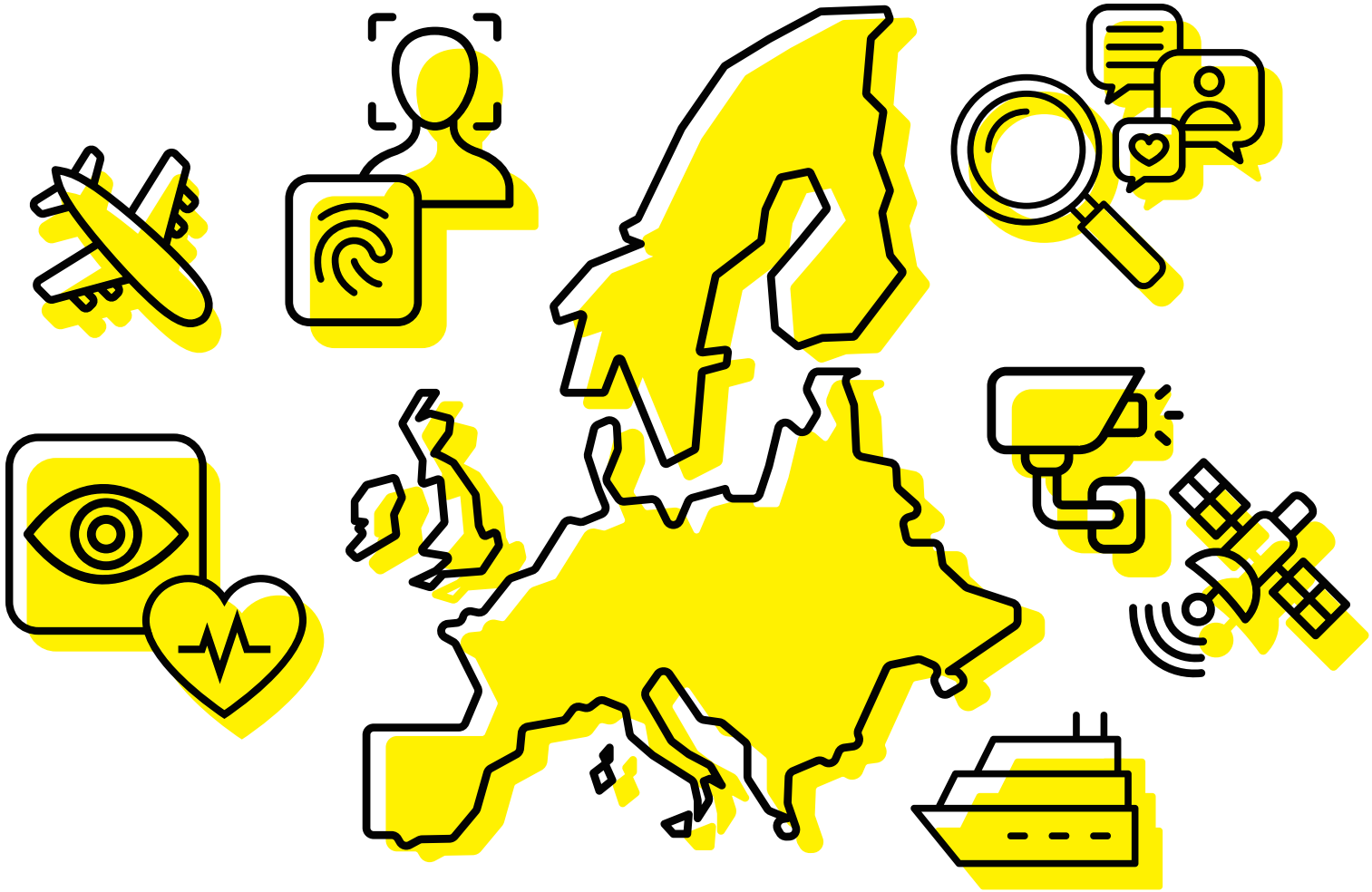
Risking Lives: Smart Borders, Private Interests and AI Policy in Europe

Philippa Metcalfe, Lina Dencik, Eleftherios Chelioudakis, and Boudewijn van Eerd



Data Justice Lab

Cardiff University / Prifysgol Caerdydd

erc

Acknowledgements

The research for this project has been supported by a Starting Grant from the European Research Council under the European Union's Horizon 2020 research and innovation program (grant agreement No 759903-DATAJUSTICE). We would also like to thank TNI, Eric Kind and Ben Hayes for earlier inputs to this report.

Contents

Executive Summary

Recent years have seen huge investment in, and advancement of, technologically aided border controls, from biometric databases for identification to unmanned drones for external border surveillance.

Data infrastructures and Artificial Intelligence (AI), often from private providers, are playing an increasingly pivotal role in attempts to predict, prevent and control often illegalised mobility into and across Europe. At the same time, the European Union is in the final stages of negotiating and adopting a final text of the proposed AI act, the inaugural EU legislation designed to establish comprehensive protections and safeguards with regards to the development, application and use of AI technology. This report explores and interrogates the interplay between smart borders, private interests, and policy surrounding AI within Europe. It does so to make apparent how the concept of 'risk' is integral to the advancement of smart border controls, while concurrently providing the framework for the governance of data infrastructures and AI. This highlights how AI is both embedded within and entrenching particular approaches to migration controls.

To understand the relationship between smart borders, private interests and AI policy, we explore four components of smart borders in Europe: the development of 'Fortress Europe' in terms of securitisation, militarisation, and externalisation; technology used in smart borders; funding and profits; and AI policy. The report demonstrates that the concept of 'risk' in the context of migration and AI is used as both a legitimisation and regulatory tool. On the one hand, we see risk used to legitimise the ongoing investment in and development of hi-tech surveillance and AI at the border to prevent illegalised migrants from reaching European territory. Here, illegalised migrants are portrayed as a security issue and threat to Europe. On the other hand, the language of risk is also adopted as a regulatory tool to categorise AI applications within the AI act. Within these policy developments, we maintain that it is essential to include an exploration of the role of private defence and security companies and, as we investigate, their lobbying activities throughout the development of the AI act. These companies stand to make huge profits from the development of smart, securitised borders, seen as the answer to the problem of 'risky' migrants. From this, we end by considering the extent to which the AI act fails to benefit and protect those most affected by the harmful effects of smart borders.

Introduction

On the 6th of February 2023 a 7.8 magnitude earthquake struck Turkey, also affecting Kurdistan and Syria, killing over 50,000 people. Whilst an outpouring of international solidarity occurred over the next days as rescue efforts were made to find survivors, EU member states were quick to discuss how the displacement of people who had lost their homes in the earthquake might impact upon the numbers of people trying to reach Europe. In the second European Conference on Border Management that took place in Athens just over two weeks later, the then Greek Migration Minister, Notis Mitarachi, stated that the wall between Turkey and Greece would be extended a further 35 km, costing 100 million Euros. He spoke of a plan to eventually extend the fence to 100km by the end of 2026[1], with more border guards deployed across the fence and further fortification with high-tech surveillance equipment including expanding the use of artificial intelligence (AI) drones and radar technology. This, Mitarachi noted, was needed to pre-empt and prevent movement across the border into Europe, in times of emergency or not[2]. The use of this tragedy by Greece to further legitimise the extension of the Evros wall demonstrates an attitude toward migration control that underlies any international aid or emergency support programme, with the mantra often being to keep the trouble out of Europe. This stance from the EU, and its member states is nothing new. Europe has long been implementing border and migratory policies that focus on externalising European borders as far south as Senegal or as far east as Azerbaijan.[3] What is novel, however, is the EU's increasing reliance on 'smart' tools and technologies in order to deter and contain those on the move from ever reaching Europe's shores.

