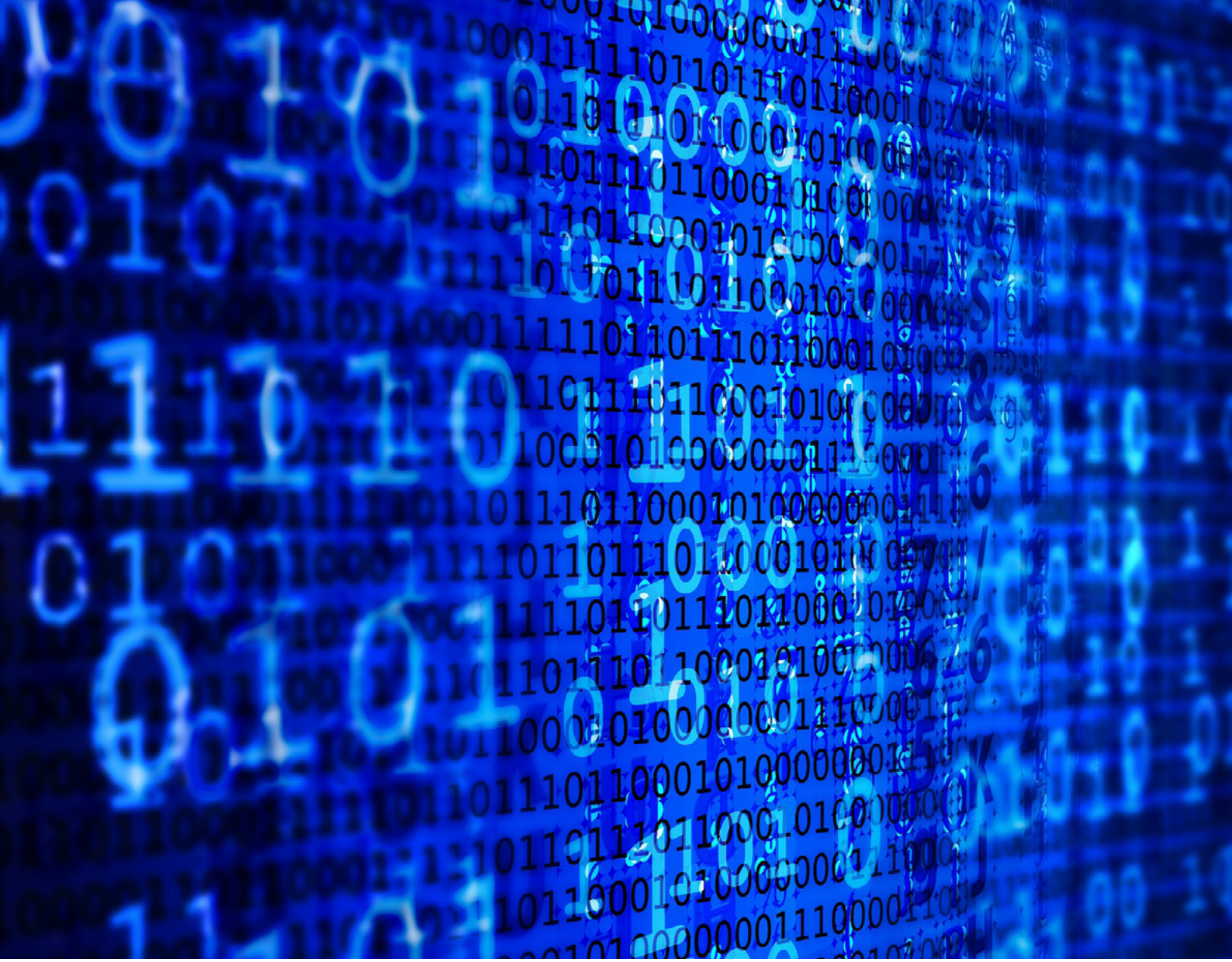

DIGITAL TECHNOLOGY, POLICING AND MIGRATION – WHAT DOES IT MEAN FOR UNDOCUMENTED MIGRANTS?

