PICUM

PLATFORM FOR INTERNATIONAL COOPERATION ON UNDOCUMENTED MIGRANTS

INPUT TO EU CONSULTATION ON ARTIFICIAL INTELLIGENCE

June 2020

PICUM is a network of 167 organisations that has worked for nearly twenty years to advance the rights and improve the situation of people who are undocumented across a variety of areas, including access to health care, access to justice, the rights of undocumented workers, labour migration, the rights of children, families and youth, as well as fundamental rights in the context of immigration detention and return.

We appreciate the opportunity to provide input to the EU's consultation on artificial intelligence.

Background

For all its purported benefits, the increased use of digital technology can drive increased discrimination against and exclusion of some groups. For people who are undocumented, the state's use of technology and processing of personal data is typically to support immigration enforcement actions and entails the policing of otherwise normal behaviours of people often belonging to communities of colour to detect whether they are present without authorisation.

Automated decision-making systems (or artificial intelligence, "AI") have the potential to exacerbate this, building human bias into algorithms deployed against groups already facing high levels of stigmatisation and discrimination – where massive differentials in power and information can impede accountability and access to redress for rights violations.

The EU's approach to AI must therefore prioritise the safeguarding of fundamental rights for everyone, with particular attention to those at greatest risk of harm. It must ensure that the pursuit of "innovation" does not obscure the real threats that AI technologies pose for individuals and for society and instead take proactive steps to identify and avert them.

Discriminatory Effects Arising from the Use of AI Technologies in the Context of Law Enforcement and Immigration Enforcement & Administration

- ***AI and law enforcement:*** Notwithstanding warnings from experts about AI's potential to reinforce existing bias, automated decision making technology is already used by police. The most extreme example is in Xinjian region of China, which uses predictive policing and mass surveillance to target Uighur Muslims. Similar technologies in the United States and Europe capture less data but target a wider variety of uses including identifying potential offenders or reoffenders, locating "high-crime" areas, determining who should be put in pre-trial detention, and deciding who should be granted parole.

  Because AI technologies, such as predictive policing, use crime statistics to assess whether an individual or a community is higher "risk" of criminal behaviour, racial bias present in existing policing approaches, as well as inaccuracies in that data, inevitably influence the programming and learning process of the AI. As a result, AI technologies have suggested increased policing in already over-policed areas leading to more arrests and thereby creating a vicious cycle. Law enforcement's ready access to databases and other personal information places individuals in situations of vulnerability at further risk.

Contact person: Alyna C. Smith, alyna.smith@picum.org

In the UK, the Kent Police, the first police force in the United Kingdom to trial predictive policing, cancelled the project after five years finding no evidence that AI technologies helped reduce crime. The civil rights organisation Liberty has argued that predictive policing programmes should be banned altogether because creating national standards and other transparency measures will not eradicate their inherent bias.

- ***AI and immigration enforcement:*** In 2019, the EU enacted two regulations that massively scale up the potential use of immigration data systems (together with data on criminal records) to pursue immigration enforcement *and* serious crimes. These regulations provide a legal foundation for the creation of a new layer of architecture on top of existing migration databases, to permit interoperability: that is, to allow the underlying databases to be interconnected in a way that purportedly supports more efficient law and immigration enforcement. PICUM partnered with Statewatch to produce a report setting out the implications of interoperability for undocumented people.

  This interoperability framework is problematic for several reasons. First, it is highly discriminatory in that it only targets non-EU nationals (i.e., foreigners) for purposes that co-mingle immigration enforcement and the targeting of "serious crimes" like terrorism, implying a false link between criminality and immigration. Second, interoperability creates a deeply complex system with multiple interconnecting databases. This technical complexity only increases the likelihood of errors and makes it extremely difficult to inform people about how their data is used, how they can rectify their data and obtain effective remedies in the event of errors or abuses. Lawyers, data protection authorities and others essential to safeguarding the rights of the millions of people whose data is concerned are still struggling to understand the new systems and what they mean for people's rights.

  The new architecture created under interoperability includes a Central Identify Repository (CIR), with the capacity to store the data of up to 300 million records. It is notable that researchers who have attempted estimate the number of undocumented people in the EU have estimated an upper limit of 4 million people. The immensity of the CIR, and the staggering scope and complexity of this web of databases, exemplify the disproportionate emphasis and approach to irregular migration in Europe. At a 2018 conference, a senior administrative at Europol stated that, where implementation of this complexity is concerned, "AI can facilitate the work" to ensure that officers get "actionable information."

  The EU will launch a Pact on Asylum and Migration in the coming weeks. It is anticipated that it will include elements on strengthened interoperability and use of artificial intelligence in the context of immigration enforcement – for instance, to fully digitise visa procedures and forecast border crossings and migration patterns; and proposing changes to existing EU legislation to permit the collecting of data to better locate undocumented people.

  - In **Hungary, Latvia, and Greece**, AI-powered lie detectors have been introduced at border checks, causing concern over how AI will account for trauma and its effect on memory as well as cultural differences in communication.

  - One study highlights the use of unpiloted military-grade drones by FRONTEX in the **Mediterranean** for surveillance and interdiction of migrant vessels, which could be contributing to rising deaths in the Mediterranean as boats are intercepted before reaching the shores of Europe.

- ***AI in immigration administration:*** Due to its promise of faster decisions, thus reducing delays and avoiding backlogs, AI technology has proved appealing to those who carry out migration and asylum-procedures, which tend to be lengthy and labour-intensive. This application of AI or automated systems potentially affects processes and functions traditionally performed by administrative tribunals, immigration officers, border agents, legal analysts and other officials responsible for immigration and refugee systems. One study highlighted the dangers of

replacing human immigration officers with technology: 7000 students were wrongfully deported because a faulty algorithm accused them of cheating on a language acquisition text.

