New technologies in migration: human rights impacts

Petra Molnar

States are keen to explore the use of new technologies in migration management, yet greater oversight and accountability mechanisms are needed in order to safeguard fundamental rights.

Experiments with new technologies in migration management are increasing: from big data predictions about population movements in the Mediterranean, to the use of automated decision making in immigration and refugee applications, to artificial intelligence (AI) lie detectors deployed at European borders. The way that technology is used is a useful lens through which to highlight State practices and raise questions about democracy, power and accountability. Making migrants more trackable and detectable justifies the use of more technology and data collection in the name of national security, or even under the banner of humanitarianism and development. Yet technology is not inherently democratic and its human rights impacts are particularly important to consider in humanitarian and forced migration contexts.

Data-driven humanitarianism

AI, machine learning, automated decision-making systems and predictive analytics are overlapping terms referring to a class of technologies that augment or replace human decision-makers. These systems process information in the form of input data, using an algorithm to generate an output. In its most basic form, an algorithm can be thought of as a set of instructions, like a recipe that learns. The data that are used by the algorithm to learn are varied and can be a body of case law, a collection of photographs or a database of statistics, some or all of which have been pre-categorised based on the designer's criteria. Such technologies can be used in various ways in different facets of 'migration management'.

Automated decision-making technologies require vast amounts of data from which they learn. For example, various UN projects have been relying on extremely large data sets – 'big data' – to predict population movements during and after conflicts and to make the delivery of humanitarian aid more efficient. However, data collection is not an apolitical exercise, particularly when powerful actors such as States or international organisations collect information on vulnerable people without regulated methods of oversight and accountability. The increasingly fervent collection of data on migrant populations – so-called data colonialism – can also result in privacy breaches and raise human rights concerns. Data collection on marginalised groups is also deeply historical. The Nazi regime relied on vast amounts of data on Jewish populations collected with the help of IBM; during the Rwandan genocide Tutsis were systematically tracked in ethnicity registries; and the US after the 9/11 attacks has collected vast amounts of data on individuals under suspicion through the Department of Homeland Security's National Security Entry-Exit Registration System. In an increasingly anti-immigrant global landscape, migration data have also been misinterpreted and misrepresented for political ends, for example to affect the distribution of aid funds and resources and to help advance anti-immigration policies.

Informed consent and the private sector

The use of new technologies raises issues of free and informed consent, particularly in the increasing instances of reliance on biometric data. For example, in Jordan, refugees now have their irises scanned in order to receive their weekly food rations. But are they able to opt out from having their data collected and retained? An investigation by IRIN News (now The New Humanitarian) in Azraq refugee camp found that most refugees interviewed were uncomfortable with such technological experiments but felt

that they could not refuse if they wanted to eat.[1] Consent is not necessarily freely given if it is given under coercion, even if the coercive circumstances masquerade as efficiency and better service delivery.

Of particular concern is the growing role of the private sector in the collection, use and storage of these data. For example, the World Food Programme recently signed a US$45 million deal with Palantir Technologies, a private company that has been widely criticised for providing the technology that supports the detention and deportation programmes run by US Immigration and Customs Enforcement (ICE). What will happen with the data of 92 million aid recipients when shared with Palantir? It is not yet clear whether data subjects will be able to refuse to have their data shared or whether there will be a model for accountability and transparency for data sharing made available to the public.