Briefing paper

PICUM
PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

Table of Contents

Background 3

Digital technology: A growing part of the EU's immigration enforcement strategy and architecture 4

The use of technology in immigration procedures 6

Racial justice dimensions of technology and migration control 7

Where do we go from here? 8

PICUM's Recommendations 10

For European Union officials: 10

For advocates working on the national/local levels: 11

Resources 12

Background

For many migrants' rights organisations, who work every day with and for migrants to support their empowerment and inclusion and against the many forms of discrimination they confront, it may not be immediately clear how questions of data protection, privacy and digital rights are relevant to their work and advocacy. None of the core and pressing challenges that face undocumented people already in Europe, and those seeking to come to Europe who have few options for regular migration, have receded. There are still too few ways for people without significant financial resources or education or the "right" nationality to migrate to Europe; there are still enormous barriers for undocumented people in Europe to access decent work, housing and health care; and still high levels of exclusion and chronic stress due to social and economic precarity, combined with the perpetual threat of identity controls and deportation. And there is still too often impunity for harassment and violence committed by acquaintances, spouses, employers, landlords, strangers, or enforcement authorities against people with insecure migration status. These challenges remain urgent and significant.

So, what about data protection and digital technology? Are these buzz words? What do they mean, in practice, for undocumented people?

Some may think of the use of drones and surveillance technologies at Europe's external borders – and yet the use of digital tools and the large scale processing of migrants' personal data extends well beyond Europe's borders and into communities – beyond even physical spaces into people's devices and their personal and biometric data. The extension of this web of surveillance increases the power of authorities to monitor – and to act – in ways often hidden from view, to screen for, identify and deter or deport foreigners meeting certain "risk" profiles. Meanwhile, civil society is shut out from many of these spaces, and criminalised for efforts to assist those whose lives are put at risk by these policies. Technology is therefore not a trendy side-show, but increasingly imbedded in the vast and intertwined systems that regulate and control migration, and that surveil and monitor migrants.

Digital technology: A growing part of the EU's immigration enforcement strategy and architecture

The trend of using digital technology for immigration enforcement follows the tendency to blur the line between immigration control and security goals. This securitisation framework is not enforced neutrally but rather reinforces existing forms of discrimination against people of colour, religious and ethnic minorities.

For instance, adopted just one year after the EU's General Data Protection Regulation (GDPR) came into force, the **EU's regulations on interoperable migration databases** regulations create a basis for interconnecting multiple migration databases (together with data on criminal records) to pursue goals related to immigration enforcement and addressing serious crimes. The interoperability framework is highly discriminatory, targeting exclusively non-EU nationals for purposes that co-mingle immigration enforcement and the targeting of "serious crimes" like terrorism, implying a false link between serious threats and immigration. It creates a deeply complex system with multiple interconnecting databases that increases the likelihood of errors and makes it extremely difficult to inform people about how their data is used and 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 EU's **Pact on Asylum and Migration**, adopted in September 2020, includes elements on strengthened interoperability and the 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. The Pact also proposes a mandatory "pre-entry" screening at the external border for anyone who enters the EU irregularly for security, health, and vulnerability checks. Significantly, this screening would also apply to people *already* present in the EU, if they entered irregularly. This means that undocumented people could be apprehended in the European countries where they reside and detained for up to three days to be "screened" – identified, registered in databases – and subject to security checks that will determine their status and their fate, raising serious concerns about increased discriminatory policing and racial profiling targeting communities of colour in Europe.

The problem is further embodied in the European Commission's proposals from December 2021 for new rules on internal borders, as part of a reform of the **Schengen Borders Code**, that would increase surveillance and controls over non-EU citizens crossing internal and external borders. The proposals reinforce the view that irregular migration is a threat to the EU that needs to be addressed through more policing – again in ways that are likely to increase racial and ethnic profiling. More specifically, the proposed amended Code would expand member states' powers to conduct identity checks at the internal borders (i.e., within Schengen) to prevent undocumented migrants from crossing them; and scale up the use of monitoring and surveillance technologies at the internal and external borders.

