entrench existing inequalities. Our central recommendation is that the development of approaches to regulation needs to be equality sensitive.

Discriminatory impacts of new information technologies

5. New information technologies can lead to discrimination in various ways.[4] We focus here on three well-documented patterns:[5] (i) AI decision-making[6] can lead to discriminatory results if the system "learns" from discriminatory data. The AI system might be trained on biased data or learn from a biased sample. In both cases, the AI system will reproduce that bias,[7] an effect that is often referred to by data scientists as "garbage in, garbage out";[8] (ii) even where the data "fed" into an AI system is apparently neutral, discrimination can occur when "a particular piece of data or certain values for that piece of data are highly correlated with membership in specific protected classes;"[9] (iii) there are serious risk of discrimination in the opaque mass collection of personal data, as well as in using such large datasets to train algorithmic systems. The examples provided in this submission illustrate the real and pertinent risk that data collected and processed in this way are used by authorities to target protected groups.

6. We provide examples of these patterns in the fields of state surveillance, employment, and national security systems.

(i) State surveillance

7. A recent study found that AI surveillance technology is spreading at a faster rate to a wider range of countries than had previously been understood.[10] At least 75 out of 176 countries included in the study are actively using AI technologies for surveillance purposes. This includes smart policing (53 countries) and facial recognition systems (64 countries).[11]

---

[4] See Borgesius, F.Z., *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making,* Directorate General of Democracy, Council of Europe, Strasbourg, 2018, available at: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73; Barocas, S. and Selbst, A.D., "Big Data's Disparate Impact" 104 *California Law Review* 671 (2016).

[5] *Ibid*.

[6] We note that there is no internationally agreed definition of "AI" and that the term refers to a broad range of processes, usually encompassing machine learning and algorithmic decision-making from big data and/or direct human input. We acknowledge that each of these processes give rise to specific human rights issues and therefore the absence of definitional clarity is a challenge. It is beyond the scope of this submission however to address this in further detail.

[7] Borgesius, above, note 4, p.11.

[8] Southerland, V., "With AI and Criminal Justice, the Devil is in the Data", ACLU, 9 April 2018, available at: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-and-criminal-justice-devil-data.

[9] Barocas and Selbst, above, note 4, pp.691-692.

[10] Feldstein, S., *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, 2019, p.7, available at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[11] *Ibid*.; see specifically the study's AI Global Surveillance Index, which presents a country-by-country snapshot of AI tech surveillance: https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf.

8. Predictive policing is a much-criticised example of how racial discrimination is perpetuated through new technologies. Tools like "PredPol" rely on "criminal records, crime statistics, the demographics of people or neighbourhoods, and even information obtained from social media"[12] to predict where crime is going to happen. However, because minority groups are often over-policed and this is reflected in the data upon which the software relies to make future determinations, it "may not represent fine-tuned algorithmic crime prediction as much as it involves the perpetuation of structurally biased policing".[13] In a 2016 study, the Human Rights Data Analysis group demonstrated that the use of PredPol in Oakland, CA would reinforce racially-biased police practices by recommending increased police deployment in areas with higher populations of non-white and low-income residents.[14]

9. Big data and predictive policing tools have fuelled the crackdown by the Chinese state in the region of Xinjiang. Human Rights Watch has reported on the creation of an Integrated Joint Operations Platform (IJOP), which collects data from multiple sources, including CCTV cameras, some of which have facial recognition or infrared capabilities, and "wifi sniffers" (devices that eavesdrop on activities or communications within wireless networks).[15] IJOP receives additional data from license plates and ID cards scanned at checkpoints, as well as health, banking, and legal records. Xinjiang authorities have also heightened surveillance efforts, including instituting mass collection of mandatory DNA samples from individuals between ages 12 and 65. This information is fed into IJOP computers, and algorithms sift through data looking for threatening patterns. Once IJOP flags an individual, that person is picked up by security forces and detained for questioning.[16]

10. Facial recognition is a biometric technology that uses cameras —both video or still images—to match stored or live footage of individuals with images from a database. These technologies are increasingly being trialed or used by police and security forces – as noted above, the Carnegie index identifies at least 64 countries that are actively using facial recognition systems. Analysis has shown the significant flaws in these technologies, which can lead to discriminatory impacts. For example, in the UK, a freedom of information request found that the use of automated facial recognition by London's Metropolitan Police Service (MPS) at the annual Notting Hill Carnival in 2016 and 2017 returned false positives in more than 98% of cases.[17] A test conducted by the American Civil Liberties Union in July 2018 found that the facial recognition tool "Rekognition" incorrectly matched 28 members of Congress, identifying them as people who have been arrested for a crime.[18] The false matches were disproportionately of

---

[12] García Muñoz, L.F., "AI Policing of People, Streets and Speech", *Artificial Intelligence: Human Rights, Social Justice and Development,* Global Information Society Watch, 2019, p.24, available at: https://www.apc.org/sites/default/files/gisw2019_artificial_intelligence.pdf.

