DROITS EUROMED RIGHTS

statewatch

EUROPE'S TECHNO BORDERS

JULY 2023

JULY 2023

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

EuroMed Rights is a network representing 68 human rights organisations, institutions and individuals based in 30 countries in the Euro-Mediterranean region.

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

Statewatch
c/o MayDay Rooms, 88 Fleet Street, London EC4Y 1DH
UK

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards.

Tel: (+44) (0) 203 393 8366
statewatch.org/about/mailing-list
www.statewatch.org

Bibliographic Information

Title: Europe's techno borders
Authors: Chris Jones, Romain Lanneau, Yasha Maccanico
Additional research: Alice Troy-Donovan
Date of initial publication: July 2023
Pages: 45
Original Language: English

ACRONYMS

AMF	Asylum and Migration Fund
AMIF	Asylum, Migration and Integration Fund
API	Advanced Passenger Information
Biometric Data	Data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images or dactyloscopic (fingerprint) data.
BMVI	Border Management and Visa Instrument
CIR	Common Identity Repository
CRRS	Central Repository for Reporting and Statistics
ECRIS-TCN	European Criminal Records Information System for Third-Country Nationals
EES	Entry/Exit System
ETIAS	European Travel Information and Authorisation System
eu-LISA	European Agency for the operational management of large-scale IT Systems in the area of freedom, security and justice
Eurodac	European Dactyloscopy
Europol	European Union Agency for Law Enforcement Cooperation
Frontex	European Border and Coast Guard Agency
IBMF	Integrated Border Management Fund
IPA	Instrument for Pre-Accession Assistance
ISF	Internal Security Fund
NDICI	Neighbourhood, Development and International Cooperation Instrument
Personal Data	Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.
PNR	Passenger Name Record
Predictive/Profiling System	An algorithmic system used to make predictions about an individual or group of people, for example their likelihood of engaging in irregular immigration.
Presentation attack	An "attack" against a biometric system in which means are used that allow an individual to present themselves as somebody else, such as fake silicone fingerprints or a face mask.
Presentation attack detection	The use of hardware and software to detect a presentation attack, e.g. by making it possible to detect when fingerprints are made of silicone.
RAC	Risk Analysis Cell
RCMS	Readmission Case Management System
SIS	Schengen Information System
VIS	Visa Information System

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The use of new technologies is fundamental to the EU's system of border control and migration management. This report explores their development and deployment over the last three decades, during which time an extensive infrastructure of surveillance systems, databases, biometric identification techniques and information networks has been put in place to provide state authorities with knowledge of – and thus control over – foreign nationals seeking to enter EU or staying in Schengen territory. Digital technologies underpin invasions of privacy, brutal violations of human rights, and make the border 'mobile', for example through the increased use of mobile biometric identification technologies, such as handheld fingerprint scanners used by police and border authorities.

On the one hand, new technologies are deployed to facilitate the movements of "bona fide" travellers. In the years to come, tourists and businesspeople will be required to hand over increasing amounts of personal information to EU and member state authorities in exchange for being granted entry to the EU. That information will then be used to train algorithms that will be applied to new applications to enter the bloc, in order to assess the level of risk or threat posed by individuals (and, where that level is deemed too high, to deny them the ability to travel to the EU).

On the other hand, new technologies are deployed to detect, deter and repel refugees and migrants seeking to enter EU territory through irregular journeys. Drones, cameras, social media monitoring, satellite imagery and networks of sensors form part of an elaborate surveillance architecture that is being continually extended. Those who do manage to enter EU territory – which is to say, if they are not illegally pushed back by EU authorities, or prevented from leaving a "third country" – are also biometrically registered and screened against a multitude of national and international databases. If they are deported, international data-sharing systems are increasingly being used to facilitate that task.

These techno-borders are backed up by vast quantities of public funding – both for the development of new technologies, and then their subsequent deployment. EU budgets run in seven-year cycles – currently, from 2021 to 2027. Compared to the previous budgetary period (2014-20), the total size of the budgets that will contribute to EU border policies has increased by 94% - although not the entirety of each of those budgets will be used for those purposes. Nevertheless, billions of euros are set to be spent on extending and entrenching Europe's techno-borders in the years to come.

Figures provided in this report give some indications of which borders are likely to be more substantially reinforced. From 2014 to 2020, the Greek authorities received almost €977 million from the EU's home affairs funds, dealing with policing; borders; and asylum and integration. In the 2021-27 period, that amount has been increased to just over €1.5 billion. The funding directed specifically towards borders has skyrocketed from almost €303 million to more than €1 billion – an increase of 248%.

This is not the only vast increase. France is to receive almost 200% more from the borders budget than it did in the 2014-20, obtaining nearly €207 million; Croatia will receive almost 100% more, obtaining €155 million; and Spain's share will increase by 34%, to some €325 million. Other Mediterranean member states, however, have seen substantial decreases in border funding: Malta will receive 45% less than in the 2014-20 period; Cyprus 40% less; and Italy's share of the borders budget has increased by just 1%, to €315 million. Nevertheless, combined with the budgets for policing and asylum, every Mediterranean member state is to receive more between 2021 and 2027 than in the previous budgetary period.

While these funds can be used to extend surveillance systems, set up connections to the EU's vast biometric databases, and purchase new equipment and gadgets for border authorities, public funding is also used to develop new border technologies. Through its security research programme, the EU has invested in automated lie detectors to be deployed at border crossing points, the development of automated border control gates, systems using "big data" to try to predict migration movements, and swarms of drones for border surveillance.

This report shows that between 2014 and 2022, the EU has provided more than €250 million to 49 projects seeking to develop border technologies. Think tanks and research institutes feature prominently amongst the top 20 entities that have benefited from that funding. Indeed, the Greek Center for Security Studies (€12.8 million), France's Commissariat à l'énergie atomique et aux énergies alternatives (€8.4 million), TNO from the Netherlands (€4.5 million), Germany's Fraunhofer Institute (€4.4 million) and the Centre for Research and Technology Hellas (€4.3 million) make up the top five. They are joined by a range of private companies, two universities, and even the NATO Science and Technology Organisation.

The use of, and demand for, new technologies for border and migration control is likely to increase substantially in the coming years, as demonstrated by the final two sections of this report. The first looks at upcoming legislation that will play a role in reinforcing Europe's techno-borders: the Eurodac Regulation, the Screening Regulation, changes to the Schengen Borders Code, and the Artificial Intelligence Act. These four measures are all currently under debate in the Council of the EU and the European Parliament, and have substantial implications for the rights of migrants and refugees. Those implications may also extend to non-white EU citizens and residents: the changes to the Schengen Borders Code, for example, look likely to encourage profiling operations within EU territory in the name of tracking down irregular migrants.

The final section of the report combs through a series of reports and studies commissioned by the European Commission, Frontex and the EU's Joint Research Centre in recent years. These have covered the potential uses of artificial intelligence, surveillance technologies and biometrics for border and migration control purposes.

None of them proposes any substantial change in EU policies in these areas. Rather, they set out ways to refine, optimise and intensify the use of existing systems – for example, through the use of new types of biometric identification systems, the further extension of border surveillance systems, and the integration of automated systems into all manner of procedures and processes. Many of the changes proposed do not require specific changes to legislation, and instead are presented as technical issues that merely require the right mixture of funding and management to be implemented effectively. In this manner, they may well escape any substantial public and political scrutiny.

There has of course been significant scrutiny of the EU's migration policies ever since the signing of the Maastricht Treaty in 1992, and even more so from 2015 onwards. While the question of new technologies has never been absent from the conversation, it often plays something of a background role.

However, the use of new technologies for migration and border control – the development of techno-borders – not only presents substantial challenges for the protection of human rights in and of itself. It also creates certain 'path dependencies' that have substantial influence over future developments, as demonstrated by the proposals outlined in the last section of this report for ever more invasive and intrusive forms of biometric identification. The development of techno-borders is also a source of substantial potential profits for private companies, who themselves have a vested interest in the wider deployment of surveillance, identification and information systems. The development of techno-borders, the influence they have on future policy developments, and the industry lobby that surrounds them, requires continuous, close and critical investigation as part of the broader struggle to implement humane migration and asylum policies.

TIMELINE: DEVELOPING TECHNO-BORDERS

The use of new technologies in the field of migration and asylum is intimately linked to efforts to enhance state control over people, particularly those who are not EU citizens. The development and purchase of those technologies has aided the expansion of the EU security, technological and surveillance industrial complex, with public funds flowing towards companies offering solutions to tackle present challenges and prospective threats, whether real or imagined. These processes have been further propelled by the creation and gradual reinforcement of Frontex, which has a growing role in conducting and contracting research studies and projects on border controls and surveillance; and the recurrent use of "crisis" and risk narratives to justify the use of exceptional measures.

While the EU has sought to incorporate advanced technologies into its border infrastructure from the 1990s onwards, the advent of the "war on terror" in 2001 provided a convenient justification for the acceleration of new digital identity and surveillance schemes. Under the guise of making the fields of asylum and migration "terrorism-proof", mistrust and suspicion of migrants and refugees was promoted in political and media discourse and underpinned a drive to accumulate personal data and justify practices of exclusion. In this respect, it is noteworthy that the repeated expansion of large-scale EU databases has consistently involved the introduction of legal provisions allowing their use for deportation purposes, as part of the ongoing drive to increase the EU's "return rate".

The use of new technologies is now firmly cemented in the EU's border policies, with a recent European Commission paper on the European Integrated Border Management strategy reaffirming "use of state-of-the-art technology including large-scale information systems" as a political priority. This is the most recent of many such policies and projects, which are recounted here under three different headings: large-scale biometric databases; biometric identity documents; and surveillance and data infrastructure.