- ***Facial recognition and immigration enforcement:*** The European Commission recognised in its White Paper on AI that the "gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights". According to a study from the U.S. National Institute of Standards and Technology (NIST), facial recognition systems tend to lead to remarkably higher rates of false positives among people of colour. And yet, according to European Data Rights (EDRI), "at least 15 European countries have experimented with highly intrusive facial and biometric recognition systems for mass surveillance."

  Despite calls by civil society for a moratorium until there has been adequate public debate and proper assessment of risks and needed safeguards to preserve fundamental rights, there have been reports that the EU plans to establish an EU-wide network of facial recognition databases. European police already have access to databases with fingerprints and DNA across the EU and, in some cases, the United States through the Prüm system. A 2019 report by national police forces in 10 EU countries, led by Austria, urges new legislation to expand Prüm to create and interconnect national police facial recognition databases in every member state. The European Commission commissioned at least two studies with outside consultancy, totalling more than 1M €, on possible changes to the Prüm system, including facial recognition technology.

  Significantly, the European Commission has indicated that: "Provided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework, the Passenger Name Record (PNR) Directive and the Advance Passenger Information Directive may at a later stage be linked up to one or more of the [interoperability] components."[1]

  The EU's Schengen Information System (SIS) will similarly be using facial recognition, DNA, and biometric data to facilitate the return of migrants in an irregular situation. All these systems raise concerns over how the learnt human bias, racial profiling as well as other technical issues will be accounted for in order to ensure the protection of vulnerable individuals.

  In **Germany**, the Federal Office for Migration and Refugees (BAMF) has been piloting projects using technology for facial recognition, automatic dialect recognition, name transliteration, and analysis of mobile data devices for identity verification which has been met with criticism.

Recommendations

The EU's proposed legislative action on AI comes in the context of strengthened data protection rights under the General Data Protection Regulation, and longstanding protections of privacy and due process under EU primary law. It also comes against the backdrop of systemic forms of discrimination against people of colour and people with a migration background, including by law enforcement, often exacerbated by the use of technology and the large-scale processing of personal data.

It is therefore critical for the European Commission to temper ambitions to harness the potential of AI technology to drive innovation to mitigate its potential to drive inequality, by prioritising fundamental rights and broader democratic values. To this end, we recommend that the EU:

- **Commit to a robust fundamental rights-centered approach as its first priority.** This entails conducting and making available publicly a fundamental rights review of AI technologies, including a specific focus on those most at-risk of its harmful impacts. It should be clear how this review influences the coordinated plan on AI, and in particular how the latter addresses fundamental rights concerns.

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems, COM(2017) 794 final, 12 December 2017.

- **Avoid creating exemptions to fundamental rights protections and scrutiny.** Review the AI coordinated plan with a view to avoiding exemptions that limit fundamental rights protections, such as by creating exemptions for certain classes of individuals. Abandon the focus on binary high/low risk distinctions in favour of one that assessments that evaluate the levels of harm and likely outcomes for individuals and society.
- **Be clear on impermissible uses to prevent fundamental rights abuses.** Such impermissible uses should include widespread biometric surveillance and biometric capture and processing in public spaces, the use of AI solely for immigration and law enforcement purposes, and their use or testing on marginalised groups such as undocumented people.
- **Ensure democratic oversight and systems of accountability.** Given the well-recognised asymmetries of information and of power between those who develop and deploy AI technology and those who are subject to it, the EU must integrate mechanisms for genuine oversight and consultation, including with civil society organisations and communities most likely to experience the deleterious effects of AI systems. There must also be accessible systems of accountability in place to permit redress for rights violations linked to the use of AI systems. Empower equality bodies, data protection authorities, and other relevant public bodies to enhance their capacities to ensure accountability for the implications of digital technology and data processing for human rights and discrimination.

Resources

Beduschi, Ana (2020), "International Migration management in the Age of Artificial Intelligence", Migration Studies.

Chen, Alex (2019), "The Threat of Artificial Intelligence to POC, Immigrants, and War Zone Civilians".

Chun, Andy H.W. "Using AI for e-Government Automatic Assessment of Immigration Application Forms". City University of Hong Kong.

Crawford, Kate (2016), "Artificial Intelligence's White Guy Problem", The New York Times.

EDRi (2020), Recommendations for a Fundamental Rights-based Artificial Intelligence Regulation.

ENAR (2019), Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe

Financial Times (2019), 'AI in law enforcement needs clear oversight'.

Grüll, Philipp (2020), 'Germany's plans for automatic facial recognition meet fierce criticism', Euractiv.

Liberty (2020), "Policing by Machine".

Molnar, Petra (2018). 'Using AI in Immigration Decisions Could Jeopardize Human Rights'. Cigi Online.

Molnar, Petra (2019), "Emerging Voices: Immigration, Iris-Scanning and iBorderCTRL - The Human Rights Impacts of Technological Experiments in Migration", OpinioJuris.

Molnar, Petra (2020), "The human rights impacts of migration control technologies". EDRi.

Nilsson, Patricia (2019), "Police fear bias in use of artificial intelligence to fight crime", Financial Times.

Parmar, Alpa (2019). Policing Migration and Racial Technologies, *The British Journal of Criminology*, Volume 59, Issue 4, July 2019, Pages 938–957.

PICUM (2020), "How do the new EU regulations on interoperability lead to discriminatory policing?"

Statewatch, (2019) "Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status".

University of Toronto (2019). 'Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System'.