To illustrate the growing focus on technologically aided borders over physical barriers, we can look to the plans announced by Mitarachi at the European Conference on Border Management conference. Although there has been some backing for the European Commission to fund the construction of the wall between Greece and Turkey, particularly by those 15 member states who attended the two Border Management conferences[4], in the end, Greece has had to finance the wall itself. Ylva Johansson, the EU Home Affairs Commissioner commented in January 2023, "If we were to spend money on walls or fences, there would be no money for other things"[5]. This comment may come as a surprise given the long-standing narrative of Fortress Europe, which conjures images of physical barriers at the edge and surrounding Europe to make it impenetrable. However, a comment made by Mitarachi to the press, where he stated that "some expenses for the fence's construction, such as those relating to matters of technology, can be financed by the European Union[6]", speaks to a more complex picture of what is and is not prioritised in European border controls. This comment demonstrates the prioritisation of high-tech, 'smart borders', where the funding and prioritisation of tech for border surveillance and fortification looms large as a part of the present and future of Fortress Europe. Here, technology is used to detect, categorise and surveil people, with a mind to predict movement and prevent entry to Europe, largely approached from a point of view where those trying to enter are seen as a risk to the security of Europe.

From this perspective, technology is used as a risk mitigation technique, able to identify and neutralise risk, and working to further the supposed security and safety of EU member states and their borders. Although not an entirely novel approach to controls within borders, risk-based approaches to security and migration are increasingly being utilised by both state and private entities to capitalise on the concept of risk for political and financial gains. Long before the advent of 'smart' border technologies, the EU had already implemented policies following securitisation, militarisation, and externalisation logics to safeguard its borders. Exploring the intricacies of these histories and the present and future of smart borders allows us to understand how these logics can be leveraged to advance particular interests. This includes both state and private entities who stand to benefit politically and financially from the use of these policies and technologies, whilst creating new risks for people denied free movement.

This report explores the relationship between smart borders, private interests and AI policy within Europe. In particular, it outlines how the category of 'risk' underpins both the advancement of digitalisation in border control at the same time as functioning as its regulatory mechanism. That is, the ongoing portrayal of illegalised migrants as a risk to Europe serves to legitimise harmful uses of hi-tech surveillance and AI at the border whilst risk is also used to classify AI applications within the AI act, the first piece of EU legislation that seeks to provide systematic protections and safeguards in relation to AI technology[7]. We wish to interrogate how risk is perceived in different ways with regards to AI systems and technology depending on what the purposes of the systems are, and who they are supposed to benefit and protect.

Outline of report

We begin in the first section by exploring the notion of 'Fortress Europe', presenting three key components behind the development of 'smart borders': securitisation, militarisation, and externalisation. Here, we look at the history of these developments and impact on policy. We explore how migration is increasingly portrayed as a threat to Europe, which is then used to legitimise a securitised response that sees border and migration policy turned into security matter. This impacts the ways in which borders are policed, where we see the increased use of military style controls, including the use of razor wires, hi-tech surveillance systems, armed police officers and violent pushback techniques.

We also discuss ongoing efforts to externalise the European border through the adoption of bilateral and multilateral agreements with third countries to try and prevent people from ever coming to Europe's borders. Together, these core components of Europe's border regime act to fortify Fortress Europe and pose dangers to illegalised migrants trying to cross into EU territory.

In the second section, we look at the wide array of technology used at different key points of migratory journeys: before people leave, as they approach the border, when they reach it, and after they have crossed it. This includes an exploration of technology such as AI used in early warning systems to predict movement, social media scraping, heartbeat detection, facial recognition technologies, hi-tech camps after someone has crossed into Europe, and European wide migration databases. This provides a broad overview of the landscape of the 'smart border'. We then move on to look at bordering beyond borders, and how the systematic use of technologies and databases for surveillance and risk assessment rests upon the assumption people can become predictable nodes of control. Borders thus become externalised further and further from Europe as movement can be predicted and halted in its tracks, stopped before someone ever manages to step foot on European soil.

Building on this, in the third section we consider the role of private companies in furthering this approach towards border controls. We explore the ongoing investment in innovative AI technologies at the border by looking at some key examples of previous and ongoing Horizon 2020 and Horizon Europe research projects that promise to deliver the sought-after next generation border that will be able to provide a comprehensive and omnipresent control over Europe's borders. These projects include the development of 'killer robots' in the forms of AI drones, lie-detecting avatars, AI social media scraping to interpret and influence people's perception of Europe, and various projects of creating an all-pervading holistic infrastructure of smart technologies for real time border surveillance.

The final section of the report takes a deeper look into the politics of these infrastructures, developments and research projects within the context of both policy and profit. To do so, we investigate lobbying activities by private companies in the policy process of the AI act by presenting research into meetings private security and defence companies have had with Ursula von der Leyen and other key Commissioners for the proposed AI Act, such as Margrethe Vestager, the Executive Vice-President and Commissioner for A Europe fit for the Digital Age, and Thierry Breton, the Commissioner for the Internal Market, as well as Senior Officials of their cabinets.

This is significant in relation to EU's prioritisation of innovation and market creation in AI. Finally, we present an overview of how these priorities are set out within the categories of risk in the proposed AI act and how the act leaves space for ongoing profiting of security and defence companies in the context of migration and beyond.

1. Fortress Europe: the securitisation, militarisation and externalisation of EU borders

The creation of Fortress Europe can be traced back to the Schengen agreement of 1985[8]. While this Agreement facilitated the movement of goods and people within Europe, it also stipulated stricter controls should be put in place at the EU's external borders. Since then, EU border and migration policies have been developed around four key pillars:

1. Boosting and militarising of border security at the external borders of the EU;
2. Development of 'smart borders', which aim to speed up processes for EU citizens and other wanted travellers and stop unwanted migrants through the use of more sophisticated IT and biometric systems;
3. Deportations of unwanted forcibly displaced persons, often preceded by (lengthy) detentions;
4. Externalisation of border security and border control to non-EU-countries[9].

This report focuses on the second pillar of the four areas of European border control today – the development of smart borders – and explores how policies being implemented to make Europe's border policies 'smarter' are interlinked with other European border policies that go towards making it almost impossible, legally, physically to reach European territory. A central issue that this report discusses is the onus on risk within smart borders, a factor that is mentioned in nearly all of the technologies, databases and other digital infrastructures we will explore below. To give a wider context to the development of smart borders, here we present three core components of Fortress Europe which set the stage for hi-tech, militarised border controls.

Securitisation

Securitisation is the transformation of a public policy issue into a security matter that is then integrated into a security agenda. The security of the nation-state is assumed to be at risk and therefore a securitised response is deemed necessary in order to deal with the threat posed. With regard to borders and migration, increasingly a securitised frame is being used, which assumes that those on the move represent a threat to the stability of Europe. Importantly, we need to understand securitisation as a political choice. We see this, for example, in chosen responses to boats with people capsizing and sinking in the Mediterranean Sea within a European controlled Search and Rescue Area (SAR). If Europe were to act according to the stipulations of International Maritime Law it would deploy a rescue mission and save these persons from drowning, bringing them to the nearest safe port. The EU and its member states, however, have often shirked such legal obligations and have instead chosen to act within a securitisation frame. They have made policy changes in this regard such as withdrawing search and rescue missions from the Mediterranean Sea, while criminalising civil society efforts that fill this void. Under a securitised approach, those onboard the overcrowded sinking raft are framed as posing a threat to Europe's stability and thus have systematically been left to die or pushed or pulled back from European waters to the country they had fled from.

Relatively speaking, this shift towards securitisation is a recent one. While the 2003 European Security Strategy[10] hardly mentioned migration, the topic was a prominent part of the Global Strategy document[11] setting the ground for the Common Foreign and Security Policy of the EU as presented in June 2016.[12] The shift towards securitisation has been possible because of a prevalent narrative – fuelled by the security industry as well as parts of the media – that portrays those on the move as a threat and conflates migration, crime, and terrorism.[13] One of the primary ways in which risk is invoked in the context of securitised borders is as a justification for the need for increased border security measures. Proponents of securitised borders argue that the perceived risks posed by irregular migration, terrorism, and other security threats necessitate the use of advanced technologies and stricter border controls.

