EUROMED RIGHTS

ARTIFICIAL INTELLIGENCE: THE NEW FRONTIER OF THE EU'S BORDER EXTERNALISATION STRATEGY

A study on the use of Artificial Intelligence and other types of technologies in the external dimension of EU migration, with a focus on the deployment of EU-funded technologies for border control.

JULY 2023

JULY 2023

EuroMed Rights
Vestergade 16, 2nd floor
DK-1456 Copenhagen K
Denmark

Tel: +45 32 64 17 00
information@euromedrights.net
www.euromedrights.org

Bibliographic Information

Title: Artificial Intelligence: the new frontier of the EU's border externalisation strategy
Author: Antonella Napolitano for EuroMed Rights
Date of initial publication: July 2023
Pages: 29
Original Language: English

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the last three decades, border externalisation has been a core tenet of the strategy that the European Union has adopted to deal with migration flows, especially those coming from the African continent. The geopolitical importance of MENA countries positioned the region at the forefront of EU plans of externalisation, becoming a testing ground for new tactics and practices.

Additionally, migration is also used by governments in the MENA region to instrumentalise EU Member States' foreign policies. As explained by EuroMed Rights: "This 'blackmailing' approach to bilateral and multilateral cooperation on migration results from externalisation policies and the conditionality approach implemented by the EU and Member States." Migrants and refugees are used as "tools" of political pressure, with origin and transit countries negotiating economic and geopolitical benefits with EU and Member States without concerns about the consequences for people, from fundamental rights violations to loss of life. Also, the logic of conditionality has been shaped through budgets structured around the external dimension of migration: the EU Emergency Trust Fund (EUTF) in 2015 and the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe) from 2021 push African countries to instrumentalise the departure of migrants in their own interests."

In recent years, a new element has been emerging in this externalisation strategy: the use of EU funds – including development aid – to outsource surveillance technologies that are used to entrench political control both on people on the move and local population.

This is a particularly sensitive topic for countries in the MENA region: journalists and NGOs have reported many times on how autocratic governments are routinely using surveillance technology tools to further repress human rights defenders and journalists, suppress freedom of expression and the media with full impunity. As highlighted by the MENA Surveillance Coalition, "the MENA region has become a breeding ground for invasive surveillance, allowing for private tech companies to reap profits off egregious human rights violations".
This report aims at building an understanding of how this new line of funding to fragile democracies and authoritarian governments is used by the European Union to manage borders and curb migration, without regard for possible human rights violations against people on the move as well as local populations.

In the first chapter, we will explore how the outsourcing of surveillance technology has become a new, increasingly central element of the European Union border externalisation strategy, particularly geared towards the strategic MENA region. In the second chapter, we will look at the threats brought by sophisticated technologies and artificial intelligence in particular to people on the move in origin and transit countries, with a particular focus on the policy developments on the EU AI Act.

In the third chapter, we will take a closer look at the European Union as a funder of surveillance. We will focus on projects in MENA countries funded under the EU Emergency Trust Fund for Africa and the new funding instrument Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI – GE).

Finally, we will conclude with a reflection on how the implementation of these new tactics in border externalisation is supporting authoritarian governments in MENA countries, further fueling instability in the region.

A NOTE ON RESEARCH AND METHODOLOGY

This report aims at building an understanding of how funding the outsourcing of advanced technologies to authoritarian regimes in non-EU countries is used by the European Union to manage borders and curb migration, without regard for the rights of people on the move as well as for local populations.

It is a complex area of work that encompasses diverse expertise. This document builds on the work of researchers, activists, academics, journalists - and suffers from the same challenges that they have faced for years.

Understanding the impact of these new technologies (and of the funding that enables their deployment) is directly related to transparency in public administration, which is severely lacking and hinders attempts to illuminate how these systems work and how they can be challenged.

Most recently, the authors of "EU migration and asylum funds for third countries", a comprehensive research requested by the LIBE Committee of the European Parliament and published in December 2022, have noted that "accessibility of data related to EU funding on displacement and migration is a significant challenge, and constitutes the most notable difficulty encountered by the study. This means in turn that assessing coherence, effectiveness and efficiency is rendered very difficult." They also mentioned the example of a group of journalists from Nigeria, Italy and the Netherlands who tried to grasp EU funding related to migration going into Nigeria, without being ultimately able to verify whether the list they compiled was the complete one.

In the attempt of providing ways for others to continue and expand on research and advocacy, in addition to the bibliography, we are sharing some of the tools and resources we used:

- The Financial Transparency System Data from 2014 to 2021
- Ted - eTendering. Call for tenders from the European Institutions
- Funds for Fortress Europe: spending by Frontex and EU-LISA
- An Open Source Guide to Researching Surveillance Transfers

ACRONYMS

AFIC: Africa-Frontex Intelligence Community
CEPOL: European Union Agency for Law Enforcement Training
DCI: Development Cooperation Instrument
DPIA: Data Protection Impact Assessment
EAAS: European External Action Service
EDF: European Defence Fund
EIDHR: European Instrument for Democracy and Human Rights
ENI: European Neighbourhood Instrument
AI Act: Artificial Intelligence Act
EUTF: European Union Emergency Trust Fund for Africa
FRONTEX: European Border and Coast Guard Agency
GACS: General Administration for Coastal Security
GDPR: General Data Protection Regulation
HRIA: Human Rights Impact Assessment
IcSP: Instrument contributing to Stability and Peace
IMSI: International Mobile Subscriber Identity
MPE: Mobile Phone Extraction
NDICI: Neighbourhood, Development and International Cooperation Instrument
OHCHR: Office of the United Nations High Commissioner for Human Rights
OSINT: Open Source Intelligence
PI: Privacy international
SOCMINT: Social Media Intelligence
UAV: Unmanned Aerial Vehicles
UNODC: United Nations Office on Drugs and Crime