LARGE SCALE BIOMETRIC DATABASES

2000

Biometric registration of asylum-seekers

- Establishment of the Eurodac database to store asylum-seekers' fingerprints
- Intended to aid in determining the state responsible for processing an asylum application
- 2013, legislation updated to grant law enforcement access to the database
- 2015, European Commission "non-paper" calls for 100% fingerprinting rate, arguing "no registration no rights"
- 2016, legislation proposed to make Eurodac a general purpose "migration management" database, including facial images, biographic data and inclusion of more groups of people

2011

EU biometric visa database comes into use

- Visa Information System (VIS), in development since mid-2000s, deployed in first region
- Full global deployment completed by the end of 2015
- 2021, new legislation approved that expands uses of VIS to aid in identifying individuals subject to deportation orders, lowers minimum age for data collection from 12 to six, and introduces an automated profiling function[1]

2013

Fingerprints and photographs in the Schengen Information System

- The SIS law enforcement database was originally launched in 1995 but has been upgraded a number of times
- In 2013 fingerprints and photographs were included for the first time, and 2018 legal changes allow the inclusion of palm prints and DNA for certain types of alerts
- 2018 legal changes also introduced alerts on deportation orders, with the aim of ensuring their mutual recognition between member states
- As of 2022, 1% of alerts were on individuals, though that equates to just over one million alerts, 56% of which were for refusal of entry or stay in the Schengen area

2017

Biometric border-crossing database legislation

- The Entry/Exit System (EES) will be used to monitor the cross-border movements of temporary visitors to the Schengen area and to automatically calculate the amount of time they are permitted to stay
- It will replace the manual stamping of passports with individual files in a centralised database (containing biographic and biometric data) that will automatically identify individuals who stay longer within the Schengen area than permitted
- The system will also be used to facilitate the automation of border controls, through the storage of biometric data and the use of 'e-gates' at border crossings
- It is currently under construction, though its entry into use has been delayed multiple times

2018

Approval of "travel authorisation" system

- The European Travel Information and Authorization System (ETIAS) will require non-EU citizens who do not require a visa to travel to the Schengen area to pay for a "travel authorisation", much like systems operated by the USA, Australia and Canada
- Individuals will have to submit biographic data to the authorities for automated checks against EU and international databases and automated profiling to determine whether they pose an irregular immigration, security or health "risk", the same form of checking and profiling being applied to the VIS
- In practice, a decision made by a border guard on a person flagged in a database is semi-automatic, and the review of those decisions – or lack thereof – seriously undermines individual rights
- The system has been repeatedly delayed but is currently expected to come into use in 2024

2018

Legislation interconnecting all EU migration and policing databases

- "Interoperability" architecture will take "identity data" (biometrics, names, nationality, date of birth and more) from five large-scale EU databases[2] and place it in a new Common Identity Repository to be used for identity checks and criminal investigations
- Aim is to make data on non-EU nationals more easily accessible to a greater number of authorities, including through the use of mobile biometric identification devices (fingerprint or face scanners)
- Statistics generated through the interoperability architecture will also be used for Frontex's risk analysis work, reinforcing its role in policy-making and operational planning

BIOMETRIC IDENTITY DOCUMENTS

2004

Biometric passport for EU citizens

- Introduced in response to post-9/11 European Council demands
- All EU or Schengen state passports (excluding Denmark, Ireland and UK) to store two fingerprints and a photograph in the chip on the passport
- 2005, International Civil Aviation Organisation (ICAO, a UN agency) adopted standards to encourage the global introduction of biometric passports

2008

Biometric residence permits

- Inclusion of two fingerprints and a facial image in EU residence permits for foreign nationals becomes mandatory

2019

Biometric identity card legislation

- It is now a legal obligation for all national identity cards issued by member states to contain fingerprints and a facial image
- The measures were presented as a way to improve peoples' ability to exercise their right to free movement within the EU but are also intended to make it more difficult to falsely acquire or forge identity cards
- German NGO Digitalcourage is seeking to have the law overturned, calling it "a disproportionate infringement on our civil rights. It treats every EU citizen like a potential criminal and [endangers] the security of our biometric data."

SURVEILLANCE AND DATA INFRASTRUCTURE

2004

Advance Passenger Information rules

- Under the Advance Passenger Information (API) Directive, air carriers must transmit the information held in passengers' passports to the border authorities of EU member states for "pre-checks" against immigration databases
- New rules currently under negotiation will further automate the data transmission process and make both immigration and policing "pre-checks" mandatory
- Discussions are ongoing on whether to extend the scheme to other forms of transport, namely rail, ferry and coach/bus journeys

2008 onwards

EU biometric visa database comes into use

- The European Border Surveillance System (EUROSUR) takes a quasi-military approach to migration control and interconnects national and EU surveillance assets including drones, cameras, sensors and other types of data-gathering technologies, with National Coordination Centres (NCCs) connected to a central hub operated by Frontex
- The system goes further than mere border surveillance, also encompassing "pre-frontier situational awareness"
- The technological backbone of EUROSUR was developed long before any legislation was proposed (a law was approved in 2012), and development was aided by EU-funded research and development projects, which continue to pursue new technologies for the system such as autonomous "drone swarms" and other surveillance devices

2013 onwards

Readmission Case Management Systems

- RCMSs enable direct communication between deporting states and destination states, facilitating "the exchange of information necessary for identity verification which includes returnee personal data, identity documents, biometric data, as well as exchange of information relevant for transfer, such as flight details"
- An individual's case can be processed through an RCMS after a deportation order has been handed down against them
- The EU has outsourced the work of developing RCMSs in target states to the International Organisation for Migration
- Armenia, Azerbaijan, Bangladesh, Georgia, Pakistan, Sri Lanka and Ukraine all currently have such systems, the possibility of setting up such a system in Ivory Coast has been explored by EU officials, and a biometric population database being set up in Senegal and financed by the EU is considered by EU officials to be useful for setting up an RCMS

2014

Passenger Name Record Directive

- Passenger Name Record (PNR) data is generated during the booking or buying of an air or other travel ticket and can contain significant amounts of personal data, including full name, addresses, phone numbers and email addresses, travel itinerary, and more
- Like API, it is used to perform "pre-checks" against airline passengers travelling to or within the EU, though only for policing (and not immigration) purposes
- Court of Justice of the European Union (CJEU) jurisprudence has restricted the transmission of data from airlines to law enforcement authorities in relation to intra-EU flights
- PNR and API plans are being pursued at a global level, in line with obligations that have been set out in UN Security Council resolutions

2014 onwards

Testing of automated "lie detectors" for borders begins

- AVATAR system deployed for testing at Bucharest airport "conducts brief interviews with travellers… monitoring respondents' body language and verbal replies to identify irregular behavior that warrants further investigation."
- Edgar Beugels, Frontex's Head of Research and Development, said "I guess passengers have to get used to talking to a machine… In the future, it could be considered to integrate AVATAR into the normal border control process."
- In 2016, the €4.5 million, EU-funded iBorderCtrl research project began, aiming to use advanced technologies to examine and judge examine travellers' "micro gestures" and "facial expressions, gaze and posture"
- The iBorderCtrl project ran its course and has not so far been deployed beyond the testing stage, but the substantial investment made in the technology suggests that it will not go away

2015 onwards

Frontex transmitting personal data to Europol

- In summer 2022, Balkan Insight published an investigation on Frontex and Europol's "Personal Data for Risk Analysis" (PeDRA) project, that seeks to use data collected by Frontex from "debriefing" interviews with migrants to feed Europol's databases and Frontex risk analyses
- Frontex sought to gather genetic data and data on sexual orientation, and on criminal suspects as well as victims and witnesses
- Data was to be harvested via "debriefing" interviews conducted at the EU's borders, where "there is no paper trail, no records of Frontex referrals to national authorities, no privacy and no lawyer is present"
- The project was subsequently put on hold pending a review, but the wide scope of data-gathering by Frontex has been made evident by subsequent press reports: "NGOs (non-governmental organisations) appear in 1,058 documents held by EU border force Frontex as part of its anti-smuggling operation with Europol, the EU's police agency"
- The transmission of data to Europol by Frontex adds a new layer to the border data landscape, in which national authorities also gather vast quantities of data that can be shared amongst each other and with EU agencies

2017 onwards

Frontex transmitting personal data to Europol

- The EUAA, when it was still known as the European Asylum Support Office (EASO), fed an algorithm with information from countries of origin and transit, data scraped from social media, real-time information on arrivals at the EU's external borders, and data on previous outcomes of asylum applications in the EU
- It sought to predict likely numbers of asylum applications a month in advance and medium-term scenarios, but the European Data Protection Supervisor (EDPS) halted the project for breaching privacy rights
- There is still clear interest in the idea, however: a 2022 academic paper on the same topic lists an EASO staff member as co-author; the EU research projects MIRROR and PERCEPTIONS are working with similar technologies; and Frontex has demonstrated to MEP delegations how it monitors social media "in order to be aware of groups of persons organising in order to move towards the EU external borders," while its 2022-24 work programme refers to "media monitoring and reporting including open-source intelligence (OSINT)"

2018 onwards

Development of Risk analysis Cells

- Frontex has overseen the creation of eight Risk Analysis Cells (RACs) in states that are part of the Africa-Frontex Intelligence Community (AFIC)[3]
- The aim of RACs is "to collect and analyse data on cross-border crime and support authorities involved in border management. This includes information on illegal border crossings, document fraud, trafficking in human beings and other types of cross-border crime"
- It is likely that in the future RACs will be connected to Eurosur: In the working arrangement between Frontex and the EUCAP Sahel Niger mission, analytical reports generated by the Risk Analysis Cell in Niamey are mentioned in the same breath as "the European situational picture," an element of Eurosur

FOLLOWING THE MONEY

A study carried out for the European Commission in 2022 found that more than €7.7 billion was spent on "the management of European borders" between 2015 and 2020, and "the biggest parts of this budget come from European funding" – that is, the EU's own budget is the biggest driver of border reinforcement and militarisation in the EU.

This looks set to continue in the current budgetary period (2021-27). EU military and security budgets have been increased from a total of €19.7 billion in 2014-20 period to €43.9 billion in the 2021-27 period, a rise of 123%. Within that, funds specifically for the purpose of borders and policing have almost all increased substantially, as shown in the table below. Aid and development funding has also now been co-opted for migration control purposes, with 10% of the €79.5 billion aid budget supposed to contribute to migration management objectives, and the EU's enlargement funds will continue to provide money to the Western Balkans and Turkey. The total size of the budgets that will contribute to EU border policies has increased by 94%, although not the entirety of each of those budgets will be used for those purposes. Nevertheless, substantial quantities will be made available for border control and "migration management" purposes, along with fresh funding for the development of new border surveillance and control technologies.

Tracking EU spending has proven a vital way for civil society organisations to investigate and challenge developments that threaten human rights. The European Commission's funding and tenders database includes information on many of the projects funded under the budgets listed below, with the exception of the Trust Fund for Africa. However, the database only concerns the portions of the budgets that are controlled directly by the Commission – in most cases, the majority of the funds are disbursed to member states to be spent in accordance with national work programmes. Information on these projects is not always publicly available, and gaining access to it may require filing freedom of information requests.

Open Security Data Europe contains data on a substantial number of those projects for the 2014-20 period, and includes some information from 2021 onwards. The CORDIS database contains information on all EU-funded research projects (such as those funded by the Civil Security for Society budget). Data on research projects can also be found on the EU's Open Data Portal, allowing more detailed investigation into and comparison of the entities receiving funds and the types of projects funded.