Front and centre in the securitisation of Europe's borders is the border security industry, which should be understood, not as an impartial actor that is called upon to deliver neutral security services to at-risk states, but rather as actively driving the security narrative and then positioning itself as an expert upon whom the EU and its member states can rely to secure their borders. The border security industry was worth $20.63 billion in 2020 and is set to grow by 5.2% or $4.6 billion until 2026[14].

Militarisation

The logical follow-on step after securitisation is militarisation. This involves the deployment of military equipment and techniques to secure the EU's borders against the threat identified in the securitisation narrative. In militarising their borders, the EU and its member states have invested in an array of border security equipment such as concrete walls, razor wires, electric fences, watchtowers and hi-tech surveillance systems, while armed border management and police officers patrol, pushback, attack, and torture[15] those attempting to cross.

Both securitisation and militarisation have the effect of rupturing the rule of law, so that 'security' rather than law becomes the primary principle from which the use of force and coercion can proceed. Consequently, the securitisation of border controls entrenches military logics as central to the EU migration control agenda, where people seeking asylum are seen first and foremost as risky individuals to be controlled, as opposed to people at risk of harm and in need of international protection.

Globally, our world has never been so militarised with almost US$2 trillion being spent annually on militarisation.[16] It is not only a feature in border and migration policies once people are on the move; European arms are also instrumental in forcibly displacing millions as TNI documented in *Smoking Guns: How European arms exports are forcing millions from their homes.*[17]

Increased border militarisation appears to be the modus operandi of the EU and its member states as part of the securitisation logic. This is a process that began with the construction of Fortress Europe in the 1990s and has been consolidated under the so-called 'War on Terror' through the incorporation of migration control into the EU counter-terrorism agenda.[18]

Nowhere is the trend towards militarism more evident than in the unabated expanse of Frontex, whose budget has increased by 7,560% per cent since 2005 to €5.6 billion for the period of 2021-2027[19]. Part of the resources allocated to Frontex will see the formation of a standing corps of 10,000 uniformed, armed officers by 2027, with a mandate that permits them to act independent of member states and to be deployed to third countries that do not share a border with the EU[20]. In effect, this move towards border militarisation has led to the formation of a de-facto European army, which will be used to keep out those seeking protection.

Externalisation

Border externalisation involves the EU and its member states making bilateral and multilateral agreements with third countries that see them adopting border and migration policies dictated from and by Europe, typically with the aim of intercepting migrants on the way to the EU before they even reach the border. There has been a significant increase in the reliance of the EU on border externalisation measures and agreements since 2005, with a massive acceleration since the November 2015 Valletta Europe – Africa Summit.[21]

Under such agreements, the EU and its member states may, for example, provide training, equipment and funding to third countries that in effect become the border guards of Fortress Europe. They assume the task of deterring and containing migrants en route to Europe's shores, often in exchange for financial gain and/or increased surveillance, law enforcement and military capabilities. Border externalisation agreements are often negotiated with nations that were once controlled by Europe as former colonies, or with economically disadvantaged countries, and therefore negotiations rarely take place on an equal footing. There are often uneven power dynamics at play that see the EU and its member states deploy a carrot and stick approach to achieve the best outcomes for Europe.

Border externalisation can take the form of third countries agreeing to detain migrants in detention facilities funded by the EU for example, as documented by TNI in *Outsourcing Oppression: How Europe externalises migrant detention beyond its shores.*[22] The report identified 22 countries in Africa, Eastern Europe, the Balkans and West Asia where the EU and its member states fund the construction of detention centres, detention related activities such as trainings, or advocate for detention in other ways such as through aggressively pushing for detention legislation or agreeing to relax visa requirements for nationals of these countries in exchange for increased migrant detention[23].

One of the most notorious examples of the extent to which externalisation is pursued by the EU is in the deals done with Libya. Libya is not a safe country and has not been so for a very long time, where the use of systematic detention, risk of slavery, and commonplace physical and sexual violence toward people subject to controls has been well documented.[24] Yet, the EU and its member states, most notably Italy, have signed off on bilateral agreements that see the transfer of equipment, training and funds to Libya for the sole purpose of detaining and containing migrants outside Europe's shores, regardless of the torturous conditions they are subjected to while detained. [25]

Yet another example is evident in role the EU has played since 2015 in developing border controls in Niger to reduce migration across the Sahara. The funding and technical support – including the use of satellite imagery – offered by EU actors has led to "thousands of incidents of migrant deaths and disappearances have been recorded in northern Niger"[26]. Border Forensics' new report demonstrates how, after 2015 and the EU Emergency Trust Fund for Africa (EUTF) created at the Valletta Summit, provided 1.8 billion euros to stem migration before people reached Europe. The report notes how this money was used to further securitise migration controls, strengthen border mechanisms, and criminalise mobility through forcing the "migration economy underground", which in turn led to drivers taking people across the Sahara turning to more dangerous routes to evade detection and endangering those who took the journey. The impact of this, they evidence, is a huge loss of life, where people stranded in the Sahara are unlikely to survive the journey.

The securitisation, militarisation and externalisation of border control has spelled disaster for those on the receiving end of these deadly policies. Between 2001 and June 7th, 2023, at least 52,760 people have lost their lives while attempting to cross the Mediterranean Sea to Europe,[27] making it the world's deadliest border crossing. In June 2023 in Greece as many as 600 people died in one shipwreck in one of the deadliest shipwrecks in recent times[28]. The yearly number of people dying is increasing year by year as policies become ever more hostile. Out of the 48,647 people missing in the last 20 years, 26,689 of these have been recorded as dead or missing in the Mediterranean Sea[29] since 2014. Understanding that many deaths and disappearances go unrecorded, the actual figures are estimated to be much higher.

2. Fortress Europe gets Smart

2.1 Stepping up Surveillance

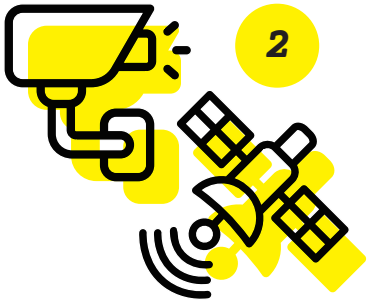
The EU already has in place an advanced technological surveillance infrastructure at internal border crossings and on its external frontiers, the goal of which is to detect mobility across borders, monitor migratory flows, and intercept and prevent people from reaching EU soil.[30] As well as this surveillance infrastructure, the EU and its Member States have deployed several tools advancing the use of big data analytics, AI, algorithms, and smart sensors, aimed at stopping people from reaching Europe and monitoring their movements both within and outside the EU. AI and big data in migration and border control can generally be divided into two categories; the use of AI to extrapolate information from large quantities of data from one or more sources/databases, and on the other hand more speculative projects where AI and big data are used for decision-making processes like AI lie detection and visa or asylum applications.[31]

A core part of Fortress Europe is composed of "virtual walls", i.e., non-physical walls compromised of high-tech surveillance that seek to restrict migrants from entering the Schengen area or to monitor their movements within it.[32] These "virtual walls' come in many shapes and forms and are increasingly becoming automated or smart. As we will show, these virtual barriers are omnipresent and those on the move are confronted with them, often unknowingly, at various stages along their migratory journey. In this sense, the increasing reliance on virtual, omnipresent borders, that expand into a space that goes far beyond jurisdiction lines demarcated on a map, means that in our daily lives we are constantly being confronted with border structures and systems. In this research we have looked at this in relation to how people's behaviour and movements are monitored at different and ongoing stages of movement:

1. Before the outset of their migratory journey before they have even departed;
2. When they are on the move;
3. While crossing jurisdictional border lines;
4. Once inside European territory.

To exemplify that borders have expanded beyond jurisdictional lines, it is worth examining Europe's 'Early Warning and Forecasting System'.