This linking of security and migration agendas has resulted in the EU and member states investing hundreds of millions of euros in the militarisation of internal and external borders. This serves to make coming to the EU more dangerous for people with limited alternatives to come via regular channels. In October 2021, Poland's parliament approved €350 million for the construction of a 5.5 metre wall along its border with Belarus, equipped with motion detectors and thermal cameras, responding to Belarusian authorities' strategy of encouraging migrants to cross the border after the EU imposed sanctions against the country for human rights violations.

This type of surveillance apparatus is not new. Since 2013, **Frontex**, the EU's border and coast guard agency, has run operation Eurosur, a framework for information exchange and cooperation between member states and Frontex to prevent irregular migration and cross-border crime through the use of drones, vessels, manned and unmanned aircraft, helicopters and satellites with radar systems, thermal cameras and high-tech sensors. Eurosur was itself inspired by Spain's surveillance system *Sistema Integrado de Vigilancia Exterior* (SIVE), which, since 2000, has been used to monitor the Spain-Morocco border and Spanish territorial waters using radar technology, high-tech cameras, vessel automatic identification system, and border guards. This was later expanded through partnerships between Spain and Senegal, Mali, Ghana, Ivory Coast, Cape Verde, Guinea-Conakry, Gambia, Nigeria, Guinea-Bissau, Mauritania and Morocco.

The use of surveillance to monitor human mobility is not limited to the sea or to land borders. In Slovenia, the police systematically gather the data (Passenger Name Records) of passengers for all flights arriving from third countries and EU member states into Slovenia, which is matched against "other police data" like criminal files. The police reportedly acquired information about nearly 800,000 airline passengers between October 2017 and November 2018, prompting the Slovenia Human Rights Ombudsman and Information Commissioner to file a complaint with the constitutional court challenging the practice. In December 2021, following a challenge to the mass surveillance measures carried out under the EU's Passenger Name Record (**PNR**) **Directive** (2016/681) by human rights advocates, Belgium's constitutional court asked the EU Court of Justice whether the PNR directive is compatible with the Charter of Fundamental Rights.

In its February 2020 White Paper on AI, the European Commission recognised 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". And yet a pilot project by a company called iBorderCtrl received EU funding to introduce AI-powered lie detectors at border checkpoints in airports in several member states, intended to monitor people's faces for signs of lying, and to flag individuals for further screening by a human officer. This EU funded project has been challenged in the EU's Court of Justice by Member of the European Parliament Patrick Breyer for the secrecy of its documents, believed to have contained information on the algorithms underlying the technology. If the algorithms were used for deception detection purposes, this could indicate a serious encroachment of fundamental rights.

There have also 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 through the Prüm system, which facilitates exchange among member states of data regarding DNA, fingerprints and vehicle registration on law enforcement matters. 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." 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.

The use of technology in immigration procedures

Beyond borders, technology is becoming a growing feature of immigration procedures, based on arguments of efficiency and increased objectivity, while implicitly reinforcing the image of certain types of migrants as inherent untrustworthy or high risk. Migration-related processes increasingly rely on machine learning, automated algorithmic decision-making systems, predictive analytics and related digital technologies. These technologies are integrated into identification documents, facial recognition systems, ground sensors, aerial video surveillance drones, biometric databases, asylum decision-making processes and many other facets of border and immigration enforcement.

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. These trends raise concerns about the ways that "discrimination and exclusion occur in the absence of explicit animus, but as a result of the pursuit of bureaucratic and humanitarian efficiency without the necessary human rights safeguards".

In Germany, for instance, AlgorithmWatch reports that the Federal Office for Migration and Refugees (BAMF) employs automated text and speech recognition systems in asylum proceedings: "Agency employees can ask asylum seekers to give them access to their cell phone, tablet or laptop to verify they are telling the truth about where they come from", running software on the data to extract from the devices. When an asylum seeker does not have a valid ID, a voice recording of the person describing a picture in their mother tongue is analysed by software to evaluate their dialect. In June 2021, a regional court ruled that the searching of asylum seekers' phones was unlawful.

