MIGREUROP BRIEF
N° 12
FIRST EDITION

PHOTOGRAPHY : **PUSHED-BACK FROM ALGERIA, MIGRANTS ARE IDENTIFIED BY THE IOM IN AGADEZ, NIGER IN 2018** © FRANCESCO BELLINA

DATA AND NEW TECHNOLOGIES, THE HIDDEN FACE OF MOBILITY CONTROL

December 2020

In a July 2020 report, the European Agency for the Operational Management of Large-Scale IT Systems (eu-Lisa) presented artificial intelligence as a "priority technology". The report underlines the advantages of artificial intelligence (AI) in the field of migration and borders thanks, amongst other things, to facial recognition technology.

AI is increasingly privileged by public actors, EU institutions and private actors, but also by the UNHCR and IOM. EU agencies like Frontex and eu-Lisa are particularly active in experimenting with new technologies, increasingly scrambling the distinction between development and implementation. Besides traditional surveillance tools, a panoply of technologies is now deployed at the borders of Europe and beyond: the addition of new databases, innovative financial technologies, or simply the gathering by 'Big Tech' of data given voluntarily – or not – by migrants and refugees during their journeys.

The COVID-19 pandemic has arrived at the right time to give new impetus to an established course of action, making it possible to test or to generalise technologies used for the control of mobility without taking into account the rights of exiles. The IOM, for example, has put its 'Displacement Tracking Matrix' at the disposal of states during this period with the aim of controlling migratory flows. New technologies at the service of old obsessions…

migreurop

Digital applications: protecting exiles, or protecting borders?

Studies on "bordering" are largely concerned with more visible technologies, such as fences, radars or drones. But recent technologies' advantages are being generalised under the pretext of protecting exiles, providing them with a service or even reinforcing their autonomy. These supposed protections are a corollary to the control of frontiers and, at the level of the EU and its member states, these technologies function as devices of "social sorting" and for the differential attribution of rights.

In numerous camps around the world, asylum-seekers receive a monthly financial payment via a prepaid card, which is presented by the UNHCR and states as a means for increasing recipients' autonomy. But these cards also facilitate surveillance (by making it possible to trace cash withdrawals and transactions) and control (recipients can only buy items considered useful by the UNHCR and from approved vendors).

Equally, the UNHCR's strategy of "digital inclusion" and "digital identity" for refugees rests on the idea of increasing their autonomy and participation in economic and social life, and combatting identity fraud. In Jordan, since 2016, an iris scanner designed by IrisGuard has been used to identify asylum-seekers in Zaatari camp. Implemented to "protect the identity" of refugees and guarantee them a "civil status", it also contributes to controlling them. The system communicates automatically with UNHCR's registration database to confirm the identity of the beneficiary, checks their account balance through Jordan Ahli Bank and Middle East Payment Services, and then confirms the purchase.

Applications such as Whatsapp, Viber, Skype and Facebook are not at first glance perceived as technologies of control. They are, however, tools for extracting data, and they are not only deployed by border guards, the police or the asylum authorities, but are also increasingly used by the UNHCR and IOM. Surveillance and control through these technologies is imperceptible, principally because the circuits of data extraction remain largely unknown.

While civil society as a whole has very little knowledge of the risks raised by these applications, in terms of the protection of privacy and personal data, exiles are even more severely impacted: in part because, even less so than others, they are not able to give any kind of consent regarding the collection or use of their data. On the other hand, their fate is closely tied to the use of these digital tools. Thus, when applications fail, when there is no connection, or when calls are unsuccessful, the risk of exiles being denied their rights, including humanitarian aid, is all the more likely.

The ways in which digital technologies can be used has been limited by privacy regulations. So when the European Asylum Support Office (EASO) attempted to use social networks to monitor migratory routes, it was forced to back down. However, it is not yet possible to hold private agencies or actors (such as Microsoft, Accenture, Leonardo, etc.) accountable in the field of migration, in particular regarding how and why they use technologies at the border, in refugee camps and in detention centres.

The European Pact on Asylum and Migration foresees the establishment of an independent control mechanism to guarantee respect for fundamental rights during "screening" procedures at the borders. But it says nothing of responsibility for the extraction of data nor about technologies deployed at borders, whether during control procedures or after them, leaving many questions unanswered.