Even before people embark on a migratory journey, the European Asylum Support Office (EASO) uses its algorithmic "Early Warning and Forecasting System" to predict whether asylum requests from a particular country are likely to increase in the weeks to come. This used to be done by deploying smart technology to monitor potential migrants' social media posts, a practice which has temporarily been banned by the European Data Protection Supervisor.



Once migrants are on the move, and particularly as they come close to Europe's jurisdictional lines, their movements are monitored through aerial, maritime and ground surveillance.

When attempting to cross jurisdictional lines at regular border crossings, migrants have biometric data gathered, stored, and compared with data available across several automated and increasingly interoperable databases. At irregular border crossings tools such as automated heartbeat detection or Facial Recognition Technology may already be used to detect them.[33]

Finally, even after crossing into Europe, migrants still run the risk of being deported. Smart portable gadgets enabling the use of Facial Recognition Technology and Automated Fingerprint Identification can be used at any time at any point throughout the Union, meaning that the undocumented constantly run the risk of being detected as irregular and being deported. For example, Greece has ongoing plans to introduce the use of biometrics to identify illegalised migrants during police stops. This will be done by comparing their biometrics against those collected in the six EU databases containing information about third-country nationals that will soon become interoperable and effectively turn into a mega database conflating migration and crime.[34] There have been ongoing investigations into the lawfulness of this tactic by the Hellenic Data Protection Authority, and it is unclear if they have begun to be used on the streets. Meanwhile, in a dangerous conflation of identity control and humanitarian assistance, people have to use a biometric card for receiving basic goods such as food and clothes in Greek reception facilities[35].

2.2 Tech used

2.2.1 Before migrating or once a journey begins

Tech discussed:

- **Early Warning and Forecasting System by European Asylum Support Office (EASO)**
- **Social media monitoring by EASO**
- **Frontex social media monitoring (eventually cancelled)**

The EU uses AI to predict migratory movements even before they occur and to monitor migratory flows once a journey has begun in countries of origin many hundreds or thousands of miles from Europe. Based on the annual report of the European Asylum Support Office (EASO), the agency has developed an "Early Warning and Forecasting System" that uses machine learning tools to analyse big data on conflict and disruptive events.[36] The goal of this AI predictive tool is that the *"EU can understand and predict arrivals of third country nationals that might exert particular pressure on national asylum and reception authorities".* [37] The tool works by selecting and weighing what are considered to be push factors, such as "conflict, economic hardship, poor governance, deteriorating political situations and social exclusion of marginalized groups" and aggregating them into a composite indicator for each country. This indicator predicts how likely it is that a major group of people will migrate from a given country within the coming weeks and seek asylum in EU countries.[38] Theoretically, this information has the potential to strengthen Europe's asylum reception system, allowing for preparation in order to provide fast and effective assistance to asylum seekers. However, in reality, responses to higher numbers of illegalised migrants attempting to cross Europe's borders are often met with harsher policies and higher walls to try and prevent people entering European territory. Consequently, this tool not only provides a means of prediction, but also facilitates further avenues of preventing people attempting to move across European borders through forecasting when and where people are likely to cross borders.

The system described above is not the first to be deployed by EASO that monitors events outside Europe's borders. From 2017 to 2019, EASO monitored social media by analysing posts on platforms such as Facebook, Instagram, YouTube, and Twitter.[39] EASO used a list of keywords to identify posts related to asylum and migration routes, smuggling, and discussions among social media users on topics such as the EU asylum systems and related processes.[40]

According to the records of these data processing activities, specific profiles were targeted, such as persons belonging to the *"Arabic, Pashto, Dari, Urdu, Turkish, Russian, Tigrinya, Kurmanji Kurdish, Pidgin English, Hausa, Edo, as well as French communities"*.[41] Based on the same document, one of the reasons behind such processing activities was to monitor updates and changes in the perceptions of the EU these persons have (sentiment analysis).[42]

In 2019, the European Data Protection Supervisor (EDPS) issued a temporary ban on EASO's practices because they were not in compliance with the applicable EU legal framework on data protection.[43] The supervisor underlined that social media monitoring creates high risk for individuals' rights and freedoms since "it involves uses of personal data that go against or beyond individuals' reasonable expectations".[44] As the EU Watchdog holds, such monitoring often results in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate.[45] Lastly, the EDPS underlined that the processing of personal data from social media creates risks to the fundamental rights and freedoms of individuals, including the rights to data protection and privacy, but transcending beyond them and potentially as far as to the right of asylum. Such risks may relate to the source of information used by EASO to produce the social media reports, as well as their dissemination and use by third parties.[46] A new use case is found in Greece, where the Hellenic Coast Guard (HCG) will upgrade its operations office as part of the ISF. A 2022 tender mentions different technologies, including social media monitoring software. The software is intended to provide the HCG with the ability to analyse profiles, create network diagrams and interactive reports, archive profiles and up to second degree connections/friend lists, their gallery, timeline, and anything else shared by the user. The tender mentions that the software should simulate human activity so that the (fake) account (generated by the software) does not get suspended by Facebook, Twitter, Instagram, Telegram, Xing and VK.[47] A coalition of civil society organisations and researchers requested from the Hellenic DPA to investigate this tender call and assess its compliance with the applicable rules on data protection.[48] It was announced in May 2023 that the Hellenic DPA have launched an investigation into its use and will collect evidence to carry out a full investigation[49].

Frontex was also planning to use AI-enabled social media monitoring tools for their risk assessment practices.[50] Specifically, the Agency published a €400,000 tender in 2019, calling on private corporations to submit their applications for offering related services to Frontex.[51] However, following public scrutiny from civil society and media organisations, including Statewatch, Privacy International and Mediapart, the Agency cancelled the tender and relinquished their plans to monitor the social media accounts of migrant communities.[52]

2.2.2 Surveillance in the immediacy of the border

Tech discussed:

- European Border Surveillance System (EUROSUR)
- European Union's Earth observation programme (COPERNICUS)
- AI to be incorporated in these systems
- Frontex watchlist to be incorporated in these systems
- Common information sharing environment (CISE)

Once migrants are in the vicinity of Europe's borders, they are surveilled by an extensive infrastructure of national and EU origin. EU-wide examples of surveillance infrastructure that monitor the external borders are the European Border Surveillance System (EUROSUR) and the European Union's Earth observation programme (COPERNICUS), previously known as GMES (Global Monitoring for Environment and Security). Both systems externalise border management practices since they extend the physical jurisdictional border outwards, as satellites and drones are designed to prevent people from reaching the Schengen Area in the first place.[53] As well, the Common Information Sharing Environment (CISE) initiative is working to make EU and EEA Member States surveillance systems interoperable to share information on maritime surveillance and intervention activities[54].