[13] Feldstein, above, note 10, p.20.

[14] Lum, K. and Isac, W., "To Predict and Serve?" *Significance* 13, No. 5, 2016, available at: https://rss.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1740-9713.2016.00960.x.

[15] Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region", available at: https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.

[16] Feldstein, S "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," *Journal of Democracy* 30, no. 1, 2019, p.42.

[17] Available at: https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2018/april_2018/information-rights-unit---mps-policies-on-automated-facial-recognition-afr-technology

[18] Show, J. "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," 26 July 2018, ACLU, available at: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28. It is noted 11 of the 28 false matches

people of colour, including six members of the Congressional Black Caucus.

11. Irrespective of their accuracy, facial recognition technologies enable the mass collection of biometric data, with very little transparency as to how such data is stored and re-used. As illustrated by the IJOP case study above, there is a real and pertinent risk that such technologies may be used by authorities to target protected groups.

(ii) Employment

12. In the private sector, AI systems are used to select prospective employees. These systems can lead to discrimination because of biased training data.[19] For example in 2018, Reuters reported that Amazon stopped using an AI system for screening job applicants because the system was biased against women: according to the report "the company realised its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way."[20] Based on the data used by the system, "Amazon's system taught itself that male candidates were preferable."[21]

13. The Trust is particularly concerned that such technologies are increasingly being used in countries that have not yet adopted comprehensive anti-discrimination laws, meaning that the legal framework to prevent discriminatory application is inadequate. For example, the Paraguayan government has implemented an employment platform "ParaEmpleo",[22] which uses AI "to analyse the specific abilities of each applicant and connect them with employment opportunities (…) through deep learning algorithms and knowledge graphs which help them find job vacancies precisely and efficiently".[23] Users create their own profiles, including their abilities, qualifications, specializations, languages, and other features. The selection criteria for applicants could lead to discriminatory impact on members of certain groups. For example, employers are able to filter candidates according to the universities where they studied. Given inequality and obstacles in access to education (due to racial, linguistic, and socio-economic conditions), this may lead to indirect discrimination against protected groups. The ParaEmpleo platform is only offered in Spanish, thus creating a barrier to access for Guaraní speakers (as well as speakers of other native languages). Both Spanish and Guarani are recognised as official languages, and only 52% of Paraguayans in rural areas are bilingual. Therefore, the fact that the platform is available in Spanish only is indirectly discriminatory on the grounds of language and potentially ethnicity.

(iii) National social security systems

14. In January 2019, the Parliament of Kenya passed an amendment to the Registration of Persons

misidentified people of colour (roughly 39%), including civil-rights leader Rep. John Lewis (D-GA) and five other members of the Congressional Black Caucus. Only 20% of current members of Congress are people of colour, which indicates that false-match rates affected members of colour at a significantly higher rate.

[19] Borgesius, above, note 4, p.15.
[20] Dastin, J., "Amazon scraps secret AI recruiting tool that showed bias against women", 10 October 2018, *Reuters*, available at: https://www.reuters.com/article/us-amazon-com-jobs-automation-in...-ai-recruiting-tool-thatshowed-bias-against-women-idUSKCN1MK08G.
[21] *Ibid.*
[22] BIG, "Algoritmos que te consiquen empleo en Paraguay," available at: https://www.iadb.org/es/mejorandovidas/algoritmos-que-te-consiguen-empleo-en-paraguay
[23] *Ibid.*

Act,[24] to include a national ID registration system as a "single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya".[25] This national ID registration system, named the National Integrated Identity Management System (NIIMS), also known as Huduma Namba (Swahili for "service number"), was launched in April 2019. Controversially, the amendments also inserted, *inter alia,* a definition of "GPS", as well as the term "biometric" into section 3 of the Act, the latter being defined as "fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid [DNA] in digital form".[26] Huduma Namba was launched before meaningful data protection and privacy laws were in place in Kenya. The Data Protection Act was enacted in November 2019,[27] though there are serious concerns both about its contents and the feasibility of its implementation.[28]

15. Registration with the NIIMS was initially mandatory. Legal challenges filed by the Kenya Human Rights Commission (KHRC), the Nubian Rights Forum, and the Kenya National Commission on Human Rights at Nairobi's High Court in February 2019 argued that the NIIMS was in breach of the Constitution. It was argued that the NIIMS violates the right to privacy because no adequate protections have been assured; the right to equality and the right to non-discrimination in the Bill of Rights, *inter alia,* as regards the Nubian community and other marginalised groups who would face further exclusion; and the right to public participation. They also challenged the constitutionality of the legislative process. [29]

16. Millions of Kenyans currently face discriminatory practices in acquiring identity cards as they are subjected to a different process for acquiring an identity card based on their ethnicity or religion.[30] The process causes administrative burdens, undue delays and even denials of documents to Kenyan citizens.[31] Other Kenyans struggle to access registration and identification facilities due to distance and cost – particularly communities living in rural, remote, or pastoralist areas.[32] In this context, moving forward with a new population register and "smart" ID card could further marginalise these communities.