A NEW TACTIC IN BORDER EXTERNALISATION: OUTSOURCING SURVEILLANCE TECHNOLOGY

In the last three decades, border externalisation has been a core tenet of the strategy that the European Union has adopted to deal with migration flows. The MENA region has been at the forefront of EU plans of externalisation, becoming a testing ground for new tactics and practices. In recent years, two new elements have become central to this strategy: funds for development aid have now officially become a tool for carrying out border control policies in countries of origin and transit, with some of them also used to outsource surveillance technologies, that are in turn employed to entrench political control both on people on the move and local population. This raises serious concerns on human rights abuses in non-EU countries.

Border externalisation is a term used by migration scholars, policy makers, civil society and the media to describe "the extension of border and migration controls beyond the so-called 'migrant receiving nations' in the Global North and into neighbouring countries or sending states in the Global South. It refers to a wide range of practices from controls of borders, rescue operations, to measures addressing the drivers of migration".

Collaborations with third countries can entail a variety of measures, such as "accepting deported persons, training of their police and border officials, the development of extensive biometric systems, and donations of equipment including helicopters, patrol ships and vehicles, surveillance and monitoring equipment". Many of these projects are funded through the European Commission, but individual member states – especially Italy, Spain, and Germany – have a leading role in supporting bilateral externalisation agreements with non-EU countries.

In the last three decades – and more aggressively since 2005 – border externalisation has been a core tenet of the strategy that the European Union has adopted in dealing with migration flows. While "measures to keep people from reaching sanctuary are as old as the asylum tradition itself", the policies deriving from this strategy have been more evident since 2015, becoming the main instrument through which the European Union seeks to stop people migrating and seeking asylum in Europe.

However, there are two relatively new elements: one is that funds for development aid – traditionally used in a strategic way – have now officially become a tool for carrying out border control policies in countries of origin and transit. The second is that these and other funds are also used to outsource surveillance technologies that are used to repress people's fundamental rights and entrench political control both on people on the move and on local populations.

Surveillance technology encompasses any digital device, software or system that gathers information on an individuals' activities or communications. Often framed as necessary to prevent crime and terrorism, these tools and techniques are extremely intrusive and hinder fundamental rights.

In 2019, the then United Nations Special Rapporteur on freedom of opinion and expression, David Kaye, presented a report on the surveillance industry and its interference with human rights to the Human Rights Council, calling for an immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place: "Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation," he wrote. He went on to mention some of these sophisticated surveillance tools, including mobile device hacking, network intrusion, facial recognition surveillance – all of them routinely used to monitor journalists, politicians, human rights advocates, and even UN investigators.

For decades, EU plans of border externalisation have pushed the southern border of Europe further south: as a result, the MENA region has increasingly become a testing ground for new tactics and practices. In the last few years, this has also translated into a newfound interest to provide and support the use of surveillance technologies in every country in the region, with the final aim of preventing departures. This resulted in serious risks for the rights of both people on the move and local populations.

According to human rights organisation Privacy International, the EU institutional support through funding, including development aid, to third countries comes in five main forms: "direct equipping of foreign intelligence and security forces; training of foreign intelligence and security forces; financing of their operations and procurement; facilitating exports of surveillance equipment by industry, and promoting legislation which enables surveillance." Privacy International also points to the creation of biometric identity systems (including providing equipment, training officials in their use, and influencing laws in beneficiary countries) as another type of initiative that can be used to share people's data with EU authorities and assist in deportations from Europe.

> "The main thing about the externalization process is that, within its context, negotiations begin with third countries without first assessing the human rights standards in those places or the way local governments handle immigration issues".

Concerns in how these EU-funded projects are implemented include the lack of Human Rights Impact Assessments (HRIA) or Data Protection Impact Assessments (DPIA), or those assessments not being conducted, or conducted as compliance checkbox rather than decision tools.

Increased scrutiny of these new ways of implementing border externalisation practices, shows that concerns are well founded.

In December 2022, the European Ombudsman found that the European Commission had not taken the necessary measures to ensure "a coherent and structured approach to assessing the human rights impacts" in the transfers of technology with potential surveillance capacity to non-EU countries supported by the EU Emergency Trust Fund for Africa (EUTF for Africa), a key funding tool launched in 2015 to "deliver an integrated and coordinated response to the diverse causes of instability, irregular migration and forced displacement." The investigation was prompted by a complaint filed by Privacy International, together with Access Now, the Border Violence Monitoring Network, Homo Digitalis, International Federation for Human Rights (FIDH), and Sea-Watch, outlining how EU bodies and agencies were cooperating with governments around the world to increase their surveillance powers.