Adopted in 2013, EUROSUR is a control and surveillance programme that coordinates the cooperation between EU Member States, Frontex and other EU Agencies in the field of border management. It is composed of national hubs, the National Coordination Centres, in each EU Member State, which are interconnected among themselves, and Frontex. Frontex also operates the EUROSUR Fusion Services (EFS) that support border surveillance in different ways, such as a sea vessel's recording services, drone surveillance, or satellite imagery.[55] Here is where the COPERNICUS satellite programme comes into the equation. While the astronomer Copernicus looked out into space, the COPERNICUS system is concerned with looking down to Earth, including for surveillance purposes.[56] Since 2015, the European Commission mandated to Frontex the border surveillance services of COPERNICUS, with its satellite data used for monitoring coasts from where migrants embark, gathering information on migration routes, as well as detecting and tracking vessels.[57]

Based on the data collected, Frontex publishes maps representing migration routes into the EU, updated on a monthly basis.[58] In the Mediterranean Sea, one of the world's deadliest borders, Frontex surveils the seas from the air with drones which it uses to share the location of migrants' rafts with the so-called Libyan coastguard that then engages in pullbacks.[59]

The EU envisions the promotion and incorporation of AI-oriented tools in the context of EUROSUR and COPERNICUS. Its plans have already been adopted or at least are enshrined in related policy initiatives. In 2021, the EU adopted Regulation 2021/581[60], which is already in force, providing for the automation of processing operations of satellite images in the context of EUROSUR, allowing machine-to-machine interconnections and automated decision support tools.[61] In this context, Frontex is mandated to develop a "watchlist" composed of entities, assets, behaviours or profiles, which, *"on the basis of risk analysis, are suspected to be connected with illegal immigration and cross-border crime"* in order to *"trigger appropriate reaction capabilities".*[62] As with the "Early Warning and Forecasting System", these tools have the potential to strengthen responses and provide vital services and support for people on the move. For example, these tools could be used to rapidly identify and respond to migrant boats in distress at sea. However, as the recent case of the Pylos shipwreck in Greece in June 2023 exemplifies, even when coast guards and Frontex are well aware of migrant boast at risk of shipwreck, or dangerously overcrowded, they are often too slow to act and save lives[63]. Moreover, the European Commission's coordinated plan on AI, published in 2018, envisaged the use of algorithms in COPERNICUS for big data analytics,[64] while AI-based machine learning tools are to be used primarily by Frontex and related Member State's authorities in the areas of geoinformation and earth observation under EUROSUR.[65] Members of the European Parliament recently requested more information about the use of algorithms in the context of EUROSUR and COPERNICUS for border management and security purposes, especially with regard to automated tasks related to risk detection, threat maps and maritime analysis.[66]

A further interoperable and security focused system used to surveil maritime territory is the CISE initiative, which has been an integral part of the EU Maritime Security Strategy (EUMSS) since 2014. Since April 2019, a transitional phase of the set-up has been underway, with the system set to be fully functional by December 2023. CISE is focused on "information exchange between authorities involved in maritime surveillance"[67] which seeks to enhance "border control, general law enforcement and defence" through rapid, real time sharing of classified and non-classified maritime data with different authorities to enable them to conduct missions at sea, adding to the far-reaching digital information infrastructures operating in the waters surrounding Europe.

Even though these systems claim that saving lives is one of their goals, the above-mentioned EU policies, envisaging the use of AI in the context of this surveillance infrastructure, do not make explicit arguments about the potential benefit of using these tools for safeguarding people's lives. Rather, the focus seems to be on using these technologies to prevent people from reaching EU borders by assessing "risks" and detecting migration routes, with rescue operations as the lowest priority. Such tools build upon the existing risk-assessment-based and data-driven approach towards migration. However, it has been argued that such an approach is ill-suited to encompass the complex dynamics of migration and to offer protection to vulnerable people.[68]

2.2.3. At the border

Tech discussed:

- **Automated heart detection devices deployed in border crossings in Greece**
- **Plans in Italy for updating Automatic Image Recognition System (SARI)**

Beyond the extensive use of AI in databases at regular border crossings, which will be discussed in the following section, AI is also increasingly used to detect irregular movement across borders. Surveillance towers are equipped with long-range thermal vision cameras and motion detection sensors, as well as with smart tools that enhance detection capabilities.[69]

One example is an automated heartbeat detection device deployed at border crossings in Greece.[70] Even though limited information is available in the respective website of the Greek authorities,[71] or the website of the vendor, it is understood that these portable devices utilize the properties of acoustic waves and sophisticated heartbeat sensors in order to autonomously detect the presence of heartbeats of any living creatures (human or animal) in a targeted area. As the vendor notes, this technology is used by the Border Protection Division of the Hellenic Police to detect people hidden inside vehicles, trucks, boxes and containers. The system operates 24/7 and can check four vehicles simultaneously completing its search function within a few seconds.[72] This technology is used to tackle *"the threat of illegal migration".*[73] Similar heartbeat detectors have been used in the past by border guards at border crossings points between Bulgaria and Greece,[74] while Frontex has been equipped with similar devices since 2014,[75] purchasing more in 2019.[76] It can be expected that migrants detected through these systems will be pushed back, as currently happens already on the seas[77] and at land[7879]. Technology targeting illegalised border crossings does not tackle the root causes of migration and will only serve to push migrants to take more dangerous routes to cross into the EU. Frontex aims to enhance the capabilities of sensors like heartbeat detection through AI: *"The optimal desired capability is likely to arrive in the form of an integrated system that draws on multiple sensors."*[80]

Meanwhile, Italy is planning to use facial recognition technology on migrants. The Italian Ministry of Interior published a new tender in early 2021 for upgrading the Automatic Image Recognition System (SARI), initially acquired by the Italian Police in 2017, but not active yet.[81]

The tender specifies that the system will be deployed to monitor the arrival of migrants and asylum seekers on the Italian coasts and other related border management activities. Following investigations by IrpiMedia, it was revealed that €246,000 from the European Internal Security Fund (ISF) will be used for "enhancing" the system, including the purchase of a licence for a Facial Recognition Software owned by Neurotechnology, able to process the video stream from at least two cameras and the management of a watch-list that includes up to 10,000 people.[82] The Italian data protection agency issued an Opinion about the use of SARI in March 2021, stating that the system would create a form of indiscriminate/ mass surveillance if rolled out.[83] The European Data Protection Board (EDPB), replying to a letter sent by MEP Sophie in 't Veld on this case, underlined that Facial Recognition Technology can undermine the right to respect for private life and the protection of personal data, but also other fundamental rights and freedoms such as freedom of expression and information, freedom of assembly and association, and freedom of thought, conscience and religion, while it clearly engenders wider issues from an ethical and societal point of view, especially when dealing with at-risk groups such as migrants.[84] Moreover, the EDPB stated that their common position together with the European Data Protection Supervisor (EDPS) is that a general ban should be imposed on any use of AI for an automated recognition of human features, such as faces, in publicly accessible spaces, in any context.[85] Hermes Center for Transparency and Digital Human Rights have also authored a report speaking to the dangers and violence inherent to the use of facial recognition used by Italian authorities for the detection, categorisation, and identification of migrants in Italy, highlighting the increased criminalisation, the lack of oversight by independent legal professionals and lack of transparency in regard to the algorithms used[86]. It is notable that in November 2022 the use of facial recognition technology in public spaces was banned, with the exception when used "to fight crime"[87], allowing the use of facial recognition when dealing with illegalised migration.

2.2.4. AI beyond the borders - Inside Fortress Europe

Tech discussed:

- **Smart portable gadgets enabling the use of Facial Recognition Technology and Automated Fingerprint Identification during police stops in Greece**
- **IPERION and other datafied reception systems used at camps in Greece**

Surveillance by various European governments mean that even once they are inside Fortress Europe, migrants are still likely to be targeted. Here we see the internalisation of borders inside EU territory and even inside the human body, [88] focusing on body as a definitive form of control, using surveillance technologies to detect, identify and detain people.[89]

As mentioned above, the Greek Police had planned to roll out in 2022 smart portable gadgets enabling the use of Facial Recognition Technology and Automated Fingerprint Identification during police stops[90], however it still remains unclear if they are used on the streets or not. The devices, which have gone through the last stage of development by INTRACOM TELECOM and cost €4 million (75% paid by the European Internal Security Fund – ISF),[91] will be portable. Police officers will be able to use them during police stops and patrols in urban environments to take a close-up photograph of an individual's face and collect their fingerprints.[92] The fingerprints and the photographs collected will immediately be compared with data already stored in national, EU, and third countries' databases for identification purposes, such as SIS II, VIS and EURODAC.[93] It is crucial to underline that the Greek police acknowledges that the use of the equipment will increase the average number of daily police stops as well as the "efficiency in the detection of third-country nationals who have exceeded the period of their legal residence in the country".[94] Thus, it is clear that one of the target groups of this technology are migrants. Greek civil society organisation, Homo Digitalis, claimed that the development and deployment of these devices does not comply with the applicable provisions on data protection law and filed a request to investigate the Hellenic DPA. [95] The DPA accepted the request and started an investigation on this matter, asking the Hellenic Police about the legal basis they will use for this processing activity.[96]