New technologies put to the test

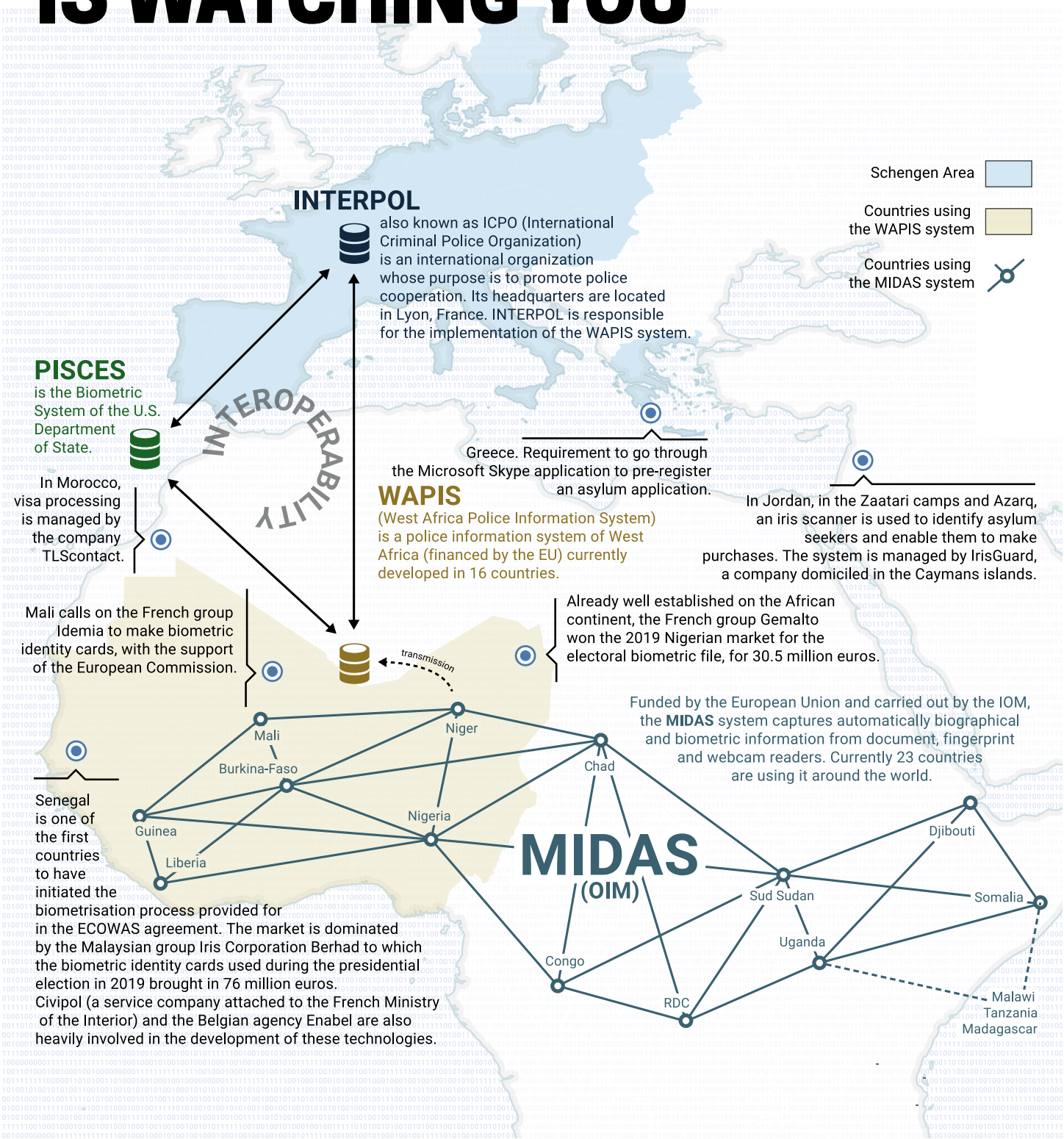
Technological advances have transformed the work of humanitarian agencies, for example through the use of drones to send equipment to inaccessible areas, with 3D printing for creating prostheses, or through the collection of biometric samples (fingerprints, dental prints or DNA) in the framework of medico-legal work for establishing the identity of victims. While in the last case the samples collected are anonymised before being sent to a laboratory, humanitarian agencies generally require the registration of personal data for carrying out their mission (such as civil status, contact details, family situation, iris scans, etc.). This system of profiling and tracing could lead to catastrophe if the data were to fall into the wrong hands.

This challenge worries humanitarian agencies and some of them, notably the International Committee of the Red Cross, have called for the creation of a "digital humanitarian space" to provide a sufficient international level of protection.

On the contrary, national and EU agencies such as Frontex openly embrace new technologies, such as biometrics, with the aim of controlling human mobility. The data collected feeds systems on asylum-seekers such as Eurodac, where the use of personal data is not limited to asylum proceedings. For example, it is also possible to use the data to confirm an individual's identity prior to expulsion.

In addition, the interoperability of EU databases, set in motion by two Regulations of 14 May 2019, has been established, reinforcing the possibility of cross-referencing the data held within different systems. The EU also exercises a right of control, via Frontex, over the system for gathering and analysing migration data installed in Makalondi in Niger (MIDAS). Furthermore, a Privacy International report shows that the EU Emergency Trust Fund for Africa has financed biometric identity systems in Senegal and in Ivory Coast, with the aim of identifying undocumented persons residing in Europe with the aim of organising their expulsion.