The Ombudsman further suggested that "the Commission's guidelines concerning the evaluation of EU Trust Fund projects, both in Africa and elsewhere, should require that an assessment of the potential human rights impact of projects be presented together with corresponding mitigation measures." Two similar complaints to the Ombudsman in relation to Frontex (the European Border and Coast Guard Agency) and to EEAS (the European External Action Service) are currently being investigated.

Human Rights Impact Assessments and Data Protection Impact Assessments

A Human Rights Impact Assessment (HRIA) enables an analysis to which a policy or project or measure affects human rights. HRIAs follow a human rights-based approach, which integrates human rights principles into the assessment process. This includes both actual impacts occurring in the present and potential impacts that could occur in the future.

A Data Protection Impact Assessment (DPIA) is a tool that gauges the ways projects, systems, programs, products or services impact the data an organisation holds, and increasingly they are being required by law for certain data processing. According to article 35 of the GDPR, a DPIA shall in particular be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- a systematic monitoring of a publicly accessible area on a large scale.

TECH AT THE BORDER, ARTIFICIAL INTELLIGENCE, AND THE AI ACT

The use of technology is usually hailed as a way to create progress, innovation or improvement, ultimately giving a sense of objectivity and efficiency.

Following their use by police forces, advanced technologies and systems that collect personal data are today key components of immigration enforcement: government authorities are exploiting these technological developments, often with the support of the private sector, to inform decision making that has real consequences on the lives of people on the move. These systems, in fact, use invasive technology and are built on potentially biased or even unscientific assumptions that discriminate against people, putting them at greater risk and ultimately depriving them of agency.

As for many other policy spaces, when it comes to border management, artificial intelligence appears to be the next frontier. Its regulation has been identified by the European Union as a priority to govern its development and its seismic consequences, but exemptions in the area of migration and asylum remain, with potential violations of the rights of people on the move.

Increasingly, police law enforcement in EU countries have been using sophisticated technology and artificial intelligence systems to profile people and places with the promise of assessing alleged 'risk' factors and 'predict' criminal behaviour. In one of their analyses, European Digital Rights (EDRi), the biggest European network defending rights and freedoms online, states that "These predictions, profiles, and risk assessments, conducted against individuals, groups and areas or locations, can influence, inform, or result in policing and criminal justice outcomes, including surveillance, stop and search, fines, questioning, and other forms of police control. They can lead to arrest, detention, prosecution, and are used in sentencing, and probation. They can also lead to other, civil punishments, such as the denial of welfare or other essential services, and increased surveillance from state agencies".

This approach has been extended to migration and border control, with a broad range of technology and data intensive systems used at different stages of the asylum process or migration management and enforcement, ultimately depriving people of their agency. These invasive systems, in fact, are built on potentially biased or even unscientific assumptions that discriminate against people, putting them at greater risk.

But despite their power to make life-changing decisions and the potential for human rights violations, the use of advanced technologies has been framed mainly as an opportunity by EU institutions without much regard for the long-term consequences of these systems on people.

In a 2020 report titled "Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security", the European Commission defines "Artificial Intelligence" (AI) as "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy to achieve specific goals". The report, written by consultancy firm Deloitte, goes on to explain that "the amount of data available for AI models to learn from is greater than ever before, and continues to grow at pace." The report also clusters "opportunities" into five different groups: chatbots and intelligent agents, risk assessment tools, knowledge management tools, policy insight and analytics tools, and computer vision tools. Functions include risk assessments and profiling, identity verification and fraud detection, behaviour/emotion recognition, speech recognition, mobile phone data extraction, electronic monitoring, and forecasting of future mobility.

While they are presented as efficient solutions for border management, these technologies with

"predictive" analytical capabilities prevent from grasping the unique experiences of the people subject to their decisions: from being denied entry in a country to family separation, their impact on migrants' free movement and human rights is incalculable.

For example, emotion recognition technologies claim to detect people's emotions based on assumptions about how someone acts when feeling a certain way, including to assess their credibility. Some member states have tested the use of these types of systems as "lie-detectors" to inform decisions about who qualifies for protection. However, journalists and experts have tested the tech and called it "not credible". Other softwares to analyse speech claim they can assess whether someone's dialect matched the region they say they are from.

The Artificial Intelligence (AI) Act

The regulation of artificial intelligence has been identified by the European Union as a priority to govern its development and its consequences. In April 2021, the European Commission proposed the first ever legal framework on AI, commonly called the Artificial Intelligence Act, or AI Act. It is considered the first binding legislation on AI in the world. The regulation also defines and regulates risks associated with AI systems, with one of the key issues being what type of AI applications are to be banned because they are considered to pose a significant risk[6].

Civil society organisations working on digital rights and migration issues have come together to denounce the uses and implications that automated risk assessment and profiling systems have in the migration context and to challenge the lack of protection for fundamental rights of people on the move. In particular, a coalition of 13 civil society organisations including EuroMed Rights have called on EU legislators to ban the use of experimental tech against people crossing borders, and effectively regulate to ensure AI is used with safety and accountability. The coalition calls for:

1. **Ban harmful AI practices in the migration context**, including predictive analytics systems used for preventing migration; automated risk assessments and profiling systems; 'Lie-detectors' and all technology that claims to categorise people and infer emotions on the basis of their biometric data; Remote Biometric Identification at the border and in and around detention facilities that enable mass surveillance.

