PICUM

PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

Input to the European Data Strategy

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 on the European Data Strategy.

I. Background

For all its 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.

For instance, in Europe personal data is widely shared in the context of undocumented people trying to report crime or mistreatment to the police. For instance:

- In Belgium, the police have a duty to report victims with irregular status to the Immigration Office. In some cases, police precincts adopt a practice of wilful ignorance, declining to inquire about a person's residence status, and thus to report. The Immigration Office also retains the discretion not to prosecute people for putative immigration offences. However, undocumented people are left with significant uncertainty about whether coming forward to engage with law enforcement, including as victims of crime, will result in their deportation in any given case.
-
- In the United Kingdom, the National Police Chiefs' Council adopted a revised policy in 2018 declaring their prioritisation of victims' rights ahead of immigration enforcement - but reserving the right to share data with the immigration service, if they became aware of it. The intention of the policy is to promote confidence in the police; however, by preserving the right to share immigration information with the Home Office, they undermine that very confidence because people coming forward cannot know if their immigration status will be shared, should it become known, and if so what the Home Office's response will be.

Personal data is also used to "police" people who are undocumented when they access health care, social services, and education. In addition to undermining their economic and social rights, their rights to due process and to the protection of their privacy and personal data, in practice this also leads to racial profiling and discrimination.

- In Germany, undocumented people have the same right to health care as asylum seekers under the Asylum Seekers Benefit Act – but the social welfare office that mediates their right to care must share their data with immigration authorities, under section 87 of the Residence Act, which governs the "transfer of data and information for foreign authorities" by all public authorities.

- In the United Kingdom, charging for secondary health care has been introduced for undocumented people and others without "ordinary residence". People with irregular status are therefore billed 150% of the cost of secondary care to the National Health Service (NHS). If a patient is unable to pay their debts to the NHS, the Home Office is automatically informed, which may have consequences for their ability to later renew or apply for a residence permit. In April 2020, the UK government updated its regulations to include COVID-19 in the list of conditions exempted from charges for migration. However, advocates are concerned that the guidance leaves doubt about undocumented people and provides no definitive assurance of a "firewall" between the NHS and the Home Office. A 2019 report revealed that an NHS trust shared patients' data with the financial firm Experian so that it could check their economic activities and determine which overseas visitors or migrants could be charted for health care. The NHS contacted an additional 51 trusts to carry out similar check.

The routine nature of privacy breaches against migrants is illustrated in the case of Germany, where the Federal Office for Migration and Refugees routinely examines data from the mobile phone of people who present with a valid passport, upon arrival in the country – without any individualised reason for suspicion – to verify information provided about their identity. This highly invasive practice has been documented in a report that ultimately laid the groundwork for litigation launched against the Germany government in May 2020 by Berlin-based digital rights defenders, Gesellschaft für Freiheitsrechte.

In 2018, the same day the EU's General Data Protection Regulation went into force, the UK enacted its Data Protection Act, which includes a specific exemption whereby certain core rights of data subjects need not be respected if doing so would interfere with "effective immigration control". PICUM brought a complaint to the European Commission, supported by several UK NGOs, arguing that this provision blatantly violates the EU's data protection rules.

These arrangements exist despite the EU's strong safeguards on the protection of personal data, which is a fundamental right under the EU Charter and protected under the 2018 General Data Protection Regulation.

II. Discriminatory Effects Arising from the Use of Digital Technologies in the Context of Border Enforcement and Administration

Interoperable EU migration databases: increasing the stigmatisation and criminalisation of migrants

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.

Clouds on the horizon: The future of digital technology and migration in Europe

- ***AI and migration enforcement:*** 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.

- ***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]

- ***COVID-19 contact tracing and people with insecure residence status:*** In the context of the COVID-19 pandemic, public and private actors have been developing mobile applications to monitor and slow the pandemic. In response, the EU in April 2020 launched a tool box for member states on the use of these apps, and guidelines on how to do this in a manner that

[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.

respects fundamental rights. Digital rights advocates have highlighted specific concerns about further stigmatising those who are sick, reinforcing discrimination against people living in poverty, people of colour, and other disproportionately affected by the virus.