Moreover, the DPA highlighted that the Greek police had the obligation to conduct a data protection impact assessment prior to signing the contract in order to comply with the European data protection framework, including the data protection by design and data protection by default obligations.[97] At the time of writing, the DPA's investigation is still ongoing in close collaboration with the European Data Protection Board, so it remains to be seen whether the DPA will forbid the deployment and use of these devices in Greece.[98] These plans to use Facial Recognition Technology on migrant communities show that they are perceived as populations that can be used for data experimentation by national governments and the EU.[99] They are the most monitored groups in Europe, even though their struggles and experiences often remain the most invisible.[100] This disproportional scrutiny of their lives exacerbates existing biases, discrimination, and power imbalances.[101] Allowing this practice during police stops mean that undocumented people live in constant fear of being randomly stopped, identified and deported. In this way, migrants carry the border with them wherever they attempt to go and cannot escape it.[102]

Lastly, because of the internalisation of borders and the intrusive mechanisms used to monitor migrants within the EU, personal data can become a person's 'ticket' for receiving food, medical assistance, clothing, and other services while surviving in refugee camps and hotspots, or for being allowed to enter and exit these reception facilities.[103] Based on the country's national strategy for digital transformation for 2020 - 2025, Greece is creating a surveillance ecosystem composed of a wide set of AI-enabled intrusive tools in all the existing hosting facilities for asylum seekers (the Reception and Identification Centers (CIR), the temporary reception facilities and the Closed-Controlled Island Centers, hereinafter all referred to as "facilities").[104] The flagship of this ecosystem is "IPERION". This system will control entry and exit to the facilities via the use of a special ID card and the simultaneous use of fingerprints for biometric authentication. This special ID card will also be used for receiving food, clothing, and other supplies in the facilities, as well as for moving from one facility to another. The use of biometric and other personal data for the provision of humanitarian assistance of basic rights and daily goods for people seeking asylum have been highlighted as both extractive[105] and as a perpetuation of colonial dynamics, both through the recurrence of coloniality[106], and the entrenching of colonial power dynamics and dependency[107].

A special mobile application will also be part of this system, and asylum seekers will have to download it in order to have access to the status of their application and receive related updates.[108] This system assumes that asylum seekers have smart phones when in fact many may not, and it obligates them to use them for the purpose of proceeding with their asylum application. Via this application, asylum seekers will also be able to access a free internet Wi-Fi connection.[109] Even though there is no available information about the technical characteristics of this mobile app, it is technically possible that Greek authorities could use this mobile app to enable location tracking and/or monitoring of the internet traffic of asylum seekers, among others. In this way, personal digital devices can be weaponised for the purposes of surveilling and suppressing targeted groups.[110]

IPERION will be interconnected with other IT systems, such as "KENTAYROS" ("CENTAUR"). This is a surveillance system deployed inside and at the perimeter of all the facilities, composed of tools such as drones and smart CCTV enabling the use of Artificial Intelligence Behavioural Analytics algorithms.[111] Again, even though there is no available information about what exactly these algorithms are supposed to do in such an environment, there is potential for these surveillance tools will be used for monitoring the population's movement and behaviour within the facilities, analysing patters, predicting "risks" and signalling related alarms which effectively turns the facilities into prisons. This intrusive technology-led ecosystem that Greece is building provides the ability to identify, trace, and monitor asylum seekers, facilitating invasive surveillance of their mobility within and at the perimeter of the facilities. The Hellenic DPA started investigating the development and deployment of IPERION and KENTAYROS in March 2022, following a successful complaint that was submitted by a coalition of civil society organisations and academics.[112]

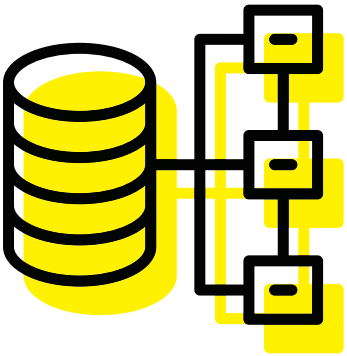
2.2.5 Databases

Six interoperable EU databases compose the "virtual walls" of Fortress Europe. Over the past years, the EU has set up these different information technology systems, while in 2019 a legal framework was adopted allowing them to become interoperable. The interoperability component risks undermining key data protection principles through the sharing of data across platforms, as will be discussed further in the following section. The use of interoperable databases also allows for the collection and processing of sensitive biographic and biometric information about migrants and travellers in a border management context. In turn, this personal data can be used to create a fixed individual identity that can be shared across European countries,[113] while different AI-empowered data processing practises, such as automated biometric identification/verification or AI-enabled profiling and categorisation, constitute key functionalities of these EU databases.

Such interoperable databases enabling the EU-wide collection, analysis, and sharing of biographic and biometric data are a clear example of the "internalisation" of border management procedures that treat the human body as a form of identification. These systems, through the use of biometric information technologies inscribe the border into the bodies of migrants, refugees and travellers themselves.[114] This means that even after crossing geographical borders and living in the EU, illegalised migrants may find it harder to evade border controls, as their body could be used to track and surveil them, heightening the risk of detention and deportation. In the paragraphs below these six databases and their interoperability components will be further analysed focusing on their scope, the data they collect, and their AI-enabled processing activities.

DATA	SIS	VIS	EURODAC	ETIAS	ECRIS-TCN	EES
DNA	Yes					
Palmprint	Yes					
Photograph	Yes	Yes				
Fingerprint	Yes	Yes	Yes		Yes	Yes
Facial Image	Yes	Proposed	Proposed		Yes	Yes
Name	Yes	Yes	Proposed	Yes	Yes	Yes
Gender/Sex	Yes	Yes	Yes	Yes	Yes	Yes
Nationality	Yes	Yes	Proposed	Yes	Yes	Yes
Date of Birth	Yes	Yes	Proposed	Yes	Yes	Yes
Travel Document Information	Yes	Yes	Proposed	Yes	Yes	Yes
Place of Birth	Yes	Yes	Proposed	Yes	Yes	

Source: European Parliament, Artificial Intelligence at EU Borders



The Schengen Information System II (SIS II)

Scope

SIS was originally established in 1995, to be updated in its second generation (SIS II) first in 2013 and then again in 2018. The provisions of the 2018 package of SIS II Regulations,[115] and became fully operational on the 7th of March 2023, being *"enhanced to include new categories of alerts, biometrics such as palm prints, fingermarks, and DNA records for missing persons, and additional tools to combat crime and terrorism"*[116]. It is the largest IT system in Europe and is operational in 26 EU Member States (Cyprus is not connected to it),[117] and four Schengen associated countries, namely Switzerland, Norway, Liechtenstein and Iceland.[118] The system constitutes a core part of the 'virtual wall', seeking to control, monitor and surveil the movements of third country nationals in the Schengen area.[119] SIS II is governed by three different EU Regulations, each of them covering a different procedure, namely (a) placing and processing alerts in respect of third-country nationals subject to return decisions,[120] (b) placing and processing alerts for refusing entry or stay of third country nationals in the Schengen area,[121] and (c) placing and processing alerts for persons or objects for the purpose of police and judicial cooperation. For only this latter category, the persons covered by the alerts can be both third country nationals and EU citizens, who are wanted persons for arrest, surrender and extradition purposes, missing persons or vulnerable persons who need to be prevented from travelling.[122]

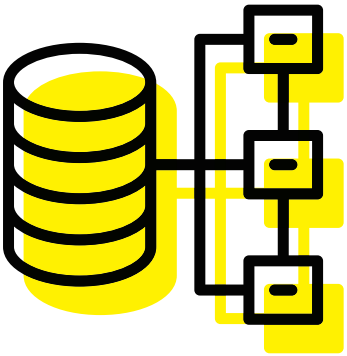
Data Collected & AI-enabled processing activities