2. **Regulate all AI high-risk systems in migration**. All AI systems used in migration should be subject to oversight and accountability measures, including surveillance technology used in the context of border control and for identity checks.

3. **Ensure the AI Act applies to the EU's huge migration databases**

4. **Make the EU's AI Act an instrument of protection**. Lawmakers must ensure the EU AI Act empowers people to seek justice, guarantee public transparency, and prevent harm from the most harmful AI systems when used in migration and border control.

On 11 May, 2023 the European Parliament's Civil Liberties and Internal Market committees voted on a final text of the AI Act. The text bans harmful uses of AI and subjects "high-risk" uses to enhanced safeguards.

Among the bans that were voted, there are:

- Emotion recognition technologies, which explicitly extends to the EU's borders.
- Biometric categorisation systems that use personal characteristics to classify people and to inform inferences based on those characteristics.
- Predictive policing systems, which use preconceived notions about who is risky to make decisions about the policing of certain groups and spaces.

While these bans are welcomed, the text still falls short on some especially dangerous elements: "the predictive policing ban, which encompassess some forms of algorithmic profiling used in the migration context, does not fully capture the several uses and implications that automated risk assessment and profiling systems have in that context. The Committees also missed the chance to prohibit predictive analytics systems used to curtail migration movements and that can lead to push-backs."

The AI Act was voted by the European Parliament on 14 June 2023. The vote upheld red lines against harmful uses of AI, including protecting people against live facial recognition and other biometric surveillance in public spaces, emotion recognition in key sectors, biometric categorisation, predictive policing and social scoring. However, the final text failed to introduce new provisions to protect the rights of migrants from discriminatory surveillance even though AI systems are increasingly developed to track, control and monitor migrants in new and harmful ways, effectively creating "a two-tiered AI regulation, with migrants receiving lesser protections than the rest of society." It will now enter the interinstitutional negotiation — also known as trilogue — with the Commission and the Council, and it is expected to be finalised by the end of 2023.

[6] Significant risk is defined as "a risk that is significant as a result of the combination of its severity, intensity, probability of occurrence, and duration of its effects, and its ability to affect an individual, a plurality of persons or to affect a particular group of persons".

EU-Funded Research and Experiments at the Border

A comprehensive analysis of technologies at the border, their impact on human rights, and whether these technologies even perform what they promise, is beyond the scope of this paper and it is already widely explored by many researchers, journalists, civil society organisations and academics.

However, it is important to highlight another worrying aspect in how artificial intelligence and technologies are employed in the context of migration and border issues: the growing number of EU-funded research projects that create or experiment with advanced surveillance and predictive tools, including forecasting tools with the objective to "forecast future mobility". These projects include initiatives purportedly designed to help humanitarian organisations and immigration authorities to better plan and allocate their resources in advance but have the potential to contribute to the securitisation approach of the European Union.

An example is EUMigraTool (EMT), developed by an EU-funded project under Horizon 2020's[6] Secure Societies program, called ITFLOWS. According to the website, the tool "will provide predictions of the number of migrants coming to a specific European country, 'analysis on drivers, patterns and choices of migration, as well as public sentiment towards migration', and 'the identification of risks of tensions between migrants and EU citizens". The data sources used for predictions include video content from TV news, web news and text content from social media, such as Twitter. The sources are from various agencies, social media platforms, and datasets.

Civil society and academics have called for a ban of the tool and urged the project to refrain from developing predictive analytics systems, noting that they could be "generating and exacerbating assumptions that particular groups present a 'security risk' or a threat of 'irregular migration', and encouraging punitive responses geared toward the interdiction of movement".[7]

THE EU AS A FUNDER OF SURVEILLANCE

In recent years, the use of development budget for border control-related projects and the use of international cooperation support as leverage for readmission agreements or to prevent departures have marked the approach of the European Union to cooperation with African countries, especially in the MENA region.

This logic of conditionality is shaped through budgets structured around the external dimension of migration: the EU Emergency Trust Fund (EUTF) in 2015 and the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe) from 2021.

One important and sometimes overlooked element is how these funds are also contributing to build government authorities' capacity (especially that of law enforcement) by outsourcing surveillance tools, techniques and training to non-EU countries. Surveillance technologies are increasingly sophisticated and often surrounded by secrecy and opacity making it hard for external actors, and even more so for the people subjected to them, to understand the underlying risks and the long-term consequences of their use. Despite this, the EU is investing large sums of money in the outsourcing of surveillance, with the overt objective to tackling smuggling and human trafficking.

This chapter explores the use of some of the funding instruments that have been or could be used to implement these projects, focusing on countries in the MENA region.

While this paper has a specific focus on direct funding to non-EU countries, the European Union supports and finances the research, testing and implementation of surveillance technology for the purpose of (or repurposed as) border control in many ways.

Frontex, the European Border and Coast Guard Agency, has seen its budget skyrocketing from EUR 142 million in 2015 to a whopping EUR 754 million in 2022. In 2022, the agency announced the expansion of its footprint in third countries, including by opening risk analysis cells, tasked to collect and analyse data on cross-border crime and support authorities involved in border management, in the framework of the Africa-Frontex Intelligence Community (AFIC). It has also recently been announced that Frontex will spend hundreds of millions of euros on border surveillance and contracts for deportation flights in 2023, as well as EUR 3 million on storing weapons and ammunition, according to a plan approved by the agency's management board in mid-February.