III. Promising Practices

- **Implementing "firewalls" that prevent the processing of personal data obtained about a victim or witness to promote access to justice and community safety.**
  - Since 2016, as part of its implementation of the EU Victims' Rights Directive, **the Netherlands** has had in place a national policy ("free in, free out") intended to promote the people in the country with insecure status to report crime without risk of immigration consequences, by prioritising support to victims and positive engagement with communities ahead of immigration enforcement. Advocates applaud the policy but say there is still work do ensure consistent implementation of the policy across the country. The policy arose out of practice developed over many years in the city of Amsterdam and the local police's efforts to work with migrant communities to foster trust and to encourage reporting of crime to support the police's work in improving community safety.[2]
  - In the context of the COVID-19 pandemic, **Ireland** has confirmed that undocumented migrants will be granted full access to social welfare and health care, and that there will be no data sharing between service providers and immigration officers, in respect of the principle of firewall. Undocumented workers who have lost their job due to C-19 will be eligible to apply for the Pandemic Unemployment Payment. **Portugal** has granted residence status to everyone with pending residence application on any ground until 1 July 2020. Individuals granted permits on this basis will be able to access health care and all other public services on equal terms as any other permanent resident in Portugal.

- **Working to bridge the gap between migrants' rights and digital rights advocates to better protect rights in the age of big data and new technology.**
  - **PICUM** organised a legal seminar in November 2019 bringing together digital rights and migrants' rights advocates to attempt to shed light on interoperable migration systems – an issue at the intersection of our respective areas of focus, but with potentially enormous consequences for the rights of migrants in Europe. PICUM is also working with partners to develop various tools to translate these policies and their implications to our members and partners. Digital rights organisations, such as **Privacy International**, **Open Rights Group** (UK) and **Gesellschaft für Freiheitsrechte** (Germany) are increasing working on issues at the intersection of digital rights and migrants' rights.

IV. Recommendations

The European Digital Strategy is being introduced in a context where technology and the processing of personal data are often leveraged for heightened levels of policing and profiling of migrants and communities of colour. It is critical that the strategy creates a shared framework that explicitly reinforces rights, and to mitigate the over-zealous use technology in ways that perpetuate discrimination and social exclusion.

[2] Timmerman, R., Leerkes, A., & Staring, R. (2019) *Safe reporting of crime for migrants with irregular status in the Netherlands*, COMPAS: Oxford.

Bearing in mind the specific concerns of people with insecure migration status, we therefore recommend that the strategy:

- Promote the establishment "firewalls", consistent with the EU's data protection rules, to ensure that personal data obtained when people access health care or social services, or report crime, is not repurposed for immigration control. This protects personal data and the safeguards the right to privacy, as well as a host of other rights, including to due process, that are the bedrock of our democracies.

- Include mechanisms that ensure careful review of the implications for at-risk groups of the use of technology; and develop clear guidelines about the use of personal data and algorithms, based on meaningful input from and engagement with relevant stakeholders including digital rights organisations, representatives from affected communities, non-governmental organisations, data protection authorities, and equality bodies. These guidelines should address data-driven profiling as a form of discrimination incompatible with fundamental rights; and clarify the strict standards for derogations.[3]

- 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.

- Identify community-based good practices for countering racial discrimination and inequality arising from the use of digital technologies.

- Support non-governmental organisations' increased and active engagement in the area of digital rights, particularly among organisations with deep knowledge of and experience with issues of migration, discrimination and inequality, but that may not have a long history of working on issues of technology.

Resources

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

European Commission against Racism and Intolerance (ECRI), 16 March 2016, ECRI General Policy Recommendation No. 16 on Safeguarding Irregularly Present Migrants From Discrimination.

Francois Crépeau, "The Case for "Firewall" Protections for Irregular Migrants: Safeguarding Fundamental Rights", 17 May 2016, *2-3 European Journal of Migration and Law* 157-183.

Molnar P., 12 February 2020, "The human rights impacts of migration control technologies".

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".

UN Committee on Economic, Social and Cultural Rights, 13 March 2017. Duties of States towards refugees and migrants under the International Covenant on Economic, Social and Cultural Rights – Statement by the Committee on Economic, Social and Cultural Rights, E/C.12/2017/1.

[3] The EU's Draft Ethics Guidelines for Trustworthy AI underscore how the use of AI can lead to discrimination, through data bias, incompleteness and bad governance. The Council of Europe's Commissioner for Human Rights has issued recommendations on how to mitigate the "discrimination risks" of AI systems, including through consultation with diverse communities. Council of Europe Commissioner for Human Rights (May 2019), Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights.