

April 2020

*Written Observations*

Dr Ana Beduschi  
Associate Professor of Law  
University of Exeter, United Kingdom

I would like to thank Professor Achiume, the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance, and the Promise Institute for Human Rights and the UCLA Center for Critical Internet Inquiry for the invitation and opportunity to contribute these written observations.

**Interplay between digital technologies, actors and interests in the context of border enforcement practices**

States and non-state actors are increasingly relying on new technologies for international migration management and border security. Three main types of technologies are particularly important in this context: big data and big data analytics, artificial intelligence (AI) and digital identity (the identification and verification of identity mediated by digital means).

Big data and big data analytics have a great potential to be used in forecasting and managing migratory flows, which are important for border management and control. Predictive analytics technics, aiming at uncovering patterns and identifying relationships in data to predict future human behaviour, can be used for capturing trends in migration flows and informing decision-making. For example, Frontex, the European Border and Coast Guard Agency, performs risk analysis and has a dedicated data science team to carry out big data analytics informing border management and control.<sup>1</sup>

Fuelled by big data, AI algorithms have the potential to revolutionise the way states and international organisations seek to manage international migration. AI is gradually going to be used to perform tasks, including identity checks, border security and control, and analysis of data about visa and asylum applicants. To an extent, this is already a reality in some countries such as Canada, which uses algorithmic decision-making in immigration and asylum determination.<sup>2</sup> In the European Union (EU), the revised Schengen Information System (SIS) will be using facial recognition, DNA, and biometric data to facilitate the return of migrants in an irregular situation.<sup>3</sup>

Digital identity technologies are being increasingly used for identity verification and identification of individuals and have the potential to be scaled up and used for border management. Digital

---

<sup>1</sup> Frontex (2020) Available at <https://frontex.europa.eu/intelligence/analytics/> (accessed 27 April 2020).

<sup>2</sup> Petra Molnar and Lex Gill, 'Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System' (2018) International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto).

<sup>3</sup> Regulation 2018/1860/EU on the use of the Schengen Information System for the return of illegally staying third-country nationals OJ L312. See also Regulation 2019/816/EU establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation OJ L135; Regulation 2019/818/EU on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 OJ L135.

April 2020

identity comports a set of attributes available in digital format, which relate to a person or entity.<sup>4</sup> These include biometric data (e.g. fingerprints, eye scans, 3D face maps), and life factors (e.g. date and place of birth). They can also be combined with evidence of government-issued ID (e.g. passport, drivers' licence), and digital activities on social media, online search history, and geotagging data. Existing digital identity platforms use blockchain and artificial intelligence to verify the identity of individuals by enabling 'digital identity wallets' to run on online platforms and mobile phone devices.<sup>5</sup> Digital identity technologies also permeate the activities of international organisations such as the UNHCR, which uses a combination of biometrics and centralised identity management tools for registration and identity verification.<sup>6</sup>

The technologization of border management and control goes together with increased interactions between the public and private sectors. The private sector plays a central role in developing the technologies that will be later deployed by states and international organisations in the field. Therefore, a key issue is that state and non-state actors operating in this field are potentially motivated by different interests. In particular, the private sector may logically follow its commitment towards profit-making, whereas states seem to have firmly embedded their immigration and asylum policies within their security agendas. Consequently, individuals' interests and the protection of their rights is often unaccounted for in the design and deployment of these technologies. A human rights-based approach is, therefore, urgently needed to address this gap and rebalance the power structures at play.

### **Urgent need for a human rights-based response**

Technology alone cannot protect human rights or prevent discrimination. Depending on how these technologies are designed and used, they may hinder individuals' human rights. Technology is not a neutral tool as it can simultaneously include and exclude individuals from protection. For instance, using blockchain technology to identify highly persecuted groups of people such as the Rohingya minority in Myanmar may allow them to access services in a host country such as Bangladesh.<sup>7</sup> However, it may also allow for more efficient ways to discriminate against these populations since identification makes them more visible.

Similar concerns relate to the deployment of AI technologies for border management and control. On the one hand, states could use AI to foresee border movements and prepare more efficiently for receiving large influxes of people. For instance, decision-makers could use AI algorithms to analyse large amounts of data and identify potential gaps in their reception facilities. These gaps could relate, for example, to the lack of sufficient places for families with children or vulnerable unaccompanied children. Identifying such gaps and acting on them would allow state authorities to prepare and adapt their reception conditions, thus complying with their legal obligations under international human rights law (IHRL).

---

<sup>4</sup> ISO, ISO/IEC 24760-1:2019. IT Security and Privacy — A framework for identity management. Part 1: terminology and concepts (2019) International Organization for Standardization (ISO) Available at <https://www.iso.org/standard/77582.html> (accessed 27 April 2020).