[6] Horizon 2020 was the EU's research and innovation funding programme from 2014-2020 with a budget of nearly EUR 80 billion. It has been succeeded by Horizon Europe, the current EU's key funding programme with a budget of EUR 95.5 billion.

[7] This is not exclusive to EU- funded initiatives. Other immigration authorities and agencies, including the Swedish Migration Agency and the Dutch Immigration and Naturalisation Service, have explored forecasting tools to predict migration flows, processing times for different types of cases. The Danish Refugee Council (DRC) developed a tool together with IBM to predict forced displacement around the world, with funding from the Danish Ministry of Foreign Affairs.

It is important to remember that these policies are also implemented by Member States, with the support of tech and security companies. The heavy involvement of the private sector represents another big concern: companies are sometimes in charge of the deployment of the technology in these countries, effectively contributing to authoritarian practices of human rights violations, with little to no scrutiny.

In the past few years, civil society organisations and journalists have been investigating the intersection of private security, military, and tech companies in the implementation of border policies. In Italy, Action Aid launched The Big Wall, a project that aims to shed light on the resources used by Italy to support border externalisation policies, currently in partnership with the Investigative Reporting Project Italy (IRPI). In Spain, Fundaciòn Por Causa has been investigating the industry of migration control since 2020[6]. CEAR (Comisión espanola ayuda al refugiado, or the Spanish Commission for Refugees), a member of Euromed Rights, also coordinates a working group of Spanish organisations trying to monitor the use of AMIF and IBMF funds for border control especially in Ceuta and Melilla. This chapter explores the use of some of the funding instruments that have been or could be used to implement projects contributing to the outsourcing of surveillance tools, techniques and training to non-EU countries. The impact of such projects could be reflected in border externalisation policies as well as on the population of the country.

This chapter owes most of the resources to the work of Privacy International: since 2019, the London-based NGO has mapped the funds and documented some of the projects that were or are currently being implemented, as well as challenging its use with EU regulators.

The EU Trust Fund for Africa

The EU Emergency Trust Fund for Africa (EUTF for Africa) was launched by European and African partners at the Valletta Summit on Migration in November 2015.

Resources allocated to the EU Trust Fund for Africa amount to EUR 5.0 billion including EUR 4.4 billion from several funding instruments. EU Member States and other donors (Norway, Switzerland and the UK) have contributed around EUR 623 million. The Trust Fund was able to make financial commitments until 2021 but EUTF for Africa programmes will be implemented until the end of 2025.

The top three main priorities of EUTF for Africa for migration-related spending are:
1. Migration restriction and reduction
2. Promotion of rights and services
3. Border management

The EUTF has often been the subject of criticism. The European Court of Auditors reported in 2018 that "its objectives are too broad to efficiently steer action across the African regions, and the European Commission has encountered difficulties in measuring the extent to which the fund has achieved its objectives. The auditors also found weaknesses in its implementation".

In the following sections, we will look at the impact of some of the EUTF for Africa projects in countries in the MENA region. However, this type of project also affects countries in other parts of the continent, especially in the Sahel. Examples of projects include:

- EUR 11.5 million allocated to Niger for the provision of surveillance drones, surveillance cameras, surveillance software, a wiretapping centre, and an international mobile subscriber identity (IMSI) catcher, an intrusive piece of technology that can be used to locate and track mobile phones by simulating to be a mobile phone tower.[7]
- A EUR 28 million programme to develop a universal nationwide biometric ID system in Senegal by funding a central biometric identity database, the enrolment of citizens, and the interior ministry in charge of the system, implemented by the French and Belgian cooperation agencies. This is a programme that could have important implications for the control of emigration from Senegal in light of the new status agreement.

The Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI – GE)

The Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI – GE) is a new funding instrument that aims "to support countries most in need to overcome long-term developmental challenges and will contribute to achieving the international commitments and objectives that the Union has agreed to, in particular the 2030 Agenda and its Sustainable Development Goals and the Paris Agreement".

It merges several EU external financing instruments which existed as separate in the previous budget period (2014-2020), including those of relevance to asylum, migration and forced displacement: the Development and Cooperation Instrument (DCI), the European Neighbourhood Instrument (ENI), the European Instrument for Democracy and Human Rights (EIDHR), and the EU's Instrument contributing to Stability and Peace (IcSP), as well as the European Defence Fund (EDF).

Migration features prominently in the regulation establishing the NDICI–Global Europe.

The total allocation for NDICI – Global Europe of EUR 79.5 billion is divided as follows:
- EUR 60.38 billion for geographic programmes, including at least EUR 19.32 billion for the

[6] A full report in Spanish is available here: https://porcausa.org/industriacontrolmigratorio/

[7] An 'IMSI catcher' is "a device that locates and then tracks all mobile phones that are connected to a phone network in its vicinity, by 'catching' the unique IMSI number. It does this by pretending to be a mobile phone tower, tricking mobile phones nearby to connect to it, enabling it to then intercept the data from that phone to the cell tower without the phone user's knowledge." More here: https://privacyinternational.org/explainer/4492/how-imsi-catchers-can-be-used-protest

Neighbourhood. The remainder is allocated for Sub-Saharan Africa, Asia and the Pacific, and the Americas and the Caribbean.