In the United Kingdom, in 2019 the Joint Council for the Welfare of Immigrants (JCWI) and Foxglove launched a legal case challenging the discriminatory nature of the secretive visa algorithms used by the UK Home Office, arguing they created three separate streams or channels for applicants, whereby applications from people of certain nationalities received a higher risk rating and were much more likely to be refused. They alleged that this type of risk streaming resulted in racial discrimination and violated the 2010 Equality Act. In August 2020, the Home Secretary announced plans to end the use of the streaming algorithm, and to do a full review of the system.

In 2022, the EU's new travel authorisation system for people of nationalities currently not requiring a visa to enter the Schengen area, ETIAS, comes into force. ETIAS is one of several EU information systems underlying the EU's "interoperability" framework, outlined above. A 2021 Frontex report makes clear that ETIAS – a database with the personal information of foreigners coming to Europe for holidays and business – is effectively part of the EU's security apparatus: "ETIAS enables the collection of information on people travelling visa-free to the EU in order to deny individuals travelling within the Schengen area who pose a security risk. This is a centralised EU system to issue travel authorisations that enhances external and internal security of the EU."

Racial justice dimensions of technology and migration control

The growing use of technology in the migration context has important racial justice dimensions. In her 2020 report on racial discrimination and the use of technology in the context of borders, the United Nations Special Rapporteur on contemporary forms of racism, Tendayi Achiume, underscores "how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies that have become so prevalent, in part due to widespread perceptions of refugees and migrants as per se threats to national security." She sets out two critical considerations.

1. In most national contexts, non-citizens have fewer rights and legal protections from abuses of state power, while at the same time being targets of xenophobia.

2. Governments retain powers in the area of border and immigration enforcement that are not subject to the typical procedural constraints guaranteed to citizens.

She concludes that, as a result, governments and non-state actors are developing and deploying emerging digital technologies for migration control in ways that are uniquely experimental, dangerous and discriminatory.

The discriminatory aspects of the expanded use of technology for migration control are largely a function of the racial discrimination inherent in migration policies themselves. In a 2018 report, the Special Rapporteur addressed racism in the context of citizenship, nationality and immigration, more generally, highlighting:

> … the impact of ethno-nationalism, and draw[ing] attention to how ethno-nationalists and other groups manipulate national anxieties about national security and economic prosperity to achieve and advance racist and xenophobic policies against indigenous peoples, non-nationals and other minority groups. In doing so, [the report] calls attention both to explicit ideologies of racial superiority and to structural racism that occurs through institutions and policies that might otherwise be ignored due to the absence of explicit racial, ethnic or religious animus.

This "ethno-nationalism", she notes, has deep historical roots, including in relation to Europe's colonial past and xenophobic policies targeting Jews, people of Romani background, sexual minorities and people with disabilities. She underlines the importance of an intersectional approach to citizenship and immigration status, as well as specific considerations of gender: "In the context of citizenship, national and immigration law and policy, States rely heavily on patriarchal laws and gender-based discrimination to achieve racial, ethnic and religious exclusion or restrictions", for instance by denying women the ability to confer nationality on their children.

The close relationship between policing and immigration enforcement– both conceptually, as we have seen, in the pervasive narrative of migration and threat, and operationally, given the role of law enforcement in immigration control in many EU countries – also has significant racial justice dimensions. Research from 2021 by the EU Fundamental Rights Agency shows that people from an ethnic minority are disproportionately affected by police stops, both when they are walking and when in a vehicle. In addition, another study from 2014 showed that 79% of surveyed border guards at airports rated ethnicity as a helpful indicator to identify

people attempting to enter the country in an irregular manner before speaking to them. In December 2021, Dutch border police announced that it would stop using ethnic profiling as a criterion to carry out identity checks following public outcry, despite an earlier ruling by the Hague District Court that border police could use profiling because ethnicity can be an important indication of nationality, and if it is not the only indicator considered and the selection decision is explainable.