More than twenty-five data categories reflecting a wide variety of biographic and biometric data are collected in the context of these three 'watchlists', such as full names, place and date of birth, gender, facial images, fingerprints, or even palm prints of the individuals concerned by these alerts. DNA profiles are also included in the system for SIS alerts on wanted persons, missing persons, or vulnerable persons.[123]

The collection of these categories of data is interrelated to the use of AI tools in the context of SIS II alerts. Specifically, already since 2013 authorities could use biometric data stored in SIS to verify the identity of a person when an alphanumeric search (search query based on name, surname, date of birth etc.) produced a hit.[124]

This process is called "Biometric Verification" (also known as "one-to-one matching") and enables the automated comparison of two biometric templates, usually already assumed to belong to the same individual.[125] However, from 2018 onwards authorities are able to use biometric data stored in SIS to also identify a person, thanks to the introduction of the Automated Fingerprint Identification System (AFIS) in SIS II operations.[126] AFIS is a biometric identification tool that uses digital imaging technology to obtain, store and analyse fingerprints' templates aiming at uniquely identifying a person.[127] This process is called "Biometric Identification" (also known as "one-to-many matching") and allows for comparing a person's biometric data collected on the spot to many other biometric data templates stored in a database.[128] For example, in this way authorities are able to collect the biometric data of an unidentified person during a police check, and compare this data to SIS II in order see whether their fingerprints match a template already stored in this database.[129]

The provisions of the SIS II Regulations allow the implementation of biometric identification of individuals based on Facial Recognition Technology, too. Specifically, it is clearly stated that facial images and photographs can be used to identify a person in a border management operation as soon as it is technically possible provided that the technology has reached a sufficient level of readiness and availability, while the European Commission was mandated to present a report on this matter.[130] This report was published in 2019 concluding that Automatic Biometric Identification System-Face (ABIS-Face) technology can be integrated in the SIS II.[131] Even though the legislation determines the use of this technology first in the context of border crossing, the study also notes that in the near future its use will be possible in the context of police and judicial cooperation.[132] Experimenting Facial Recognition Technology with third country nationals first is another example of how the use of migration management technology renders certain vulnerable communities as technological testing grounds.[133] Further risks involved relate to the accuracy of the facial recognition, such as the possibility of a false positive, where the system indicates a match incorrectly. This is further explored in the EURODAC section below.



The Visa Information System (VIS)

Scope

VIS became fully operational in 2011, allowing Schengen countries[134] to process applications for short-stay visa (or transit) in the Schengen Area, exchange data, and facilitate visa checks at border crossings.[135] In 2018, the European Commission put forward a proposal for updating VIS aiming at expanding its scope.[136] The proposed rules were adopted in 2021, with Regulation 2021/1134,[137] reforming and updating the VIS, and Regulation 2021/1133 setting the conditions for VIS' interoperability with the rest of the EU IT systems in the field of migration and border control.[138] The scope of VIS is now extended to cover also long-stay visas and residence permits, facilitating the exchange of data between EU Member States on related applications and decisions.[139]

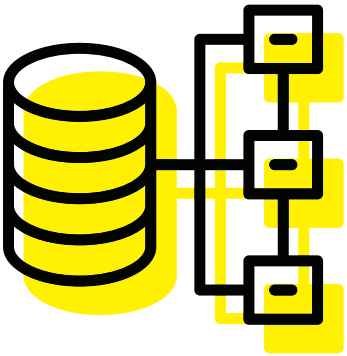
Data Collected & AI-enabled processing activities

Different categories of biographic and biometric data are collected in the context of revised VIS rules. The system stores all ten fingerprints and a facial image of the visa applicants/holders, as well as biographic data included in their travel documents.[140]

Automated biometric identification was used in the context of VIS based on the fingerprints collected, even before the revision of its rules . Specifically, the Biometric Matching System (BMS) of VIS allows border authorities to perform identification and verification tasks regarding third country nationals.[141] For example, visa applicants' fingerprints are checked with VIS during the application procedure and are verified against the database for possible duplicates, while fingerprint searches in the VIS are carried out at the EU external borders for verification and identification purposes. In 2019, 7 million biometric searches were performed, and 17 million biometric authentications took place, the latter mainly at border posts.[142]

Additionally, the use of Facial Recognition Technology for biometric matching is now allowed following VIS' revisions. More precisely, the facial images collected shall have sufficient image resolution and be of sufficient quality to be used in automated biometric matching in accordance with the international standards as set out in the International Civil Aviation Organization (ICAO).[143]

In the context of AI-enabled profiling, the older legal framework of VIS did not provide for automated profiling tasks. Nevertheless, a related study funded by the European Commission and conducted by Deloitte had indicated a number of "opportunities" for incorporating AI technologies in VIS functionalities, especially in the context of automated risk assessment of individuals and automated identification of irregular travelling patterns, used mostly to identify terrorist suspects, for example if a person has a perceived illogical layover.[144] The revised rules on VIS allow for algorithm enabling profiling based on specific risk indicators, which are a combination of data including one or several of the following information from the visa applicant: (a) age range, sex, nationality; (b) country and city of residence; (c) the Member States of destination; (d) the Member State of first entry; (e) purpose of travel; (f) current occupation (job group).[145] Such risk indicators shall, in no circumstances, be based solely on a person's sex or age or on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation.[146]



The European Asylum Dactyloscopy Database (EURODAC)

Scope

EURODAC became operational in 2003, being the first IT System allowing for the storage of fingerprints in an EU-wide database on short-stay (Schengen) visas. It determines the Member State responsible for examining applications of a third country national or a stateless person who has made an application for international protection.[147] EURODAC is currently under a revision process, with the suggested provisions expanding its application to controlling secondary movements of third country nationals in an irregular situation, too.[148] Secondary movements *"occur when refugees or asylum-seekers move from the country in which they first arrived to seek protection or for permanent resettlement elsewhere."* [149]

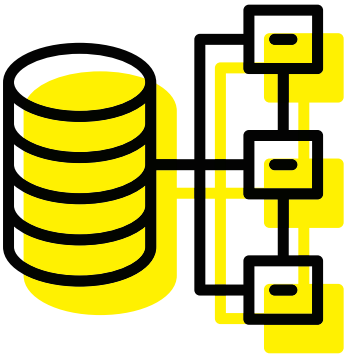
The proposed revisions provide for the interaction of EURODAC with other EU IT Systems in asylum, return and resettlement procedures. In this context, EURODAC will be used, among others, for controlling migration flows and detecting secondary movements of third country nationals in an irregular situation(being a refugee or asylum seeker is considered an 'irregular situation'), "complementing" the profiling objectives of the European Travel Information and Authorisation System (ETIAS).[150] If the proposal is adopted, EURODAC will be transformed from an information system of limited aims and capacities into a support tool for a range of EU policies on asylum, resettlement and irregular migration.[151] The EURODAC system reportedly has at least 10 false positives per year resulting in wrongful deportation.[152]

Data Collected & AI-enabled processing activities

Under the current legal regime, the data collected in EURODAC is limited. Specifically, applicants of international protection provide to the system their fingerprints (all of the fingers or at least the index fingers), and their sex, as well as some information about their application.[153] Moreover, currently, EURODAC stores the fingerprints of third-country nationals or stateless persons found crossing the external border in an illegalised manner. Authorities may also fingerprint third-country nationals or stateless persons found irregularly staying in a Member State, but in contrast to the first two categories, registering their fingerprints is currently not mandatory.