- EUR 6.358 billion for thematic programmes (Human Rights and Democracy; Civil Society Organisations; Peace, Stability and Conflict Prevention; and Global Challenges).
- EUR 3.182 billion for a rapid response mechanism
- EUR 9.53 billion for a "cushion" of unallocated funds, to top up any of the above-mentioned programmes and the rapid response mechanism in case of unforeseen circumstances, new needs, emerging challenges or new priorities.

As this study is conducted early on in the current funding period, no comprehensive report on NDICI-Global Europe implementation, including analysis related to the spending targets, has yet been published. However, in the following section, we will provide examples of projects implemented under funding instruments that today form part of the NDICI-GE.

EU projects in the MENA region

The heavy allocation of funds from the EU migration budget mostly towards border management and the conditional approach to returns to the detriment of protection and integration programmes are big concerns in the way EU funding, including development aid, has been used in the MENA region (and in the African continent in general) in recent years.

The enhanced use of advanced technology in border security systems, poses renewed threats to human rights. Such systems push migrants to take more dangerous routes and contribute to the weaponization of migration that will endanger migrants' lives further. The consequences of the use of surveillance technology can be extreme – leading to abuse of fundamental rights both on people on the move and on local population, from the right to privacy and freedom of expression, to rights of association and assembly, religious belief, non-discrimination, and public participation, right to asylum and non-refoulement, to the loss of life.

In July 2022, it has been reported that the European Union has supplied the Moroccan authorities with spyware for extracting data from mobile phones for the official purpose of combating "irregular migration" and human trafficking. But in the absence of controls of the uses made of the software, it could also become a tool for the surveillance of journalists and rights activists.

Looking at the policing approach to border management and to the use of surveillance technology in EU countries, it is not surprising that many EU-funded projects in the MENA region see the involvement of the European Union Agency for Law Enforcement Training (CEPOL). The EU agency is responsible for developing, implementing, and coordinating training for law enforcement officials from across EU and non-EU countries, and has seen its budget rocket from EUR 5 million in 2006 to over EUR 9.3 million in 2019. Training offered includes courses on law enforcement techniques (including those involving surveillance), cybercrime and counterterrorism. However, as the following examples will show, their support to counterparts in non-EU countries does not come with an assessment of the legality of the use of those techniques, some of which lack safeguards in EU countries themselves, nor on whether they are used in criminal investigations or to crackdown on migrants or political opposition.

These elements can further contribute to an unstable political environment that can destabilise the region.

Algeria

Algeria is included in projects funded under the European Neighbourhood Policy and a small number of regional projects funded by the EUTF; some of them are in the field of migration, including the project called "Dismantling the criminal networks operating in North Africa and involved in migrant smuggling and human trafficking" that allocated EUR 15 million to law enforcement agencies in Algeria, Egypt, Libya and Tunisia (see more in the section on Egypt).

Privacy International investigated the role of CEPOL, the EU law enforcement training agency, in facilitating training in open-source intelligence gathering to several third-country authorities, including Algeria. These trainings were funded under the Instrument contributing to Stability and Peace (IcSP). With a budget of EUR 2.3 billion for 2014 – 2020, IcSP was the EU's main financing instrument supporting security initiatives and peace-building activities in partner countries (as of 2023, it has been merged into NDICI.)

According to Privacy International analysis, in April 2019, CEPOL organised a training session for members of Algeria's National Gendarmerie, a police force. The training describes the use of specialised surveillance tools available to law enforcement agencies, including software used to track the location of devices, as well as open source tools: "Participants are advised to use "sock puppets" for open-source research – anonymous and fake profiles used to gather intelligence that are harder to trace. To avoid detection, the officers are directed to purchase different sim cards for different accounts, use picture editing tools, and to remember to post frequently and outside of work hours. Participants are also recommended online platforms to make it easier to manage numerous fake accounts at the same time. Such tactics are not only contrary to terms of use policies implemented by social media platforms, but they also explicitly contradict the EU's own policies on disinformation."

It is unclear whether these tools and techniques have been used to curb migration flows, or on local groups or populations, and how. Privacy International's report, however, highlights a potential connection with the 2019 protests in Algeria: "At the same time as CEPOL was advising participants how to thwart these restrictions, in Algeria's capital in April 2019, a huge protest movement known as the Revolution of Smiles was taking place, culminating in the resignation of President Abdelaziz Bouteflika after 20 years in power. What followed was a wave of online disinformation and censorship, driven by networks of pro-regime fake accounts posting propaganda and reporting high-profile democracy activists. Known as 'electronic flies', there is no indication that any of these troll networks were organised by anyone who attended the training – but nevertheless the promotion by the EU of techniques used to silence pro-democracy voices in a key neighbour [country] must ring alarm bells."

Social Media Intelligence (SOCMINT) and Open Source Intelligence (OSINT)

Social media intelligence (SOCMINT) refers to the collective tools and solutions that allow people and organisations to collect and analyse conversations, social data points etc gathered from social media sites, using both intrusive or non-intrusive means, from open and closed social networks. This can happen both with or without the platform's permission.

This type of information gathering is one element of OSINT (Open-Source Intelligence). The Berkeley Protocol on Digital Open Source Investigations defines OSINT as "a subcategory of open source information that is collected and used for the specific purpose of aiding policymaking and decision-making, most often in a military or political context. [...] Open source information encompasses publicly available information that any member of the public can observe, purchase or request without requiring special legal status or unauthorised access." Examples of such information include public flight data and satellite imagery, but also records concerning an organisation's finances or directors.