---

[24] Registration of Persons Act (Cap 107 Laws of Kenya) [1998] Revised 2012, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/RegistrationofPersonsActCap.%20107.pdf.
[25] Statute Law (Miscellaneous Amendments) No. 18 of 2018, p. 321-325, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf.
[26] Statute Law (Miscellaneous Amendments) No. 18 of 2018, p. 321, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf.
[27] The Data Protection Act No.24 of 2019, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
[28] See for example, ARTICLE 19, "Kenya: Protect the Data Protection Framework", 25 November 2019, available at: https://www.article19.org/resources/kenya-protect-the-data-protection-framework/; and "Kenya: The Data Protection Bill, 2019", July 2019, available at: https://www.article19.org/wp-content/uploads/2019/11/Kenya-Data-Protection-Bill-2019-final-2.pdf.
[29] *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others (Interested Parties); Centre For Intellectual Property & Information Technology (Proposed Amicus Curiae)* [2019] eKLR, Para 4, available at: http://kenyalaw.org/caselaw/cases/view/172447/.
[30] Open Society Justice Initiative Briefing Paper "Kenya's National Integrated Identity Management System," September 2019, p.4, available at: https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68-25ef390170c3/briefing-kenya-nims-20190923.pdf.
[31] *Ibid*.
[32] *Ibid*., pp.4-5.

17. Aside from these concerns, it is also unclear how the data collected by NIIMS will be stored, secured and used.[33] It will enable the government to undertake mass collection of personal data on all persons in Kenya. This is particularly concerning as the country has a well-documented history of discrimination on the basis of ethnicity and other characteristics. [34]

18. A three-judge bench ruled in April 2019 that the government could proceed with the collection of personal data under NIIMS, but directed that it should not make registration mandatory; link access to services to enrolment; collect DNA or GPS data; set a deadline for enrolment; or share data between agencies or to third parties.[35] Nevertheless, national media sources reported registration stations have been set up in multiple areas with 35,000 Morpho Tablet 2 data capture kits in use across the country.[36] It was further 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 taken against those who fail to register,[37] and that some government employees received a memo warning that their salaries would not be paid unless they registered for NIIMS.[38] In July 2019, a draft Huduma Bill was published in an attempt by the Kenyan government to circumvent the High Court's orders relating to NIIMS. The draft Bill not only makes access to goods and services dependent on registration, it also imposes criminal penalties, including prison time, for failure to register.[39] It fails to address the issues raised in the constitutional challenge. The High Court is expected to hand down its determination in January 2020.

Conclusion

19. This submission has sought to provide examples to illustrate discriminatory patters associated with new information technologies. However, the discriminatory potential of such technologies is yet to be fully understood. Our examples have focus on discrimination on the grounds of race, ethnicity and religion, but these patterns extend across characteristics, and indeed in the intersection of characteristics. For example, a study on the error accuracy of three prominent facial recognition tools found that dark-skinned women had an error rate of 34.7%, compared to 0.8% of light-skinned men.[40]

---

[33] We note that Kenya is enthusiastically using AI technology for State surveillance as demonstrated by the Carnegie Index, above, note 11.

[34] Equal Rights Trust in partnership with KHRC, *In the Spirit of Harambee: Addressing Discrimination and Inequality in Kenya*, February 2012, available at: https://www.equalrightstrust.org/ertdocumentbank/In_the_Spirit_of_Harambee.pdf.

[35] *Nubian Rights Forum & 2 others v Attorney-General & 6 others*, above, note 29, Para 107.

[36] Weitzberg, K., "Kenya's Controversial Biometric Project Is Shrouded in Secrecy," *Authoritarian Tech*, 3 May 2019, available at: https://codastory.com/authoritarian-tech/kenya-biometric-project-shrouded-in-secrecy/

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

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

[39] The text of the Bill is available at: http://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf.

[40] Hardesty, L., "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems", *MIT News*, 11 February 2018, available at: http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; citing Buolamwini, J. and Gebru, T., "Gender Shades: Intersectional

20. It is vital that an equal rights approach to addressing the actual and potential harms of new information technologies is adopted. This requires listening to the voices of the communities affected. Governments and international institutions must therefore engage equality defenders in developing legal and policy approaches to the regulation of new technologies and AI.

21. In closing, we would like to once again express our gratitude to the Special Rapporteur for the opportunity to set out our position on the essential role of equality defenders in remedying the harms of new technologies.

Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research 81: 1-15*, 2018, available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.