BIG DATA IS WATCHING YOU



Sources :

Mediapart, *Au Niger, l'UE mise sur la police locale pour traquer les migrants*, 28 February 2019

IOM Brochure, *Un système d'information efficace et abordable pour la gestion des frontières*, 2018

Interpol website, WAPIS Programme

Mediapart, *Au Mali, Niger et Sénégal, le marché de l'identité en plein essor*, 5 March 2019

Le Monde Diplomatique, *Les réfugiés, une bonne affaire, payer en un clin d'œil*, May 2017

World Food Programme, *WFP Introduces Innovative Iris Scan Technology To Provide Assistance To Syrian Refugees In Zaatari*, 6 October 2016

Socialnetlink, *L'UE finance l'état civil du Sénégal avec une technologie biométrique de 28 millions d'euros pour identifier et faciliter les expulsions*, 23 November 2020

Digital platforms and financial-humanitarianism

While the role of private corporations and giant contractors in migration industry has been widely analysed by NGOs and human rights organisations, little has been said about the opaque role played by financial actors and high-tech corporations.

In 2016, the European Commission has funded and implemented a Cash Assistance Programme for asylum seekers. The Cash Assistance Programme consists in a monthly financial support which is given to asylum seekers and which is uploaded on prepaid cards, sponsored by MasterCard (EUR 90 for a single person, or EUR 150 if the person lives in a reception centre with no kitchen equipment). The Programme is run by the UNHCR and the financial provider involved, called Prepaid Financial Services, is based in London. For each transaction, beneficiaries have to pay a commission fee to the Greek banks where they take cash from. The financial provider traces the card transactions of the card beneficiaries and where these have been made. Every prepaid card is associated to a unique UNHCR financial wallet: that is, they are not associated with individual bank accounts, and asylum seekers cannot transfer their own money there.

In France, the cash assistance allocated to asylum seekers by the Ofii (Office français de l'immigration et de l'intégration) has been replaced by debit card only meant for payment in shops that accept the card, not to withdraw cash. Such a system is hampering in many daily instances (purchase of small food quantities, of bus tickets, rent payment to private landlords etc.). Non-profit organisations have denounced the very downgrading impact which such a process is having, mostly meant to exert a greater control over the people forced to use it, so they stress.

Actually, prepaid cards are also used as a way for disciplining and controlling exiles - by introducing restrictions on the products they can buy, or in some cases not allowing them to use the card at the ATM machines.

Moreover, the incorporation of digital technologies in the asylum regime raises major stakes about the economic circuits and the value produced in what has been called 'techno-humanitarianism'. Microsoft's partnership with the UNHCR traces back to 1999, and it has been further strengthened over the last two years. Some of Microsoft's services are used by UNHCR officers allegedly to speed up responses to humanitarian emergencies and "protect" refugees' data. As an example is BIMS, a system where the data of 250,000 refugees and internally displaced persons (IDPs), or Project Profile and Progres, which are storing a large amount of personal data such as 'the number of persons present in the camp, their age, the mortality rate, the geographical area of origin, the type of protection needed and even the medical status as well as details on food habits and nutrition'. Such a partnership, albeit official, does not clarify if Microsoft can access data, store it, and to what end.

In a similar manner, apps such as Viber, WhatsApp and Skype are by now widely used by international agencies – e.g. the UNHCR and the IOM – as well as by state actors to communicate with asylum seekers. In Greece, since 2016, migrants who want to claim asylum on the mainland are obliged to book an appointment with the Asylum Service via Skype.

The mandatory Skype call has been denounced many times during collective protests organised by asylum seekers in Athens over the last three years. The latter have reported about the lines being always busy in addition to the need for and Internet connection to call during specific weekly time slots. The Greek government has recently activated a Viber chat to keep asylum seekers updated about the situation in Lesvos. Those benefiting from the Cash Assistance Programme were bound to download the app so they could report the technical problems encountered with their prepaid cards.

Such an insight into financial actors and apps sheds light into an emergent field of the migration industry that should be object of close scrutiny: these "invisible" actors which (actively) contribute to controlling and governing migration, constantly extract data from exiles. The kind of data they extrapolate - and might retain – inform about migrants' behaviours, movements and social interactions. The extent to which and how many actors access data and are making profit out of it is yet to be researched and assessed. The fear of general surveillance over exiles via social networks is spreading and has prompted some to hide their identity online not to be tracked. It is unknown however if anonymity will be possible much longer with mobile phones increasingly equipped with biometric locking processes based on fingertip or facial recognition.

The bibliography is available on Migreurop website: www.migreurop.org in the section *Publications / Notes*.
http://www.migreurop.org/article3021.html

migreurop

Migreurop is a network of associations, activists and researchers, with a presence in around twenty countries across Europe, Africa and the Middle East. The network strives to raise awareness of and to oppose policies that marginalise and exclude migrants, notably, detention in camps, various forms of displacement and the closure of borders, as well as the externalisation of migration controls by the European Union and its Member States. In this way, the network contributes to defending migrants' fundamental rights (including the right '*to leave any country, including their own*') and to promoting freedom of movement and settlement.

www.migreurop.org

Connect with migreurop on and @migreurop

MIGREUROP - CICP - 21ter rue Voltaire 75011 Paris

Photography by Francesco Bellina – Graphic design by La Société
Managing editor: Claudia Charles

WITH THE SUPPORT OF:

ccfd-terre solidaire · The Fund for Global Human Rights · Fondation un monde par tous · Fondation Abbé Pierre