2014-2020		**% change**	**2021-2027**	
Budget			**Budget**	
Internal Security Fund - Police	EUR 1bn	+ 90%	EUR 1.9bn	Internal Security Fund
Internal Security Fund – Borders and Visa	EUR 2.7bn	+ 131%	EUR 6.2bn	Integrated Border Management Fund – Borders and Visa
Asylum, Migration and Integration Fund	EUR 6.9bn	+ 43%	EUR 9.9bn	Asylum and Migration Fund
Security research programme ('Secure societies')	EUR 1.7bn	- 9%	EUR 1.6bn	Civil Security for Society
Development Cooperation Instrument	EUR 19.7bn	+ 21%	EUR 79.5bn	Neighbourhood, Development and International Cooperation Instrument
European Development Fund (outside of EU budget)	EUR 30.5bn			
European Fund for Sustainable Development (outside of EU budget)	EUR 350m			
European Neighbourhood Instrument	EUR 15.4bn			
Instrument for Pre-Accession Assistance II	EUR 10.7bn	+ 32.7%	EUR 14.2bn	Instrument for Pre-Accession Assistance III
Total	**EUR 58.5bn**	**+ 94%**	**EUR 113.3bn**	**Total**

Integrated Border Management Fund: Border Management and Visa Instrument (BMVI)

Budget: €5.2 billion

The BMVI aims "to ensure strong and effective European integrated border management at the external borders… while safeguarding the free movement of persons within it and fully respecting the relevant Union acquis and the international obligations of the Union and Member State." It will also fund actions intended to reinforce the EU's common visa policy.

The activities that can be financed through the BMVI include the development and use of large-scale IT systems, the reinforcement of border checks and surveillance, "technical and operational reinforcement" at borders and in "hotspots", and purchasing equipment for Frontex. It can also be used to aid the border externalization agenda by funding activities in third countries, for example through the deployment of immigration liaison officers to gather information and intelligence.

It is the successor the Internal Security Fund – Borders (ISF-Borders), which ran from 2014-20.

Internal Security Fund (ISF)

Budget: €1.9 billion

The ISF is intended to reinforce the powers of the police and other law enforcement actors, and thus its primary focus is not on border or immigration control. Nevertheless, the €579 million "thematic facility", a portion of the ISF that is distributed by the European Commission, can be used "for supporting actions in or in relation to third countries," including "combating cross-border criminal smuggling networks." This may bolster the work of the "operational partnerships" that the EU has been establishing in recent years with non-EU states, which in some cases has explicitly involved the purchase of new technologies for police forces: a project in Niger involves the use of "wiretapping equipment and digital GPS maps," as well as "identification and biometric tracking of people linked to criminal networks of irregular immigration and human trafficking."

It is the successor the Internal Security Fund – Police (ISF-Police), which ran from 2014-20.

Asylum and Migration Fund (AMF)

Budget: €9.9 billion

The AMF aims "to contribute to the efficient management of migration flows and to the implementation, strengthening and development of the common policy on asylum and the common policy on immigration." The extent to which it may be used to fund the purchase of new technologies for asylum and migration purposes is unclear, but amongst its specific objectives are "strengthening and developing all aspects of the Common European Asylum System (CEAS), including its external dimension," and "countering irregular migration."

It is the successor to the Asylum, Migration and Integration Fund (AMIF), which ran from 2014-20.

Civil Security for Society

Budget: €1.6 billion

The Civil Security for Society research and development budget funds projects dealing with disaster preparedness and response (ranging from terrorist attacks to industrial disasters, floods and forest fires); 'protection and security' (encompassing crime, radicalisation, terrorism and border control); and cybersecurity.

Projects generally involve a consortium of different organisations cooperating to develop some new type of technology, technique or procedure. Thus, the end result may come in the form of a tangible product (for example, a new type of camera or piece of software) or knowledge intended to assist in the future development of such a product. As noted above, the security research programme funded numerous projects developing "smart borders" technology, and the programme has also been used to develop multiple technologies for incorporation into EUROSUR.

Since the 2021-27 programme began operating, six border security projects worth a total of nearly €32 million have been launched. During the 2014-20 period, the predecessor programme ("Secure societies") financed 43 border security research projects worth €242.5 million in public funding. A number of these are seeking to develop technologies explored in the studies examined in section 5 of this report.

For example, the €3.5 billion ODYSSEUS project hopes to develop technologies that "will allow citizens to cross borders without any intervention by just leveraging their smartphones combined with strong and continuous identity verification" – that is, continuous biometric surveillance. The EURMARS project (€5.9 million in public funding) is building "a secure multitasking surveillance platform… clustering high altitude platforms technology, satellite imagery, UxVs [drones] and ground-based sensors into a novel joint surveillance capability." In a similar vein, I-SEAMORE (€6.5 million) hopes to use AI and big data analysis to fuse data from aerial and maritime drones and open sources (including satellite data), to enable "wide maritime border and coastal areas monitoring, analysis of potential threats, support to search and rescue operations, detection of illegal activities, among others."

Trust Fund for Africa

Budget: €5 billion

The Trust Fund for Africa was set up following the 2015 Valletta Summit between European and African states, and to date €5 billion have been pledged for projects "to address the root causes of instability, forced displacement and irregular migration and to contribute to better migration management." Payments continued until the end of 2021 and it has now been folded into the NDICI budget.

Millions of euros have gone to projects aiming to boost border controls and surveillance, while others are helping African states set up biometric population registers, ostensibly to facilitate the acquisition of benefits and exercise of rights (for example voting) by citizens of those states. However, such databases also assist in the enforcement of EU immigration controls, by facilitating

the identification of individuals that EU states wish to deport. The French company Milipol says a project in Ivory Coast aims to identify "people genuinely of Ivorian nationality and [organize] their return more easily," according to Euronews. As noted above, a similar project in Senegal is also intended to boost EU deportation efforts. The European Ombudsman found that the European Commission had failed to properly assess the human rights risks of these projects, following a complaint from multiple human rights organisations.

Neighbourhood, Development and International Cooperation Instrument (NDICI)

Budget: €79 billion

NDICI "aims to support countries most in need to overcome long-term developmental challenges," and incorporates a number of funding instruments from the 2014-20 period that were part of the EU budget and that sat outside it (such as the Trust Fund for Africa).

The aim of providing development assistance has been subverted by the inclusion of a requirement for 10% of the total to be "dedicated particularly to actions supporting management and governance of migration and forced displacement within the objectives of the Instrument." Furthermore, 10% of the NDICI's "Neighbourhood instrument" will be used as an "incentive towards reforms" in a number of areas in third states, including migration. CONCORD, an aid group, described the inclusion of migration-related clauses in the final legislation as "shameful".

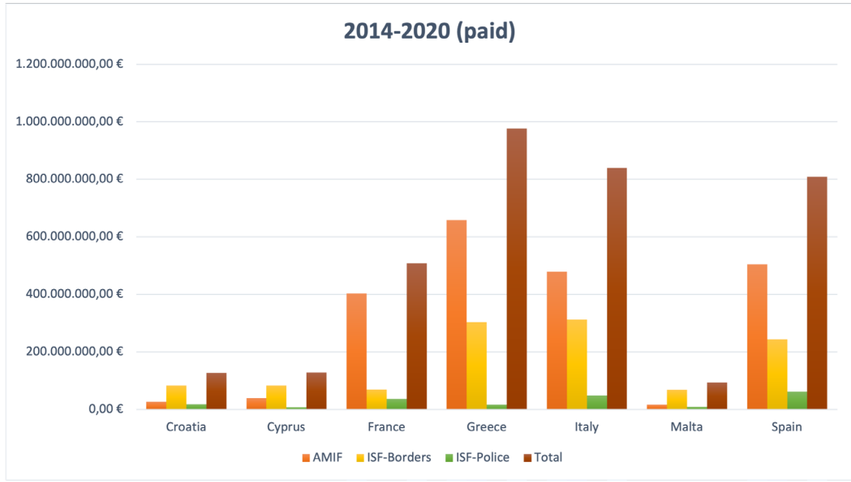
Instrument for Pre-Accession Assistance (IPA III)

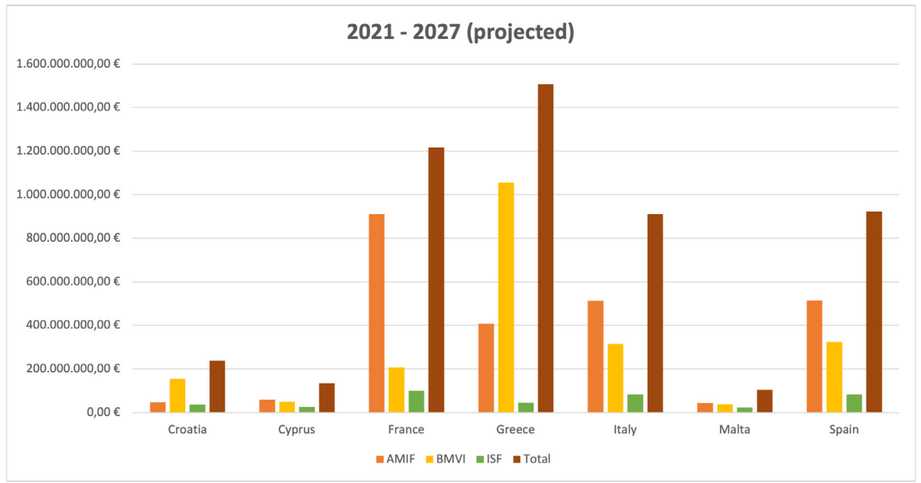
Budget: €14.2 billion

The IPA is used to support "reforms" in countries that are in the process for becoming EU member states, and substantial portions of the total budget of €14.2 billion can be used for border and migration control purposes. One of the objectives of the budget is to "improve migration management, including border management and tackling irregular migration, as well as addressing forced displacement." This goal falls under the heading of "rule of law, fundamental rights and democracy," where it is a priority alongside corruption, organized crime and security, fundamental rights, democracy and civil society. It is unclear how much funding will go towards migration and borders specifically, but the heading it falls under will receive a total of almost €2.3 billion between 2021 and 2027. It is noteworthy that the only measure of success included in the budget is for the number of "refugees, asylum seekers and other persons of concern to the UNHCR" in the Western Balkans and Turkey to increase by 2027, underlining the geopolitical role of these regions as migration "buffer zones" for the EU.