Where do we go from here?

On 21 April 2021, the European Commission **proposed new legislation on artificial intelligence (AI)**, the AI Act. Given concerns about its use for migration control and law enforcement ends, advocates welcomed the proposal's ban of certain uses of AI, including the use by police of real-time facial recognition in public spaces; and its categorisation of some uses of AI for migration, asylum and border control as "high risk". But the proposal has been criticised for its loopholes, its strong focus on developers and providers of technology rather than on affected individuals, and weak safeguards on "high risk" uses.

The AI Act is yet another example of how the EU's aspirations for leadership in tech and privacy governance are marred by its massive expenditure of resources and political attention to target non-EU citizens for ever-more invasive and harmful forms of surveillance, monitoring and policing.

In November 2021, a large and diverse coalition of organisations – variously specialised in migrants' rights, patients' rights, disability rights, digital rights, among others – joined a call for changes that would bring it into line with fundamental rights.

In Germany, a coalition including partners as varied as Doctors of the World and Society for Civil Rights (Gesellschaft für Freiheitsrechte), a legal advocacy organisation specialised in privacy rights, joined forces to advocate against policing of migrants that goes beyond migration policy. Their campaign, called *Gleich Behandeln* ("Treat Equally"), targets section 87 of Germany's Residence Act on the "transfer of data and information to foreigners' authorities", which obliges public authorities to report undocumented people they come in contact with to the immigration authorities. The result is that people with irregular migrations status in Germany face immigration control consequences if they try to obtain health care to which they are entitled. In 2021, following this campaign, the new German coalition government adopted a coalition agreement with a pledge to lift these obligations.

Such large and diverse coalitions are critical to influencing the issue of technology in ways that are discriminatory and harmful. Building them requires advocates to step out of their comfort zones to develop the knowledge, relationships and trust needed to work effective together in ways that leverage the efforts and insights of migrant rights, human rights, digital rights, and anti-racism advocates, among others.

Meanwhile, the **EU Anti-Racism Action Plan**, adopted in September 2020, is meant to step up action to counter racial discrimination and racism within the EU. The plan is ambitious in its scope and has been welcomed by anti-racist organisations in Europe. It is the first time structural, institutional and historical

racism have been acknowledged by the EU. Colonialism, slavery and the Holocaust are explicitly mentioned in the Action Plan when addressing the need to acknowledge and teach the historical roots of racism, as is the need to mainstream racial equality and anti-racism in EU and national policies – including in the areas of digital technologies and migration. Consistent with the motivation behind its publication, the Commission specifically addresses discriminatory policing towards racialised communities in Europe, including racial or ethnic profiling, recognised as unlawful and damaging for reporting of crimes.

And yet, a few days later, the Commission released a new Pact on Migration and Asylum with a strong focus on increasing the number of migrants to be returned and setting border procedures that will increase their detention, where interoperable migration databases and the scaled up use of digital technology are centrepieces.

The EU and member states' increasing deployment of technology to support militarised approaches to immigration control stands in stark contradiction to its standard-setting legislation on data protection and privacy – protected under the EU Charter of Fundamental Rights and the GDPR – and its bold stance against racism. It is therefore critical for the European Commission to use the opportunity of new AI legislation and the Anti-Racism Action Plan to recalibrate its approach, by prioritising fundamental rights and broader democratic values.