These techniques are today widely used by many actors for different purposes. They include researchers, journalists and law enforcement, as investigation tools, including for violations of human rights and war crimes. However, they have also been misused and abused by police forces to monitor specific communities, with a chilling effect on freedom of expression.

Egypt

The EUTF for Africa funded a project called "Dismantling the criminal networks operating in North Africa and involved in migrant smuggling and human trafficking" that allocated EUR 15 million to law enforcement agencies in Egypt, as well as to Algeria, Libya and Tunisia to build identification and investigation capacities. Activities included establishing a group of 'cyber specialists', 'criminal analysts', and 'forensic specialists' capable of conducting online investigations and collecting evidence from digital devices, and training them.

The United Nations Office on Drugs and Crime (UNODC) delivered capacity building training and provided light equipment, such as IT and forensic tools to actors dealing with law enforcement and criminal justice, with regards to "special investigation techniques, such as criminal intelligence analysis, crime scene investigation and evidence management, and the use of digital forensic evidence during the investigation and prosecution of organised crime groups".

Under the Development Cooperation Instrument (DCI), the main financial instrument in the EU budget for funding aid to developing countries in 2014-2020, Egypt was one of the beneficiary countries (with Djibouti, Eritrea, Ethiopia, Kenya, Somalia, Sudan, South Sudan) of EUR 6 million allocated to "address mixed migration flows", by establishing reception centres, and increasing capacity to tackle smuggling groups, implemented by Expertise France. Training to 28 law enforcement and judicial officials from the beneficiary countries was delivered by the Italian Carabinieri Corps, the French Gendarmerie Nationale and the French National Police.

Libya

In 2017, more than EUR 42 million was allocated from the Trust Fund for Africa for a border control project called "Support to Integrated border and migration management in Libya", which included the provision of patrol boats, SUV vehicles workstations, radio-satellite communication devices, and other equipment to authorities in Libya. The programme was led by the Italian government and included the training and equipping of Libyan authorities in ways that raise human rights concerns around, for instance, the misuse of data and possible privacy infringements of third country populations in a vulnerable position.

According to a document obtained by Privacy International, in 2018 FRONTEX provided a training to Libya's General Administration for Coastal Security (GACS) which included secure "evidence for prosecution and intelligence purposes", including from electronic devices, how to acquire fingerprints, including from "children and people with vulnerabilities", as well as "basic self-defence techniques that can be used during the apprehension of suspects on board, including the use of force and its limitations". The project had a second phase allocating EUR 16.8 million.

The IcSP fund also provided EUR 4 million for the "Provision of geospatial intelligence to the UN Stabilisation Mission in Libya".

Morocco

A privileged partner of the EU in migration control cooperation since the early 90s, Morocco has been getting funding disproportionately focused on border management: for example, of the total EUR 238 million drawn from the EU Emergency Trust Fund for Africa in Morocco, 190 million are allocated for border control-related projects, while only 28.3 million for programmes related to protection and rights.

Under the EU Trust Fund for Africa, the Border Management Programme for the Maghreb region allocated EUR 55 million to Tunisia's and Morocco's Interior ministries for the "purchase and maintenance of priority equipment, capacity building and development of necessary standards and procedures at national level". In Morocco, it developed an IT infrastructure collecting, archiving and identifying digital biometrics; it also provided aerial surveillance equipment, as well as vehicles and communication equipment for different field units.

Before that, Moroccan law enforcement also benefited from training provided by CEPOL, the European Union Agency for Law Enforcement Training. Funded by the IcSP, activities included EUR 6.4 million provided to CEPOL to train authorities in Algeria, Jordan, Lebanon, Morocco, Tunisia, and Turkey in counterterrorism.

Documents on trainings to Morocco's security forces as recipients show that mobile phone extraction tools and social media intelligence techniques are among the topics of the training. These are extremely intrusive tools and techniques whose use by police forces is highly regulated in European countries and subject to judicial oversight.

This extract in particular refers to a training provided to Morocco's Directorate General for National Security (DGNS): "Participants are advised to use open-source websites designed to access information from Facebook, including Stalkscan, WhoPostedWhat, PeopleFindThor, and Facebook Matrix, as well as social network analysis tools used to visualise relationships. In a module on how to analyse Twitter in real time, participants are advised to use open-source tools designed for scraping tweets from the platform".[6]

Morocco also benefited from EUR 3 million provided to train and develop investigative capabilities in the Maghreb. One such activity, implemented by the Terrorism Prevention Branch of the United Nations Office on Drugs and Crime, included training police in Morocco on "wiretapping/telephone tapping and videotaping" and "special investigation techniques on the Internet/Electronic surveillance (anonymous browsing for investigation purposes, interception of data and mails, decryption of encoded data, etc.)".

Tunisia

The aforementioned project by the Border Management Programme for the Maghreb region, which allocated EUR 55 million to Tunisia's and Morocco's Interior ministries, included the provision of and training in 'state of the art technology', as well the establishment of a screening system to allow border agencies to collect data at border crossing points, to be further analysed at the central level, and conduct risk analyses for travellers.