KEY FIGURES

Overview of EU home affairs funding for Mediterranean member states, 2014-2027
Source: European Commission





Overview of border security research funding, 2014-2022

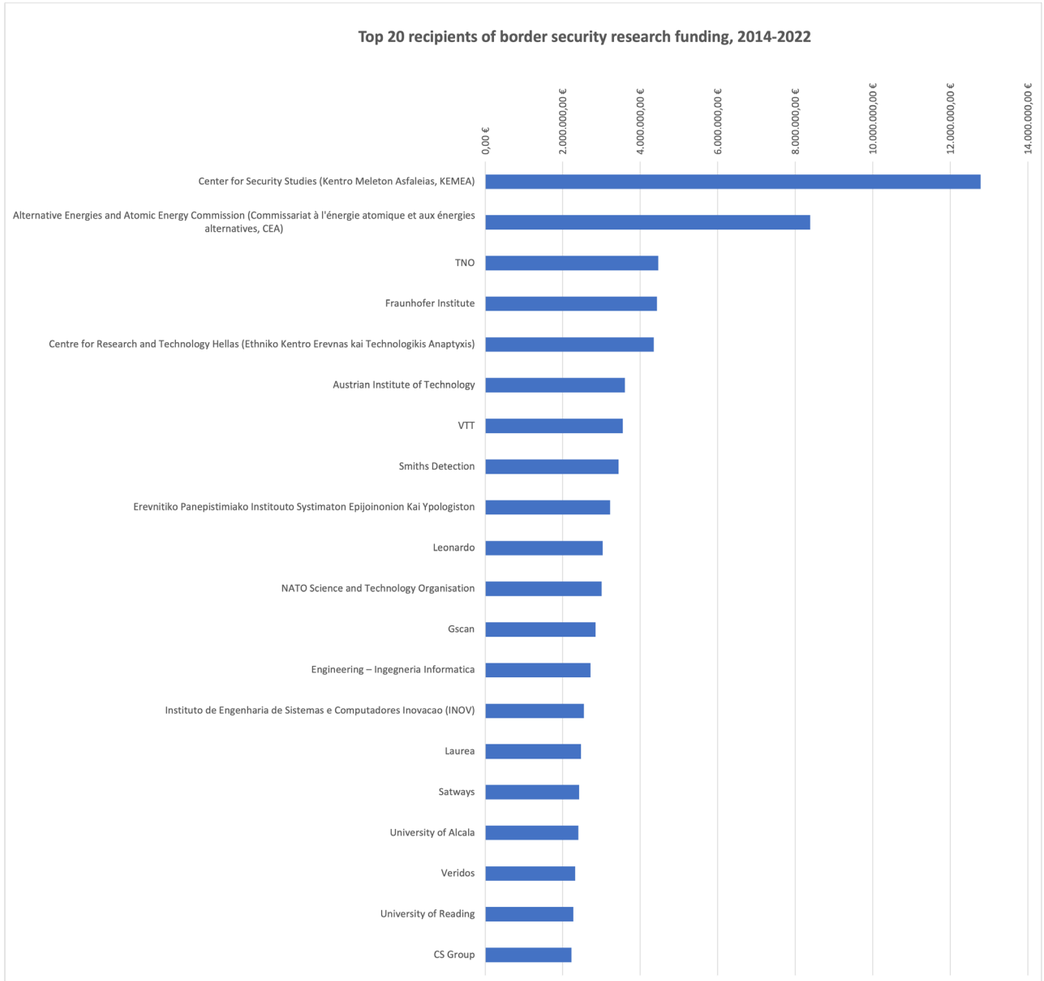
Source: EU Open Data Portal

	2014-20 (Horizon 2020)	2021-22 (Horizon Europe, program runs until 2027)
Number of projects funded	43	6
Total funding	€242,537,138	€7,972,525

TOP 20 RECIPIENTS OF BORDER SECURITY RESEARCH FUNDING, 2014-2022

Source: EU Open Data Portal

Organisation	State	Horizon 2020		Horizon Europe		Total	
		Projects	Funding	Projects	Funding	Projects	Funding
Center for Security Studies (Kentro Meleton Asfaleias, KEMEA)	Greece	13	€12,039,394	2	€745,313	15	€12,784,707
Alternative Energies and Atomic Energy Commission (Commissariat à l'énergie atomique et aux énergies alternatives, CEA)	France	5	€7,809,622	1	€575,375	6	€8,384,997
TNO	Netherlands	7	€3,744,358	1	€718,979	8	€4,463,336
Fraunhofer Institute	Germany	9	€4,433,411	0	-	9	€4,433,411
Centre for Research and Technology Hellas (Ethniko Kentro Erevnas kai Technologikis Anaptyxis)	Greece	8	€4,347,045	0	-	8	€4,347,045
Austrian Institute of Technology	Austria	3	€2,628,023	1	€979,306	4	€3,607,329
VTT	Finland	5	€2,981,963	1	€571,201	6	€3,553,164
Smiths Detection	France	3	€3,439,111	0	-	3	€3,439,111
Erevnitiko Panepistimiako Institouto Systimaton Epijoinonion Kai Ypologiston	Greece	5	€2,724,729	1	€501,750	6	€3,226,479
Leonardo	Italy	3	€3,029,944	0	-	3	€3,029,944
NATO Science and Technology Organisation	Belgium	7	€3,006,205	0	-	7	€3,006,205
Gscan	Estonia	1	€2,844,875	0	-	1	€2,844,875
Engineering – Ingegneria Informatica	Italy	4	€1,696,313	2	€1,023,688	6	€2,720,000
Instituto de Engenharia de Sistemas e Computadores Inovacao (INOV)	Portugal	4	€1,494,325	2	€1,050,225	6	€2,544,550
Laurea	Finland	5	€2,470,375	0	-	5	€2,470,375
Satways	Greece	5	€2,425,938	0	-	5	€2,425,938
University of Alcala	Spain	1	€1,257,485	1	€1,148,948	2	€2,406,433
Veridos	Germany	2	€2,324,075	0	-	2	€2,324,075
University of Reading	UK	3	€2,276,181	0	-	3	€2,276,181
CS Group	France	1	€1,973,209	1	€253,750	2	€2,226,959



CASE STUDY: SPAIN'S SOUTHERN BORDER

Spain's southern border has undergone substantial technological reinforcement over the last three decades, giving a clear indication of how the deployment of new border technologies plays out on the ground and the negative effects it has upon people seeking access to EU territory. What began with a barbed wire fences now involves drones, satellites, thermal imaging cameras and facial recognition systems, amongst other technologies. At the same time, the country's system for the management of asylum applications have been expanded and interconnected with other databases, demonstrating the trend towards the "interoperability" of data systems that has been enthusiastically taken up by EU institutions.

A recent report coordinated by the organisations Irídia and Novact tracks developments at the southern border over that period, noting that:

"The 'technification' of the southern Spanish border… has become central to the external fortification of the European Union, with sophisticated systems of video surveillance, artificial intelligence and biometric technology to close the way to migration and control the entries and exits of the population of third countries."

While the fall of the Berlin wall in 1989 was a cause for celebration across the continent, it did not take long for a European government to start building new border walls. In 1995, 100 Guardia Civil agents were deployed to Ceuta and Melilla to step up surveillance, and at that time a "surveillance road" eight kilometres long and six metres wide was built around Ceuta, "with an integrated system for automatically detecting people, video cameras and a megaphone system for giving warning messages."

This was followed by repairs to existing fences in Ceuta and Melilla in 1996, after a number of attempts by people to reach Spanish territory. Then, in 1998, the government of José María Aznar financed the construction of new, taller, stronger, double-layered fences. Aznar was leader of the right wing Partido Popular, but the trend for increasing fortification of the border has been taken on by governments of all stripes in the years since, including the current centre-left administration, which describes itself as the "progressive coalition".

More surveillance technologies were to follow. In 2002, the port city of Algeciras became host to the first element of Spain's Integrated External Surveillance System (SIVE, Sistema Integrado de Vigilancia Exterior), with other sites later added to locations along the country's coastlines. The aim is to provide an early warning system through the use of sensors to detect vessels travelling towards Spain.

Irídia and Novact argue that the deployment of the SIVE led to what was then the principal maritime migration route to Spain (across the Strait of Gibraltar) being diverted to a crossing over the Atlantic Ocean to the Canary Islands. At the time (2005-2009), the Asociació Pro Derechos Humanos de Andalucía (APDHA) reported a huge increase in deaths at sea resulting from this shift in routes, based on estimated figures. However, the deployment of SIVE nodes on the islands then led to a further diversion to Ceuta and Melilla as primary entry points – thus leading to the construction of yet more fences and associated surveillance technologies.

In 2005, the Spanish government (now headed by José Luis Zapatero of the centre-left Spanish Socialist Worker's Party) announced the construction of a third layer of fencing. The fence itself was to be accompanied by "the most advanced technology to impede the entry of irregular migrants," such as new surveillance cameras. Zapatero also ordered the deployment of the army to support the Guardia Civil.

Between 2000 and 2008, the report states:

"…the European Union and the Spanish state invested €230 million in deploying and implementing SIVE, alongside €72 million for the automation and extension of the fences in Ceuta and Melilla between 2005 and 2013. These two elements constitute the biggest border business niche in Spain."

This does not include funds awarded to the Moroccan government with the aim of controlling migration. A Statewatch report found that between 2001 and 2018, almost €215 million was provided to Morocco by the EU to finance border security projects, an amount that does not include bilateral funding from Spain.

There was more to come, and "2013 would be key in terms of the technification and militarisation of the southern border," says the report. "On one hand, the Spanish government announced the reinforcement of the already-triple fence in Ceuta and Melilla with a metallic 'anti-climb' fence and the reintroduction of razor wire," which had been introduced in 2005 and then removed two years later following protests in response to the injuries it caused. Furthermore, the Guardia Civil acquired "a second surveillance helicopter, while the first was equipped with a thermal camera and a powerful spotlight."

Legislation establishing the European Border Surveillance System (EUROSUR) was also approved in 2013, giving formal backing to a process that had begun some years earlier (see section 2). SIVE, itself a network of surveillance devices and technologies, is just one national node in the EUROSUR network, which integrates National Coordination Centres of all EU member states. The intention is also to integrate surveillance systems in third countries into the network, to further enhance the "situational awareness" enjoyed by Europe's border guards. At the same time, the introduction of the Entry/Exit System (EES, see section 2) in the years to come will require the biometric identification and authentication of anyone crossing the borders of Spain and any other EU member state.

In January 2019, the PSOE government approved a new plan aimed at the "reinforcement and modernisation of the land border protection system in Ceuta and Melilla," made up of short and medium-term measures. The former included installing a new video surveillance system in Ceuta and expanding the existing system in Melilla, "the modernisation and reinforcement of the security infrastructures at the border perimeters," and the installation of a facial recognition system at the border crossing points at Tarajal, Ceuta and Beni Enzar (in Melilla). The medium-term measures included a vague commitment to set up "a new smart border [frontera inteligente] at the Beni Enzar border crossing," and a total of €32.7 million from the EU's Internal Security Fund and Asylum, Migration and Integration Fund was set aside for the work.

Irídia and Novact remark that while this plan has "a kinder look," the aim is "to obtain total control of every person that tries to cross the border" whilst "collecting very sensitive information." Although razor wire was removed from the fences for the second time in 2019, again following public pressure:

"...the Spanish state has continued its policy of installing both architectural and technological barriers to prevent access to migrant persons and refugees. All these systems have required the management of a multi-million budget concentrated in 10 companies, who have taken seven out of every 10 euros in public funding for migration management."