PICUM's Recommendations

For European Union officials:

- **Adopt an Artificial Intelligence (AI) Act that recognises and addresses the fundamental rights implications of some uses of artificial intelligence**. This means, among others;
  - » ensuring that the AI Act applies to uses of AI in the context of the EU's migration databases;
  - » ensuring that uses of AI in the migration context for profiling and individual risk assessments, for polygraphs and emotion detection are recognised as presenting an unacceptable risk to human safety and to fundamental rights;
  - » including uses of AI in the migration context for predictive analytics and automated surveillance for detection (i.e., not just identification) among high-risk uses of AI;
  - » including in the AI Act robust and consistent update mechanisms for "unacceptable" and "limited" risk AI systems, as well as obligations on users of high-risk AI to conduct a fundamental rights impact assessment;
  - » creating individual rights in the AI Act as a basis for judicial remedies, as well as a right to effective remedy where those rights have been infringed and a mechanism for public interest organisations to lodge a complaint with national supervisory authorities.
- **Ensure democratic oversight and systems of accountability of uses of digital technology and large-scale processing of personal data**. Given the well-recognised asymmetries of information and of power between those who develop and deploy digital 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 harmful effects of these systems. There must also be accessible systems of accountability in place to permit redress for rights violations linked to the use of these systems and technologies. This requires empowering equality bodies, data protection authorities, and other relevant public bodies to ensure accountability for the implications of digital technology and data processing for human rights and discrimination; and creating rights of redress for those harmed.
- **Live up to commitments under the EU Anti-Racism Action Plan by mainstreaming a racial equality perspective across all policy areas, including migration**. Scholarship has made clear that the politics of race and the politics of migration are deeply intertwined. The European Commission should, through its Equality Task Force and other structures, take steps to identify and address the racial equality dimensions of the EU's migration policies, with meaningful engagement from racial justice and migrants' rights advocates in the process. This includes deleting the provisions of the Schengen Borders Code which would lead to an increase in the use of surveillance technologies and racial profiling.

For advocates working on the national/local levels:

- **Connect with digital rights and racial justice advocates in your national context** to explore and understand together the policies and practices that affect undocumented people in your country – at the border (e.g., remote surveillance, screening procedures), in their interactions with immigration authorities in asylum and visa procedures, and in their interactions with the police.

- **Inform undocumented people of how digital technology affects them – and about how to defend their rights**. The lack of transparency around the use of digital technology and its complexity make it very hard to understand where and how it is being used, much less to monitor and hold public and private actors accountable for its use (and misuse). What is clear is that there will be practical consequences for migrants, and they should be aware of how they will be affected – and how they can challenge errors and violations of their rights. We all need to do what we can to support them in this. While problematic in many ways, EU law provides strong protections for the right to privacy and data protection, regardless of a person's residence or migration status. National data protection authorities and human rights bodies can also be an important source of information and provide avenues for accountability.

- **Press for policies that ensure that immigration enforcement is kept separate from the delivery of key services**. Advocate for the creation of "firewalls" to ensure that undocumented people who try to get health care, go to school, access services, report crime or seek redress for labour rights violations do not face immigration consequences, and these safeguards are well publicised and robustly implemented.

- **Document the impact of digital technology on undocumented people**. Where you see uses of digital technology that are discriminatory or harmful, or barriers to accountability, document it. This will provide evidence that can support advocacy as well as possible legal challenges to change problematic laws and practices.

- **Engage and advocate**. Digital rights and migrants' rights can seem like distant spheres, with little in common. But the world is changing, and the overlap between digital rights and migrant rights is closer than ever, and the stakes higher than ever. It is critical that organisations and advocates step out of their silos and have the courage to educate themselves and to speak up, together, on these issues that are at the intersection of our work, recognising and leveraging their respective areas of expertise and competence. It is critical that advocates push back against the framing of digital rights issues and solutions as mainly technical matters for computer scientists and "experts", and that the broader human rights and racial justice context be brought to bear in this work and advocacy, through collaboration and joint advocacy.

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'.

PICUM
PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

Rue du Congres / Congresstraat 37-41, post box 5
1000 Brussels
Belgium
Tel: +32/2/210 17 80
Fax: +32/2/210 17 89
info@picum.org
www.picum.org

© PICUM, 2022

Cover: Geralt - Pixabay

This report has received financial support from the European Union Programme for Employment and Social Innovation "EaSI" (2021-2027). For further information please consult: http://ec.europa.eu/social/easi. The information contained in this publication does not necessarily reflect the official position of the European Commission.