The assessment of risk factors and threshold for investigations on people and organisations are of concern. In their (successful) complaint to the European Ombudsman, a coalition of human rights NGOs note that "trainings provided by CEPOL on financial investigations given in Tunisia provide a concerning insight into how CEPOL raises awareness about the risk of charities raising funds for terrorism, and how in doing so it risks promoting suspicion and regulatory actions designed to undermine the freedom of civil society. [...] Topics covered include techniques for investigating informal banking systems such as hawala banks (a transfer system popular across North Africa, the Middle East, and the Indian subcontinent), analysing accounting records, and understanding the use of businesses by financiers of terrorism."

Between 2016 and 2018, the Instrument contributing to Stability and Peace (IcSP) also funded a EUR 1 million euro project aimed at developing the capacity of Tunisian security agencies to counter terrorism by developing "intelligence processing and analysis", "providing training in digital intelligence gathering including through social media and digital mapping", and "developing inter-service cooperation among Tunisian security agencies". The implementing partner was Civipol, a well-connected French company owned partially by some of the largest armed companies in the world.

[6] Scraping is "the process of extracting data from a digital source for automated replication, formatting, or manipulation by a computer program." In this case, it refers to the use of tools to gather public data from the social media platform automatically.

CONCLUSIONS

Human rights standards, transparency and accountability should be at the heart of cooperation with third countries. Currently, instead, the EU is proactively seeking agreements with non-EU countries either to stop people from arriving at the EU's border or to take back their nationals. The fixation with this securitarian logic against migration, which leads to an ever increasing focus on the externalisation of border control, has enormous consequences for people on the move, restricting their freedom of movement, access to asylum and access to safe and legal pathways for migration. Migrants and refugees are used as "pawns" in a game of political pressure and negotiations for economic and geopolitical benefits with the EU and Member States.

This paper has shown how nowadays, border externalisation takes many shapes, one of them being the outsourcing of surveillance technologies to third countries, which is emerging as an increasingly central element in the external dimension of migration control. These tech and data intensive systems are used to enforce control on migrant populations — with the ultimate objective to prevent departures. However, migrants and refugees are not the only people affected: while many of the EU-funded projects we have mentioned purportedly tackle smuggling and trafficking networks, the outsourcing of surveillance technologies is clearly providing new tools and tactics to authoritarian governments who use it to repress dissent and opposition, with the effect of further contributing to instability in the region.

The EU and Member States should not use invasive techniques for migration control, nor outsource the tools to do it to non-EU countries. Rather, they must comply with their international and EU legal obligations. In order to reverse this trend, it must therefore be ensured that any agreement with third countries prioritises compliance with international human rights obligations, and lives up to standards of democratic accountability and transparency.

BIBLIOGRAPHY

- Akkerman M., "Expanding the fortress The policies, the profiteers and the people shaped by EU's border externalisation programme", Transnational Institute, 11 May 2018
- ASGI, Un laboratorio di esternalizzazione tra frontiere di terra e di mare Una prospettiva da Senegal e Mauritania, May 2022
- Bagnoli L., Papetti F. "How Italy built Libya's maritime forces", IrpiMedia, 22 December 2022
- Campbell Z., D'Agostino L., "How an EU-funded agency is working to keep migrants from reaching Europe", Coda Story, 31 May 2023
- Campbell Z., D'Agostino L., "How the EU supplied Morocco with phone-hacking spyware", Disclose, 25 July 2022
- EDRi, "Artificial Intelligence Act Amendments Prohibit predictive policing and profiling AI systems in law enforcement and criminal justice", May 2022
- EuromedRights, "Call on the EU: Restore rights and values at Europe's borders", 26 November 2021
- EuromedRights, "Stop bargaining on the back of migrants", 30 January 2021
- Gallagher R., Jona L., "We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive", The Intercept, 26 July 2019
- Jones C., Kilpatrick J., Maccanico Y., "At what cost? Funding the EU's security, defence, and border policies, 2021–2027. A guide for civil society on how EU budgets work", Statewatch, April 2022
- Lopez Curzi C., "The externalisation of European borders: steps and consequences of a dangerous process", Open Migration, 12 July 2016
- Migration Control Info, Border and Surveillance Technology & Industry
- Ozkul, D."Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe", 2023
- Privacy International, "Complaint on EU surveillance transfers to third countries", 21 October 2019
- Privacy International, "Revealed: The EU Training Regime Teaching Neighbours How to Spy", 10 November 2020
- Privacy International, "Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes", 10 November 2020
- Privacy International, "The EU Funds Surveillance Around the World: Here's What Must be Done About it", 18 September 2019
- United Nations Human Rights, Office of the High Commissioner (published jointly with the Human Rights Center at the University of California, Berkeley, School of Law), Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law, 3 January 2022
- Woollard C., Liebl J., Davis L., Casajuana E. , "EU migration and asylum funds for third countries", European Parliament, December 2022

ACKNOWLEDGMENTS

European Artificial Intelligence & Society Fund

EuroMed Rights would like to thank the European Artificial Intelligence & Society Fund whose support enabled this research.

The sole responsibility for the content lies with the author(s) and the content may not necessarily reflect the positions of NEF, or the Partner Foundations.

DROITS EUROMED RIGHTS

Vestergade 16, 2nd floor DK-1456
Copenhagen K Denmark

tel +45 32 64 17 00
mail information@euromedrights.net