Automating immigration

A 2018 report I co-authored explored the impacts of automated immigration decision making in Canada,[2] a practice with which other States that receive large numbers of immigrants are also experimenting. The report looks at how these processes create a laboratory for high-risk experiments within an already highly discretionary and opaque system. In the US, these experiments are already in full force. For example, in the wake of the Trump administration's executive orders on migration, ICE used an algorithm at the US–Mexico border which justified detention of migrants in every single case.[3]

Instances of bias in automated decision making, particularly regarding race and gender, are also widely documented. When algorithms rely on biased data they produce biased results. These biases have far-reaching results if they are embedded in the emerging technologies being used experimentally in migration. For example, in airports in Hungary, Latvia and Greece, a new pilot project spearheaded by a company called iBorderCtrl has introduced an AI-powered lie detector at border checkpoints.[4] Passengers' faces will be monitored for signs of lying, and if the system becomes more 'sceptical' of a person through analysing a series of increasingly complicated questions, it will select them for further screening by a human officer. While this use might seem innocuous, can an automated decision-making system account for trauma and its effects on an asylum seeker's memory, or for cultural differences in communication? Furthermore, facial recognition technologies continue to struggle when analysing women and people with darker skin tones. These experimental uses of AI also, again, raise concerns about privacy and information sharing without people's consent.

What happens when an algorithm like this makes a mistake? For example, in May 2018, an algorithm led to the wrongful deportation of over 7,000 foreign students from the UK after concluding they had cheated on a language acquisition test after analysing sound files.[5] If you want to challenge an algorithmic decision like this in a court of law, is it the designer, the coder, the immigration officer or the algorithm itself who is liable? Much immigration and refugee decision making already occupies a difficult legal space. The impact on the rights and interests of individuals is often very significant, but great deference is given to the immigration decision-maker and the procedural safeguards are weak. It is unclear how a whole new system of decision making will affect mechanisms of redress. There is also a serious lack of clarity surrounding how courts will interpret algorithmic decision making and relevant administrative law principles such as procedural fairness and the right to an impartial decision-maker.

Mechanisms for accountability and oversight

No global regulatory framework yet exists to oversee the use of new technologies in the management of migration. In much technological development, intellectual property laws and proprietary considerations prevent public access to data sets and impede full understanding of the technology. Although conversations around the ethics

of data and technology use are taking place, and broad global strategies and regional mechanisms are being explored, we need a sharper focus on mechanisms for oversight. Private sector actors already have an independent responsibility to ensure that the technologies they develop do not violate international human rights. Technologists, developers and engineers responsible for building this technology also have existing special ethical obligations to ensure that their work does not facilitate human rights violations. Unfortunately, the growth of government surveillance, immigration enforcement and border security programmes can incentivise and reward industry for developing rights-infringing technologies.

States must also commit to creating and enforcing such oversight mechanisms. Our report on automated decision making in Canada makes several recommendations for States and other actors in migration management with global applicability:

- commit to transparency and report publicly what technology is being developed and used
- adopt binding directives and laws that comply with internationally protected human rights obligations
- establish an independent body to oversee and review all use of automated technologies in migration management
- foster conversations between policymakers, academics, technologists and civil society on the risks and promises of using new technologies.

These emerging conversations must also address the lack of involvement of affected communities. Rather than more technology 'for' or 'about' refugees and migrants being developed and vast amounts of data being collected, people who have themselves experienced displacement should be at the centre of discussions around when and how emerging technologies should be integrated into refugee camps, border security or refugee hearings – if at all.

Petra Molnar *petra.molnar@utoronto.ca*
Lawyer, International Human Rights Program, University of Toronto Faculty of Law
https://ihrp.law.utoronto.ca

This article is based on the author's current research at the University of Cambridge.

1. Staton B (2016) 'Eye spy: biometric aid system trials in Jordan' bit.ly/IRIN-biometric-aid-Jordan

2. Molnar P and Gill L (2018) *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System* bit.ly/Molnar-Gill-2018

3. Oberhaus D (2018) 'ICE Modified Its "Risk Assessment" Software So It Automatically Recommends Detention' bit.ly/Oberhaus-ICE-2018

4. Picheta R (2018) 'Passengers to face AI lie detector tests at EU airports' bit.ly/AI-liedetectors

5. Baynes C 'Government "deported 7,000 foreign students after falsely accusing them of cheating in English language tests"', *The Independent*, 2 May 2018 bit.ly/Baynes-deportation-020518