Those companies have been examined in detail in a 2020 report by porCausa on Spain's migration control industry, although one company of interest not mentioned in the report is GMV, a Portuguese firm that holds the contract for managing EUROSUR as well as Spain's "integral system for the management of applications under international protection."

The system, SISGEPI, demonstrates well the trend towards making databases and information systems "interoperable". The central system is connected to a multitude of other databases including police, criminal records, civil registration and visa systems, for the purpose of conducting background checks on asylum-seekers. Novact have noted that "the centralisation and interoperability between databases poses grave risks for people's privacy." The more data that is interconnected and the greater the number of access points, the more likely it is that data will be accessed and used illegally.

In fact, Spain's gendarmerie force, the Guardia Civil, were systematically (and illegally) accessing SIGESPI between 2013 and 2014 for the purpose of criminal investigations, logging some 1.5 million searches in that period. The practice was denounced in 2015 by the Policía Nacional, who control the system. Granting police forces access to systems holding data on asylum-seekers and other foreign nationals for the purpose of criminal investigations is now standard practice at EU level, following the adoption of controversial changes to Eurodac in 2013. In practice, this has the effect of criminalising these groups: if similar databases storing information gathered from citizens do not exist, there is no way they can be subject to the same level of police scrutiny.

On the one hand, then, increasingly advanced technologies are deployed to keep people out of the EU. On the other, they are used to ensure stricter control over those who do manage to enter. The ongoing reinforcement of the Spanish border demonstrates well the futility of the 'Fortress Europe' approach to migration: despite 30 years of more fencing and new surveillance equipment, the number of people seeking to cross – and, despite the odds, getting across – has not decreased. Instead, their journeys have simply become more dangerous. Meanwhile, those who do manage to make it to EU territory are processed through systems that make use of increasing amounts of personal data drawn from a whole host of sources, raising risks of privacy violations, data protection breaches and questions of proportionality. Nevertheless, based on the plans discussed in section 5 of this report, these trends are set to continue.

STATE OF PLAY: UPCOMING LEGISLATION

Much of the legislation that makes up the New Pact on Migration and Asylum is now in the final stage of negotiations between the Council and the Parliament. A number of these files – the Eurodac Regulation, the Schengen Borders Code and the Screening Regulation, will further propel the expansion of Europe's techno-borders.

EURODAC

A revamped Eurodac Regulation was initially published in 2016, but a further revised version was published in September 2020 as part of the Pact. At the time of writing, the Parliament had agreed its position on the proposal, but discussions were ongoing in the Council. In September 2021, Statewatch and 25 other NGOs warned that Eurodac is evolving from "a tool supporting the implementation of the Dublin Regulation to a weapon against migrants." The intention is to massively expand the database and the purposes for which it can be used. As well as fingerprints, facial images and a wealth of biographic data will be stored in the database. Data will also be gathered from a far broader group of people: firstly, by expanding the categories of persons covered by the database to irregular migrants, persons disembarked following search and rescue operations, and persons eligible for resettlement in the EU; secondly, by lowering the age limit for data collection to six. Currently, the system holds information on asylum-seekers and people apprehended in connection with the irregular crossing of an external border who are 14 and older.

The proposal includes the possibility of imposing "administrative sanctions... for non-compliance with the fingerprinting process," including against children. This would institute in law practices that infringe the right to dignity, integrity of the person, liberty and security – not to mention the best interests of the child – that were previously set out in a set of guidelines. The EU Parliament's position on the proposal maintains the possibility of imposing sanctions.

SCREENING REGULATION

The proposed Screening Regulation seeks to harmonise practices across the EU with regard to "checks on persons and efficiently monitoring the crossing of external borders". It will also see the large-scale detention of people arriving irregularly at the EU's external borders, with a view to their swift expulsion. It comes alongside existing rules on border control (in particular, the Schengen Borders Code) and on the identification of individuals set out in asylum and migration legislation (for example regarding Eurodac, the VIS and the EES).

A study published by EuroMed Rights in May 2021 found that:

> "No country of first arrival would benefit from the proposed border procedure rules… Spain and Italy would respectively have to multiply by 6 and 7 times their number of formal and informal detention facilities should the EU Pact rules be implemented. Under these rules, in a situation of crisis similar to that of 2015, Greece would have to multiply by 34 its detention facilities."

With regard to individuals who have irregularly crossed an EU external border, are disembarked following a search and rescue operation, or file a claim for asylum at an external border, the Screening Regulation will introduce common rules for:

- a preliminary health and vulnerability check;
- an identity check against EU databases;
- registration of biometric data (i.e. fingerprint data and facial image data) in the appropriate databases, to the extent it has not occurred yet; and
- a security check via a query of relevant databases, in particular the Schengen Information System (SIS), to verify that the person does not constitute a threat to internal security.

The stated aim is to ensure the referral of individuals to the correct procedure and appropriate protection in case of special needs. The Commission proposes an independent monitoring mechanism to supervise that the screening is taking place in accordance with fundamental rights protection, although the Council's position on the text seeks to massively water down the scope of that mechanism. The Parliament, on the other hand, aims "to strengthen the mechanism and to ensure its independence." A separate Regulation is under discussion to permit access to the EU's criminal records information database as part of the screening procedure.

The checking of biometric data with European information systems is key to the screening process and raises certain procedural rights questions. In case of a "hit" in a database following a search with biometric or other data, the searching authority has to contact the authority responsible for registering the alert to seek detailed information on the reasons the information that triggered the hit was recorded in the system. This procedural step is meant to guarantee the protection of the principle of effective remedy and of equality of arms, but the extent to which that information is always supplied to individuals is unclear. CJEU jurisprudence has constantly recalled this position since Spain v. Commission in 2006, the most recent judgement dating from 2020 in R.N.N.S. and K.A. v Minister van Buitenlandse Zaken.

MEPs are seeking to use the Screening Regulation to prohibit the use of certain invasive technologies. The EP's position on the text states:

> "Third-country nationals shall not be subject to any intrusive biometric surveillance technologies nor predictive analytics and biometric categorisation in or around the reception or screening facilities or during the screening. The use of lie detection systems or long-range listening devices shall be prohibited."

If the provision makes it into the final text, it may spell trouble for initiatives such as Greece's CENTAUR program, which claims to use "cameras, drones and AI-assisted movement analysis" to detect "suspicious crowds and incidents."

The screening process is also meant to involve the verification of "objects in possession of third country-nationals" in order to help determine an individual's identity. Numerous EU states seek to extract data from mobile phones to verify individual identities and investigate their asylum claims. The German federal administrative court recently made a landmark ruling on the proportionality of mobile data extraction in asylum cases, permitting it only when identity or nationality cannot be established by less intrusive means. There are currently no specific safeguards in the text concerning mobile phone data extraction, which is likely to become a point of contention between authorities and applicants in the future.

SCHENGEN BORDERS CODE

In May 2017, the European Commission published a recommendation calling for an increase in identity checks and surveillance within the EU, stating that "the intensification of police checks in the entire territory of Member States, including in border areas and the carrying out of police checks along the main transport routes such as motorways and railways, may be considered necessary and justified." This was followed in December 2021 by a legal proposal to reform the Schengen Borders Code, which "lays down rules governing border control of persons crossing the external borders of the Member States of the Union," although it also includes provisions allowing the temporary reintroduction of internal border controls between Schengen states, in cases of "a serious threat to public policy or internal security."

In a bid to avoid the ongoing imposition of internal border controls by member states – which, in some cases, have now been in place for years – the proposal includes various alternative options. These include more extensive patrols and identity checks in border areas, provided those checks are not equivalent to border controls, and new rules to make it easier for states to carry out summary returns of migrants engaged in "secondary movements" in the Schengen area.

The proposal was condemned by a coalition of almost 40 NGOs, who argued that it will increase the use of monitoring and surveillance technologies, without adequate safeguards, and increase the likelihood of racial profiling and other fundamental rights violations. Article 23 of the proposal, dealing with identity checks within member states' territory, says:

> "The exercise of powers may include, where appropriate, the use of monitoring and surveillance technologies generally used in the territory, for the purposes of addressing threats to public security or public policy."

According to the Platform for International Cooperation on Undocumented Migrants (PICUM):

> "As it stands now, the new Schengen Borders Code would turn the Schengen area into a tech-controlled space where racial profiling gets de facto legitimised, access to asylum is curtailed and freedom of movement is undermined".

The Council has agreed its position on the proposal, while the Parliament is still engaged in internal negotiations.

ARTIFICIAL INTELLIGENCE ACT

Apart from the Migration Pact, the European Commission proposal on the AI Act also deals with technologies meant for migration and borders. The EU's proposed Artificial Intelligence (AI) Act aims to address the risks of certain uses of AI and to establish a legal framework for its trustworthy deployment, thus stimulating a market for the production, sale and export of various AI tools and technologies. However, certain technologies or uses of technology are insufficiently covered by, or even excluded altogether, from the scope of the AI Act, placing migrants and refugees (people who are often already in a vulnerable position) at even greater risk of having their rights violated.

The proposal takes a "risk-based approach" to regulating artificial intelligence technologies, with the intention of boosting technological innovation and, thus, economic growth. AI systems are to be categorised by the level of risk they pose to health and safety and fundamental rights, with three different levels proposed: unacceptable (banned); high risk (use must meet certain requirements); and low risk, or "uses with specific transparency obligations" (permitted as long as they meet those transparency obligations).

The Act also introduces three different categories of users and providers who will be covered by the Act: providers who place on the market or put into use AI systems within the EU (whether or not those providers are established in the EU or elsewhere); users of AI systems located within the EU; and providers and users of AI systems that are located in a non-EU state, when the output of that system is used within the EU.

In relation to migration and asylum, the proposal makes no reference to the need to uphold international legal obligations, and does not contain particularly stringent provisions to govern the use of AI technologies for immigration, asylum and border control purposes. For this reason, a coalition of NGOs including EuroMed Rights and Statewatch has been working to seek amendments to the text that will "ban the use of experimental tech against people crossing borders and effectively regulate to ensure AI is used with safety and accountability."

The iBorderCtrl project described above is a good example of the type of technology that would be permitted by the AI Act, albeit in the high risk category. Equally, predictive analytics systems may rely on various types of AI technology. In combination with border surveillance systems, they may be used to aid in the organisations of pushbacks. Under the AI Act, they would be categorised as low risk. The Commission's proposal also seeks to exclude the EU's large-scale IT systems from the provisions of the AI Act, despite – or perhaps because – they will soon incorporate automated profiling technologies that would otherwise be classed as high risk.