<sup>5</sup> See Sovrin, Control Your Digital Identity (2020) Available at <https://sovrin.org/> (accessed 27 April 2020); ID2020 (2020) Available at: <https://id2020.org/> (accessed 27 April 2020).

<sup>6</sup> See UNHCR (2020) Available at <https://www.unhcr.org/registration-guidance/> (accessed 27 April 2020).

<sup>7</sup> Rohingya Project, *A Rohingya initiative* (2018) Available at <http://rohingyaproject.com/> (accessed 27 April 2020).

April 2020

On the other hand, states with increased AI capabilities may be inclined to put measures in place to prevent migrants' and asylum-seekers' arrivals. Regrettably, that would reinforce the existing *non-entrée* policies; in other words, the current variety of measures aimed at preventing access by migrants and asylum-seekers to a state's territory.<sup>8</sup> *Non-entrée* policies encompass visa controls, carrier sanctions, the establishment of international zones, and maritime interceptions on the high seas.<sup>9</sup> AI technologies could be instrumental for each of these policies, for example, by streamlining visa controls and identity checks in offshore facilities. Besides, AI technologies could be used to reinforce unlawful *non-refoulement* practices (as forbidden by Article 33 of the Refugee Convention). For example, such technologies could assist targeted maritime interventions aiming at returning migrants and asylum-seekers to places where they may fear for their lives or freedom. In this regard, AI is at risk of becoming another political tool, used to reinforce old state practices, which aim to curb international migration and prevent asylum-seekers from reaching their territories.

Moreover, there are growing reservations about the emergence of a form of 'surveillance humanitarianism' within international organisations' practices.<sup>10</sup> The claim is that by increasingly relying on technology to collect personal data of vulnerable people such as migrants and refugees, these organisations create additional bureaucratic processes that could lead to exclusion from protection. International organisations should, therefore, strive to protect the data of the vulnerable people they intend to serve. Such concerns echo much of the recent scholarship that has raised the alarm about the adverse effects of data-driven AI in society.<sup>11</sup> In particular, research demonstrates that AI algorithms can reinforce stereotypes leading to social injustice<sup>12</sup> and that the uses of AI technology may narrow the scope of the welfare state.<sup>13</sup> Moreover, due to their 'black box' nature and the fact they may be protected under trade secrets, AI algorithms may contain undetectable inaccuracies and mistakes, which can lead to unlawful discrimination.<sup>14</sup>

To summarise, these technologies should be developed and deployed within ethical and legal frameworks, in particular, IHRL. IHRL should thus serve as a baseline for action in this field, with an emphasis on guiding policy and providing for the protection of individuals' rights in the context of border enforcement. Policymakers should bear in mind that the use of AI technologies may lead to mistakes. For example, AI algorithms may accidentally misidentify a migrant as a terrorist or miscalculate the risk of ill-treatment upon deportation to their country of origin. Blind over-reliance on AI technologies could lead to serious breaches of human rights if in these scenarios, migrants were deprived of liberty due to misidentification, or if they were subjected to torture or inhuman treatment upon deportation. As technologies evolve, human rights should occupy a prominent place in their design and deployment.

---

<sup>8</sup> James C. Hathaway, *The Rights of Refugees under International Law* (Cambridge University Press 2005).

<sup>9</sup> Thomas Gammeltoft-Hansen and James C. Hathaway, 'Non-Refoulement in a World of Cooperative Deterrence' (2015) 53 *Columbia Journal of Transnational Law* 235–61.

<sup>10</sup> Mark Latonero, 'Stop Surveillance Humanitarianism' (New York, The New York Times 11 July 2019).

<sup>11</sup> Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018); Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin 2017); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019) Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018).

<sup>12</sup> Noble (n 11).

<sup>13</sup> Eubanks (n 11).

<sup>14</sup> Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

April 2020

## References:

The present observations were based on my published research, in particular:

- Ana Beduschi, [International Migration Management in the Age of Artificial Intelligence](#) (2020) 8 *Migration Studies* 1-21.
- Ana Beduschi, [Human Rights and the Governance of Artificial Intelligence](#) (2020) Research Brief, Geneva Academy of International Humanitarian Law and Human Rights, University of Geneva.
- Ana Beduschi, [Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights](#) (2019) 6 *Big Data & Society* 1-6.
- Ana Beduschi, [The Big Data of International Migration: Opportunities and Challenges for States under International Human Rights Law](#) (2018) 49 *Georgetown Journal of International Law* 981-1017.
- Ana Beduschi, [Vulnerability on Trial: Protection of Migrant Children’s Rights in the Jurisprudence of International Human Rights Courts](#) (2018) 36 *Boston University International Law Journal* 55-85.