At the time of writing, the Council has agreed its position on the proposal. The parliamentary committees responsible for the file voted in mid-May to include a number of important protections, although it is not all good news: the text still contains "loopholes favouring industry actors over people's rights," and "MEPs failed to include in the list of prohibited practices where AI is used to facilitate illegal pushbacks, or to profile people in a discriminatory manner." The text still has to be voted on by the Parliament as a whole (rather than just the two responsible committees) prior to the start of secret "trilogue" negotiations with the Council.

AUTOMATING THE FORTRESS: PLANS FOR THE FUTURE

There is significant enthusiasm within EU and member state institutions for the further development of new technologies. A series of in-depth reports have been produced for the European Commission and Frontex in recent years that give an insight into the future direction of the technologies that will be deployed for immigration, asylum and border control purposes. One of these (which has been analysed elsewhere) argues that "legislations and regulations appear to be the barriers that technology developers will need to overcome to ensure the use of their AI-based solution," underscoring the tensions between these technologies and existing legal frameworks. Substantial work has also been undertaken by Europol and Frontex to map out the "future of travel".

The increasing reliance on technological "solutions" raises questions about whether they really are as advanced as their proponents claim, or whether they mainly provide a route to turn prejudice and discrimination into a "pseudoscientific" endeavour that waters down the responsibilities of states, public bodies and officials for the results of their actions. At the same time, the turn towards advanced risk assessment and profiling of individuals will lead to claims against people that are much harder to rebut than, say, criminal charges brought due to past behaviour. There is a clear need for close scrutiny and vetting of algorithms and technologies deployed in high-risk scenarios such as migration and border control.

There is no guarantee that all the technologies discussed in these reports will eventually be deployed at the EU's borders. The reports have been commissioned at a time when there is substantial hype about the ability of "artificial intelligence" to carry out all manner of tasks, and the consultancy firms producing reports for state actors have a vested interest in encouraging the use of new technologies, as their services may then be required to help install or implement new systems. Nevertheless, the intended direction of travel is clear: an increasing refinement and optimisation of systems of surveillance and control. This work is currently being undertaken behind closed doors by national and EU officials, with little to no public scrutiny or discussion.

ARTIFICIAL INTELLIGENCE

Summary

A 2020 study for the European Commission explored "how AI can be leveraged in the context of Border Control, Migration and Security." It proposed options for how EU institutions and agencies could "transform the opportunities identified in the first stage of the study into a programme of work for implementation." The resulting "roadmap" set out five relevant forms of AI technology for EU border control:

- chatbots and intelligent agents;
- risk assessment tools;
- knowledge management tools;
- policy insight and analytics tools, and
- computer vision tools.

The report identified nine different areas in which AI could be deployed, which are outlined below. Of the most significant concern from a fundamental rights perspective are:

- the use of AI to assess visa and travel authorisation applications;
- automating procedures for granting international protection;
- the deployment of automated, biometric mass surveillance at EU borders; and
- the use of AI-powered mass surveillance to monitor and assess peoples' compliance with immigration rules.

Areas of interest

The study argues that deploying AI in visa and travel authorisation applications could allow for swifter and improved risk assessments of third-country nationals, greater transparency and consistency in the issuing process, more efficient and simpler procedures, and a reduction in the number of manual tasks needing to be performed by officials.

This could be done through the use of chatbots during an online application process – for example, to answer questions from applicants, assess information provided and check data quality. AI could also be used to "triage" applications and determine which require a more thorough risk analysis – a technique that was employed by the UK Home Office for visa applications and withdrawn under threat of a legal challenge. The Dutch authorities have also been found to be using an algorithm in the visa procedure that data protection officials described as unlawful and

as leading to ethnic profiling. As the Deloitte report notes, one of the "challenges" in this area is the risk of "inadvertent racial bias".

The study also suggests that AI could be deployed to detect "irregular travelling patterns", although it notes that this would require more extensive data collection: "the model would also require data to be provided by different airlines, for which there are not necessarily legal obligations in place." AI could also be used to "tailor questions asked to the applicant creating an augmented application form." While the study underlines that this would require changes in national laws to address differentiated data collection and usage, the proposal also raises serious questions regarding procedural fairness for visa applicants.

It should be noted that although the study was published in 2020, EU legislation on the European Travel Information and Travel Authorisation System was approved in 2018, mandating the introduction of automated profiling technologies on applications, albeit not explicitly referring to AI. The same kind of checks are to be introduced into the Visa Information System in accordance with legislation that was proposed in 2018 and approved in 2021. Furthermore, legislation on Passenger Name Records (PNR) and Advance Passenger Information (API) also requires the transfer of flight information to the authorities (see section 2 of this report).

With regard to the issuing of documents for long-term stay or migration in the Schengen area, the study again proposes the use of chatbots for the application process, and the automated "triaging" of applications in order to speed up risk assessments and background checks. It also proposes the use of chatbots for applications made by individuals for permission to move to another EU member state. This could facilitate "reuse of previously submitted documents and information," as well as answering questions and providing information, though it would also require sharing of personal data between member state authorities that may not currently be adequately regulated, as well as potentially failing to flag high-risk individuals and incorrectly flagging low-risk applicants. Any such system should therefore not be used as a "direct substitute" for human decision-making. Again, the use of AI is expected to enable shorter processing times and a decrease in manual work for officials.

The study proposes substantial automation of procedures for granting asylum or other forms of international protection, "to facilitate and speed up the current process while gathering additional insights." This would include using AI for "sensory analysis of an individual," to see whether they should be "further investigated by a human social worker or granted special procedural guarantees." Technology could also be deployed to assess the likelihood of an individual absconding, "to allocate refugees to geographic regions... where they are more likely to find work and integrate smoothly," and aid with "risk assessment of returns to country of origin". Once again, the use of chatbots during the application process is recommended, for "going through the steps which do not require human expertise."

A number of benefits are associated with the deployment of AI in the asylum procedure: "possible shorter waiting times" for applicants and an associated reduction in costs for states; "limiting the risk of granting international protection to individuals who are ineligible or have bad intentions"; more uniform procedures due to reducing the dependence on human decision-making; and reducing manual tasks for officials.

The study notes risks posed by these plans – notably, the need to keep a "human-in-the-loop" due to potential inaccuracies in the technology, which could lead to "incorrect decisions from vulnerability assessments or regarding placement into a detention centre." Changes to the law may also be required due to the changes in data collection and usage that would be needed, and the study also notes that using AI for refugee allocation and integration would be "difficult to measure". What it does not mention is that using AI to automate substantial parts of the asylum procedure is likely to further dehumanize a process that is already marked by a failure to treat individuals fairly and with dignity. There is no indication that the introduction of AI technologies would do anything to resolve this – if anything, it seems likely to exacerbate the problem.

The study's proposals for the SIS include a truly alarming proposal to use "computer vision to detect SIS alerts using cameras" deployed at border points. That is to say, it proposes plugging CCTV cameras into an AI-enabled, EU-wide police database so that wanted or suspected individuals can be tracked down via their faces or vehicle number plates. This is precisely the type of biometric mass surveillance – "an unlawful practice that unfairly treats everyone like a suspect" – that civil society organisations have called for to be banned, a call that may well be incorporated into the European Parliament's position on the AI Act. The Prüm system of national police biometric databases poses similar risks.

The study notes that this proposal "is at risk of violation of a number of ethical principles" and that inaccurate technology may lead to unjustified police checks of individuals, but it nevertheless includes it in the roadmap, saying that "it would most likely be easier to begin with detecting vehicles and expand to people and other objects."

It is noteworthy that the Italian authorities have already attempted to deploy a facial recognition system, ostensibly to be used to try detect matches of people disembarked following rescue operations in the Mediterranean with a watchlist maintained by the police. In 2021 the Italian ombudsman found that the system, which was purchased using money from the EU's Internal Security Fund, "would enact a form of indiscriminate/mass surveillance" and prohibited the deployment. However, a separate system, used to verify authenticity of the photographs in travel documents, was approved by the ombudsman.

Given the size of the SIS database, which "is difficult for humans to search manually," the study proposes using AI "to aid in the knowledge management of the SIS." AI could also be used for the automated completion of forms used by the SIRENE Bureaux, the entities responsible for "exchanging information and coordinating activities related to SIS alerts."[4]

The study proposes using AI to "triage border crossers" and for "operational resource planning," in order "to improve swift border crossings while at the same time improving security of the current border crossing points." This is expected to speed up border crossing times, enhance security through AI-powered risk assessments and "consistency in the selection of travellers being called for the second line border check by using a data-driven decision process," and improve resource management, for example through the more efficient deployment of staff.

Once again, the study notes the risks posed by automated risk assessments, raising issues related to privacy, the need for legal changes, potential problems with "unethical bias (e.g. against a certain gender or demographic group)," and the potential for inaccurate results. No mitigating measures are suggested to deal with these risks, and with regard to the privacy implications of more intrusive screening and vetting at the border, the study states that while it cannot be done

without using personal data, "it is mandatory for the traveller to provide this information when at a border crossing point."

The study proposes AI not just to enhance the ability of the EU to control individuals crossing its borders, but to ease the management of the large-scale databases and IT systems that make up its digital border infrastructure. Through "big data analytics and metrics," failures or other unwanted incidents in the systems could be predicted; and chatbots could be introduced to assist the "first and second-line service desks" in their tasks, as well as training new users of the systems. This would require access to vast quantities of data, although it would not necessarily be "personally identifiable." Poor AI decision-making "could have significant effects on systems and uptime".

Even policymaking in the fields of borders, immigration and asylum could benefit from AI technology, according to the Deloitte study. Technology could be deployed to examine the extent to which EU law has been transposed and implemented in the member states, undertake automated information-gathering from the media and official documents to aid in the detection of public and policy trends, ensure "effective and simplified stakeholder communication," and enable "prediction of stakeholder perception and acceptance of new policy." Amongst the risks of using AI to aid in policymaking, the study notes "confirmation bias (where public opinion appears skewed towards those who are most vocal) and even algorithmic exploitation to intentionally bias analysis with misinformation."

The final area in which the study suggests AI could be deployed concerns topics that relate to one or several of the planned initiatives. This includes translation, identification of forged or fraudulent documents, using a "historic case reasoning engine" to ensure consistent decision-making, improve the accuracy of facial recognition algorithms, and even "AI to monitor the ethicality of other AI systems" – what might be termed 'meta-AI'.

One of the more troubling proposals included in this section is for "post-application monitoring of TCN [third-country nationals]." The study notes that as things stand, "there is limited monitoring after issuing a permit to a TCN," opening up possibilities for abuse. To deal with this, the study proposes a highly intrusive form of AI-powered mass surveillance:

> "For example a TCN might receive a residence permit because of marriage with an EU resident. However, the couple could be separated soon after issuing the permit. In this case the conditions for providing the permit do no longer apply. The system would try to assess whether conditions for the permit issuance are still valid by analysing various sources of data (e.g. address or tax information) and provide insight on the probability of fraud.
>
> Another example is to monitor if a TCN is complying with the restrictions of the issued work permit, such as number of days worked. This could be checked by analysing tax statements."

SURVEILLANCE TECHNOLOGIES

Summary

A 2022 study by the European Commission's Joint Research Centre and Frontex sought to "assess challenges and opportunities in emerging technology and science" that could address the "operational needs" of EU border authorities. It is based on an examination of scientific publications and patent applications and includes information on 11 types of border surveillance technology in which Frontex has an interest. It analyses what it calls "weak signals" of technology that is emerging, but not yet ready for operational deployment; and emerging applications of technology that can be used for border management.

The 11 technologies identified are divided into "first priority" and "second priority", according to Frontex's interests.

First priority technologies:
- High Altitude Pseudo Satellites (HAPS);
- the internet of things;
- intelligent video surveillance;
- radar technologies; and
- underwater sensors.

Second priority technologies:
- video synopsis
- parafoil unmanned aerial vehicles (UAVs, that is, drones);
- algorithmic surveillance; and
- "micro drones".

Each of these surveillance technologies poses issues with regard to fundamental rights: certainly, to privacy and data protection, but depending on how they are deployed they may also impinge upon the right to leave one's country, the right to claim asylum, and the right to liberty and security.

Areas of interest

High Altitude Pseudo Satellites (HAPS) are deployed at altitudes of 20km or higher, above the range of conventional aircraft, and can come in the form of balloons, airships or planes.

Their benefits include persistent surveillance of the area they cover, and they can be deployed in a complementary manner to drones and satellites. Surveillance and imaging systems can be deployed on HAPS in combination with machine learning technologies to identify "highly frequented routes", "points of interest" and "anomalous behaviour", as well as offering the possibility of predicting the movement of objects (and, presumably, people). The EU is currently providing almost €6 million to a research project, funded through the Civil Security for Society budget, aiming at "clustering high altitude platforms technology, satellite imagery, UxVs and ground-based sensors into a novel joint surveillance capability."

The internet of things (IoT) is described as "the network of physical objects or 'things' embedded within electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data through the internet." In an everyday context, this may include a person's fridge, television, "smart speaker" or other domestic devices. For the purposes of border surveillance, the devices in question may be robots, sensors and cameras. A network of these devices allows "surveillance at a distance", with the imagery and data they capture potentially reducing the need for border guards to be physically present in remote or difficult-to-reach locations. A 2020 paper written by a group of Spanish academics examined the feasibility of deploying an IoT-based surveillance system at Libya's borders in the Sahara, which could "increase the areas covered, while reducing the human intervention within the monitoring operation." The paper does not mention any of the human rights risks related with deploying border surveillance infrastructure in Libya, instead focusing on the technical requirements of such a system.

GNSS (Global Navigation Satellite System) radar "is mostly used for sea-level measuring and state of sea estimations but can also be used for target location at sea," which "has advantages of all-weather capabilities and worldwide coverage." The study cites numerous technical research papers that highlight the possibility of using a technology developed for environmental and weather observation for the purposes of tracking and classifying vessels at sea, which would substantially enhance the maritime surveillance capabilities of EU border authorities. The study also examines "track while scan" technology, "in which the radar allocates part of its power to tracking the target or targets while part of its power is allocated to scanning, unlike the straight tracking mode, when the radar directs all its power to tracking the acquired targets." However, it notes: "No recent articles mentioning border or surveillance were retrieved for this technology."

The use of **underwater sensor networks**, which are also used for marine exploration, oil and gas inspection and military applications, may also prove useful for enhancing maritime surveillance. However, one paper cited in the study states that the promise of the technology "still fails to meet real-time constraints," as it is undermined by the "exhaustive amount of time and substantial power" that large-scale data transmission and collection requires.

"**Video synopsis** is an activity-based video condensation approach to achieve efficient video browsing and retrieval for surveillance cameras," the study notes. In order to reduce the time required to trawl through video footage and retrieve segments of interest, video synopsis "aims to shorten long video sequences into... compact video representation by rearranging the video events in the temporal domain and/or spatial domain" – that is, by automatically selecting footage of interest over certain periods of time or relating to certain places covered by video surveillance systems. In this way, footage from cameras used for border surveillance could be parsed by an algorithm and only those sections containing people or vehicles would be displayed to an official.

Algorithmic surveillance, described by the JRC study as "a form of automated decision-making," involves the application of algorithms to surveillance camera footage or sensor data to "make clarifications and educated guesses on the data." Scientific articles cited in the study propose multiple potential uses for border surveillance: to detect, count and track people's movements in an area; to use face recognition algorithms to identify or recognise people; vessel detection and tracking for maritime surveillance; and "real-time object recognition and tracking". This form of technology has been developed and tested by multiple EU research projects, and the JRC has previously published in-depth reports on the topic.

The final technology with border surveillance potential identified by the study is the use of "**nano or micro drones**," which "aim to reduce the weight, sizes, and costs associated with drone technology." Amongst the institutions based in the EU that have produced research papers on the topic, five of the top 10 are from Italy. A paper cited by the study looking at the use of "mini-drones and swarms and their potential in conflict situations" argues that "swarming and associated abilities" can be used "to overwhelm a combatant as well as bring extra functionality by means of extra sensors spread throughout the swarm." As with other emerging technologies, the EU's Civil Security for Society budget has financed relevant research projects. Most notably, "autonomous swarm of heterogeneous RObots for BORDER surveillance" (ROBORDER) was awarded €8 million, and aimed to develop and demonstrate "a fully-functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles."

The only technology identified in the study considered useful for border control rather than border surveillance is the blockchain, "a database in which information is stored in a distributed manner." The technology makes it possible to "combine novel biometric approaches, decentralized digital identity and border control environment strongly to each other," argues the study, making it possible to "provide new kind of data and use cases to border control scheme in open manner while preserving privacy." Potential uses cited in the study are for registering departure and arrival records, "information exchange, inter-agency cooperation, revenue collection," carrying out security checks, checking the authenticity of travel documents and identity verification.

BIOMETRICS

Summary

A study published by Frontex in September 2021[5] sought to provide "technology-related insights on the future of biometrics for its implementation in border check systems that could be utilised by the European Border and Coast Guard (EBCG) community in the short- (2022-2027), medium- (2028-2033) and long-term (2034-2040) perspectives."

Following an analysis of 20 "technological clusters",[6] the project identified five "key technology clusters" (KTCs) deemed to have the greatest potential to influence border management practices:

- contactless friction ridge recognition;
- 3D face recognition;
- infrared face recognition;
- iris recognition in the near infra-red spectrum;
- iris recognition in the visible spectrum.

As with the other technologies examined in this section, these seek to further intensify and refine existing models of biometric identification, by expanding the types of biometric identifier that can be used and where and how they may be captured.

In the words of Frontex's then-director, the intention is to deploy new biometric technologies to create a "seamless" experience for travellers to Europe. In this vision, the right kind of traveller would not need to stop or wait at a border crossing, because they will have been screened in advance and they will be biometrically identified at a distance as they walk through airport corridors. The wrong kind of traveller, of course, would not be able to expect such a smooth journey.

Areas of interest

Contactless friction ridge recognition is a type of biometric technology "in which the friction ridge mark signature of a finger, palm, foot or finger-knuckle is acquired without direct contact of the relevant body part with a sensing surface, mostly employing video or image acquisition." It is not currently used for border checks, but it can allow for "person recognition at a very short distance," and in the future is expected to offer "stand-off person recognition (at a few metres' distance)".

While current face recognition technologies rely on a 'flat' photo of an individual's face, **3D face recognition** uses three-dimensional features of the human face to perform automated recognition and matching: "Once the 3D geometry of the human face is acquired, it is used to extract distinctive features on its surfaces. 3D face recognition is claimed to have the potential to achieve better accuracy than its 2D counterpart."

Infrared face recognition covers "thermal infrared face recognition and near-infrared face recognition." These use various types of infrared technologies to capture and scan individual's faces and perform biometric matching operations, for example, against an infrared image stored in a database. The study says that the technology has "impressive presentation attack detection capabilities," and infrared images are "relatively easy to capture".

Iris recognition in the NIR (near infra-red) spectrum has "impressive recognition capabilities in terms of accuracy – this modality is very distinctive." It also allows for "contactless acquisition" – that is, there is no need to touch a device to have your iris scanned. Another technology examined in the study is "iris recognition at a distance," which could be done "metres away from the subject" and "might be implemented even for a person walking."

The fifth key technology cluster, **iris recognition in the visible spectrum**, "includes iris recognition technologies based on images of the iris captured in the visible spectrum of light." The study says the technology displays "good capability readiness from 2028 onwards," but that it also has "many challenging aspects, especially in the case of individuals with dark irises (caused by higher melanin pigmentation and collagen fibrils) because the unique pattern of the iris is not clearly observable under visible light."

Like the study on AI discussed above, the project developed a "set of roadmaps" and "capability readiness roadmaps." These seek to answer three questions: "'Where are we now?' (in 2021), 'Where do we want to go?' (in 2040) and 'How can we get there?' (2022-39)." The researchers also envisaged four different potential future scenarios that may affect how biometrics are deployed for border checks, taking into account factors based on economic criteria (for example, a dynamic or slow EU economy) or conflict (a peaceful or conflictual world).

The content of the "roadmaps" indicates that the future vision is much like something out of a dystopian science fiction film. The study envisages that by 2040, "contactless friction ridge recognition" will be combined with "other solutions (e.g. facial recognition), which jointly allow seamless travel," and that "3D face recognition" will be deployed for "on-the-fly facial feature extraction and automated recognition for border checks". Face recognition technologies will also be deployed on drones. For "iris recognition in the NIS spectrum," the vision for 2040 is:

> "...the widespread use and acceptance of this technology, enhanced technical performance that enables fast processing (to obtain comparison scores), iris image acquisition at a distance and from a moving subject (allowing seamless or near-seamless border checks) and iris presentation attack detection techniques."

The report notes that "the combination of iris, fingerprint and infrared face recognition allows an extraordinary level of accuracy."

Were these plans to unfold as intended, it would undoubtedly make life easier for those granted the ability to benefit from "seamless" travel, albeit at the cost of handing over increasing amounts of sensitive personal data, and no doubt substantial payments from public funds to the private

companies selling the technology. However, in allowing an ever-increasing refinement of the methods of control and identification, these technologies will contribute to creating an experience that is far from "seamless" for those forced to make irregular journeys. The report also notes "infrared face recognition" could be used "for crowd control at mass events" or for hunting criminals and fugitives. Thus, should they be adopted and deployed, these technologies are also likely to lead to an increase in and surveillance and control far from the physical border itself.

In the meantime, some technologies are expected to come into use more quickly than others. The report argues that "3D face recognition and Iris recognition in the NIR spectrum, followed by Iris recognition in the visible spectrum, are expected to perform better than the other KTCs as they display good capability readiness from 2028 onwards."

From paper to practice

The use of "roadmaps" is standard practice in both government and business for long-term planning. Unfortunately, they do not invite any form of democratic deliberation, decision-making or public debate. If EU and member state officials have already quietly agreed to work towards the adoption of ever-more intrusive technologies in the name of automating Fortress Europe, how will those plans be taken forward and how might they be challenged?

One possibility is through the work of EU agencies and their associates in the member states. In 2019, Europol and Frontex set up the 'Future Group on Travel Intelligence' with aim of "identifying and elaborating new operational opportunities" by building on the data processing opportunities offered by the EU's 'interoperable' databases. While it has now been formally dissolved, the group proposed the establishment of a "European System for Traveller Screening" and argued that its final report "constitutes a comprehensive study material for the next decade at least, to propose improvements in relation to the future of Travel Intel and external border management."

The group's final report argues:

> "Border management should also rely on automated targeting or screening systems for performing risk management on the travellers with advance information… The experiences of border authorities outside the EU have demonstrated the operational added value of this. This would require legislative changes and most likely the use of AI to combine those sources effectively."

German MEP Cornelia Ernst, of The Left group in the European Parliament, said that "the daily lives of millions of people" should not be shaped by "agencies that long ceased to be controllable by the public and the parliament." A parliamentary question from Ernst revealed that law enforcement experts that were not "formally representing their competent authority" participated in the group, and potentially officials from intelligence services.

The final report gives limited consideration to questions of fundamental rights. Most comments relate to the accuracy and minimisation of the data (key safeguards in European data protection laws) and the lawfulness of the processing, including the prohibition of discriminatory profiling. There are no considerations of the impact on other rights, such as the challenges of interoperability and artificial intelligence for the protection of the right to an effective remedy. The plan to install a European System for Traveller Screening, however, may well be ongoing, with the possibility of a study overseen by the EU Innovation Hub for Internal Security, coordinated by Europol.

Indeed, the Innovation Hub has already undertaken work that seeks to advance some of the topics raised in the studies examined in this section. Its 2022 annual report reveals that eu-Lisa led a project under the aegis of the Hub that sought to "further investigate how AI technologies could enhance the analytical capabilities related to risk profiling/ screening rules/ risk indicators," in the ETIAS and the VIS, by exploiting the vast quantities of data stored in the forthcoming Common Repository for Reporting and Statistics (CRRS). The Hub has also played host to a project on refining the technologies to be used for capturing and storing peoples' biometric data in the Entry/Exit System, as well as the project that led to the production of the study on "biometrics for the future of travel" examined above.

A more recent study carried out by Frontex through the Hub looks in-depth at the potential of High-Altitude Pseudo Satellites (HAPS) for border surveillance, building on the identification of the technology as of "first priority" interest in the study on "weak signals" also examined above. The report concludes that "HAPS has a real potential to be a capability enabler and multiplier for the EU security ecosystem, in particular when used in conjunction with other technologies such as satellites." In fact, the technology "occupies the sweet spot between UAS [unmanned aerial systems] and satellites, leveraging the capability of being operational for longer than the former, while being cheaper than the latter."

The initial report is to be followed by another:

> "Directly following the delivery of this report, the second phase of this study will commence, focusing on specific use cases and the identified application in order to maximise the opportunities provided by HAPS solutions. As part of this exercise, the study team will identify a set of use cases across the three main categories– Earth observation, navigation, and communication – in close collaboration with Frontex and other stakeholders."

Whether the public or their representatives in the European Parliament will ever be consulted on the deployment of increasingly persistent and pervasive border surveillance technologies is an open question – but if they weren't consulted on the roadmap itself, why bother consulting them when the journey has already begun?

CONCLUSION

The development of a digital Fortress Europe reflects broader changes in economy, society and technological development in the Global North over the last three decades. The role of digital technologies has increased enormously and will continue doing so in the years to come, driven by demands for greater speed and efficiency in decision-making. Those demands are, in turn, propelled by the interests of the companies and institutions that stand to profit from the digitisation of administrative procedures, social interactions and a whole host of aspects of everyday life; and by the officials that see opportunities for perfecting systems for social management and control.

The EU's new border control strategy, published in March this year, sets out "the common European vision for European integrated border management over the next five years" (2023-27), and makes clear the key role that technology is supposed to play. One of the strategy's policy priorities deals with precisely this issue:

> "European integrated border management, especially border checks and border surveillance, should be supported by advanced, mobile and interoperable European technical systems and solutions that are compatible with large-scale EU IT systems. This is to guarantee more efficient and reliable border control. The European Border and Coast Guard should have the capacity to make best use of state-of-the-art technologies, including mechanisms to secure the data."

This and the other policy priorities included in the strategy are to be fleshed out in a "technical and operational strategy" to be adopted by Frontex, and national strategies on integrated border management will be adopted by every EU member state. The intention is to reinforce the level of coordination between EU agencies and national authorities and ensure uniform means and methods of border control across the EU, in order to "prevent and combat irregular immigration, enhance effective returns, prevent cross-border crime, and facilitate legitimate travel."

With regard to the use of new technologies for "migration management", what will this mean for individuals? As highlighted in this briefing, future developments point towards the refinement, optimisation and intensification of surveillance data collection technologies, with starkly different impacts for different groups of people.

For the "millions of bona-fide travellers" who come to the EU every year – a number that is expected to increase substantially in the future – their journeys may well become simpler, with industry and governments seeking to provide a "seamless travel experience". That experience is premised on extensive and repeated forms of digital authentication and verification. According to a senior employee at French technology company IDEMIA:

> "Through the use of remote services, travellers can start their journey from the comfort of their home. For example, they can securely complete their biometric check-in with a selfie. The app's cutting-edge software contains presentation attack detection. There is also an increasing interest in contactless biometric technologies... touchless devices can also identify travellers on the move, enabling greater efficiency and a better user experience while respecting their privacy."

The World Economic Forum, meanwhile, is advocating digital solutions:

> "A risk-based approach, powered by sophisticated AI, will require trusted, high-quality, and verifiable data across the entire traveller experience. This cannot be achieved in a system that involves manual checks of paper-based credentials... The question is not whether digital travel credentials are to be used, but how."

This is the vision shared by EU and member state officials, and indeed by states around the world, with organisations such as the International Civil Aviation Organisation, International Air Transport Association and the World Customs Organisation seeking ways to embed this approach in national planning. Whether the collection of increasing amounts of personal data, repeated biometric identification and authentication and the possibility of ongoing tracking of an individual's movements and activities – for example, through the use of AI to monitor and assess compliance with immigration rules – really amounts to "respecting privacy" is not a question raised in these accounts.

There is of course an unpleasant underbelly to these plans for technology-powered, "seamless" journeys. The French collective of undocumented people, Les Gilet Noirs, wrote in a pamphlet produced for a 2019 protest at one of Paris' airports:

> "For some Roissy Charles de Gaulle is a place for travel and consumption. Those for whom this comes easy are a minority coming from the bourgeois and/or white worlds. It's this world that colonizes and wages war. The entrance to their fortress is the airport. It is well guarded by the military, police and cameras... In this place we also meet many of our own. Nevertheless, we don't want to see ourselves here.
>
> We are hidden or shut behind a curtain in the plane or underground, very close to terminal 2 in the holding area for those who are awaiting deportation...or in the basement of the four-star Ibis hotel with the blessings of the Accor company.

This place exudes racism on a planetary scale.

Those at the front pass through showing only their official documents, those at the back are threatened, handcuffed, gagged and insulted by the police."

Work is well underway to digitise deportation procedures within the EU, the aim being to make those procedures "seamless" for the officials responsible for them. Meanwhile, police violence is rampant at the borders, being used to deflect, deter and deny entry to thousands of people seeking safety every year – with one estimate suggesting that the Greek authorities alone pushed back a minimum of 103,628 people from the start of 2019 until 1 March 2022.

Assaulting and robbing innocent people does not require the use of any advanced technology, but those technologies can and do facilitate the violence meted out at Europe's borders. Surveillance systems make it possible to pinpoint small boats or groups of people, something that should facilitate the provision of care and support – but is instead used to either intercept or ignore them.

Nowhere is this clearer than in the Central Mediterranean, where aerial surveillance footage and location data provided by people in distress is regularly provided to the so-called Libyan Coast Guard to conduct pullbacks, or simply neglected by the authorities. While the EU's border surveillance aims, in part, at "contributing to saving the lives of migrants and ensuring their protection," this lofty goal means little in a context of poisonous, xenophobic politics that sees those lives discarded.

It is evident that over the years, efforts by civil society organisations, campaigners, activists and elected officials have blunted some of the sharpest edges of new legislation, successfully calling for more limited data collection, improved privacy protection, and reduced scope. Nevertheless, the overall development of a digital Fortress Europe has not been substantially impeded, and when it comes to the increasing integration of new technologies into this infrastructure, the opportunities for public intervention appear more limited. There is no role for parliaments or the public over which technologies to develop and deploy, nor any democratic scrutiny, oversight or control of the myriad roadmaps and plans that have been drawn up. This calls for new ideas, coalitions and movements able to find effective means of challenging these developments, in order to halt further entrenchment of the surveillance, control and violence enacted and enabled by Europe's techno-borders.

Endnotes

1 Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1134

2 Eurodac, the EES, European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN) and the EES.

3 Nigeria, Gambia, Niger, Ghana, Senegal, Ivory Coast, Togo and Mauritania.

4 SIRENE stands for "supplementary information request at the national entries." Every Schengen state, as well as Europol, has a SIRENE bureau.

5 The report was published under Frontex's name, but the study was undertaken by Steinbeis 2i GmbH (S2i), with support by 4CF Sp. z o.o. (4CF), Erre Quadro S.r.l. (R2) and the Instytut Optoelektroniki – Wojskowa Akademia Techniczna (WAT).

6 DNA: DNA biometrics. Face recognition: infrared face recognition; 2D face recognition in the visible spectrum; 3D face recognition. Fingerprints: infrared friction ridge recognition; 3D friction ridge recognition; contactless friction ridge recognition; contact-based friction ridge recognition. Iris: iris recognition in the NIR spectrum; iris recognition in the visible spectrum; iris recognition at a distance. Veins: eye vein recognition; hand vein recognition. Heart signal recognition. Hand geometry recognition. Periocular recognition. Keystroke recognition. Gait recognition. Handwriting recognition. Speaker recognition.

ACKNOWLEDGMENTS

EuroMed Rights and Statewatch 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.

European
Artificial Intelligence
& Society Fund

THANK YOU !