However, the numbers indicate that collecting and storing fingerprints of third country nationals or stateless persons found staying irregularly in a Member State is also common practice. Specifically, Member States transmitted a total of 644,926 sets of fingerprints to EURODAC during 2020.[154] Out of these, 62% represents fingerprint data sets of applicants for international protection, 25% represents fingerprints of a third country national or a stateless person, who is found irregularly staying within a Member State's territory, and 13% refers to fingerprints of a third country national or a stateless person, found irregularly crossing external borders. Nevertheless, the new proposal, if adopted, would introduce a mandatory requirement also to collect and store fingerprints of third country nationals or stateless persons who have been found irregularly staying on EU territory.[155] Moreover, the amount of personal data collected will be radically increased. More precisely, the proposed provisions will allow for the collection of a wide variety of biographic and biometric information on top of those collected already, such as facial images, names, date and place of birth, nationality, and more.[156]

The use of Artificial Intelligence (biometric identification and verification) was already implemented in EURODAC since its rollout in 2003, for searching and matching fingerprints existing in the database.[157] The proposal put forward by the European Commission enables the use of Facial Recognition Technology to identify people based on the facial images that will be collected in the system, too. However, the European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), will have to carry out a study on the technical feasibility of implementing face recognition technology in EURODAC, before such tools are deployed in practice.



The European Travel Information and Authorisation System (ETIAS)

Scope

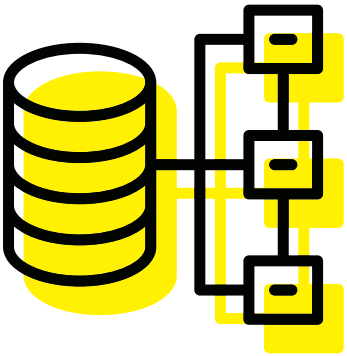
ETIAS was established in 2018[158] and is expected to become operational in 2024, being pushed back several times[159]. This database is another example on how the EU treats people who plan to travel to Europe as risk factors that must be calculated, profiled, and categorised. The official language in the text of the ETIAS Regulation states that the scope of the database is to assess *"whether the presence of… third-country nationals in the territory of the Member States would pose a security, illegal immigration or high epidemic risk."*[160] It requires all visa-exempt travellers from non-EU countries to obtain authorisation prior to their departure through an online application form. In simple terms, the ETIAS system will function like the ESTA scheme in the U.S.A., requiring people coming from non-EU countries that do not need a visa to travel to the EU, to acquire a travel authorisation.[161][162]

Data Collected & AI-enabled processing activities

The ETIAS database will not store any type of biometric information, like fingerprints or facial images, of the visa-exempt travellers. However, different data categories will be collected such as the applicant's surname, nationality, country and city of residence, home address, email address and telephone number, educational status (primary, secondary, higher, or non), or current occupation (job group). Moreover, the applicants will have to answer specific questions such as whether they have stayed in a specific war or conflict zone over the previous 10 years and the reasons for their stay.[163]

Even though automated biometric identification technologies are not part of the ETIAS system, the use of AI tools is still prominent. The ETIAS Regulation provides for the establishment of automated profiling tools, namely the ETIAS "screening rules" complemented by the ETIAS "watchlist".[164] More precisely, the ETIAS screening rules constitute an algorithm-enabled profiling practice system that examines applications of visa-exempt third-country nationals to assess whether these applicants could pose – what EU calls – a *"security, illegal immigration or high epidemic risk".*[165]

The algorithm compares the individual profile of a traveller with a set of specific risk indicators established by the ETIAS Central Unit, which is part of Frontex. Three years after the start of operations of ETIAS and every four years thereafter, the Commission shall evaluate ETIAS, including its screening rules used for the purpose of risk assessment. These risk indicators are composed of a combination of data including age range, sex, nationality, country and city of residence, level of education and current occupation (job group). Such data can be used as a proxy for revealing sensitive information about individuals or their socioeconomic status. For example, it is widely accepted that information associated with an individual's place of residence, such as a home address, could be used to construct proxies for race and ethnicity based on the distribution of race and ethnicity within a particular geographic area.[166] Moreover, information about a person's educational level or current occupation could be used as a proxy for inferring the socioeconomic status of a person.[167] Such database systems are enhancing the powers of EU and Member States to exclude certain people for being authorised to travel to the Schengen Area, and they expand control over the mobility of "unwanted" and "undesirable" populations. At the same, this migration management procedures perpetuates the sorting and categorising of third country nationals into more and less desirable types of travellers,[168] based on their perceived wealth and ethic profile.



The European Criminal Records Information System that concerns Third Country Nationals (ECRIS -TCN)

Scope

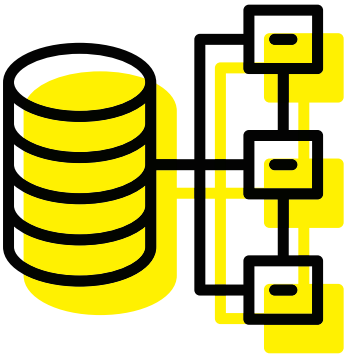
ECRIS-TCN was established in 2012 providing for the decentralised exchange of criminal records information among EU Member States. Additionally, in 2019 a new Regulation was adopted establishing a centralised version of the ECRIS-TCN system that will be operated by the EU Agency for large-scale IT-systems (eu-LISA) and will become operational in 2023.[169] This database allows for the exchange of criminal records on convicted third-country nationals and stateless persons in EU Member States for the purpose of identifying the Member States where such convictions were handed down.[170] The provisions of ECRIS-TCN also cover EU citizens who hold a nationality of a third country and who have been subject to convictions in a Member State.[171] The Meijers Committee highlighted that the inclusion in ECRIS-TCN of EU citizens who hold a nationality of a third country has negative effects on the equal treatment of EU citizens of immigrant origin, since the overwhelming majority of Union citizens who also hold the nationality of a third country are immigrants themselves or (grand)children of immigrants.[172]

Data Collected & AI-enabled processing activities

Both biographic and biometric data of convicted third-country nationals, stateless persons, and EU citizens who hold a nationality of a third country and who have been subject to convictions in a Member State are stored in the context of ECRIS-TCN. This data includes categories such as full names, place and date of birth, nationality, gender, ID numbers, as well as fingerprint data that have been collected in accordance with Member State's law during criminal proceeding.[173] Facial images of the convicted persons will also be stored in the system, if the law of the convicting Member State allows for the collection and storage of facial images of convicted persons.

When it comes to the use of AI tools in the context of ECRIS-TCN, Automated Fingerprint Identification is allowed already by the ECRIS-TCN Regulation. Facial recognition technology may only be used for automated authentication purposes, namely, to confirm the identity of a person who has been already identified because of an alphanumeric search (search query based on name, surname, date of birth etc.) or a search using fingerprint data.

However, according to Article 6 of the ECRIS-TCN Regulation the European Commission is empowered to adopt a delegated act (a non-legislative act that supplements EU legislation) concerning the use of facial images for automated identification purposes when it becomes technically possible. Before exercising this empowerment, the European Commission shall consider the necessity and proportionality principles, as well as technical developments in the field of facial recognition software in order to assess the availability and readiness of the required technology. The same approach was used for the adoption and use of Facial Recognition Technology in other EU databases, such as SIS II.



The European Entry/Exit System - (EES also known as Smart Borders System)

Scope

The EES was established in 2017[174] and is anticipated to become fully operational at the end of May 2023[175] . It records and stores the date, time and place of entry and exit of short-stay visa holders and visa-exempt travellers crossing the EU borders.[176] The system aims at replacing the passport stamp procedure, allowing the processing of biometric data of individuals. The EES will also calculate the duration of the authorised stay and automatically generate alerts for "overstayers" when such an authorisation has expired.[177] National law enforcement authorities and Europol will be able to access the EES.[178] Statewatch has noted how the EES will likely require substantial additional investment in personnel and infrastructure to track down and deport people, while the proportionality of the system itself is questionable, *"given the estimate that just one in every 1000 people who legally enter the Schengen area will 'overstay'"*[179]*).*

Data Collected & AI-enabled processing activities

The categories of personal data collected are both biometric and biographic, namely surname, date of birth, nationality, sex, number of travel document, a facial image and fingerprint (the latter only for visa-exempt third-country nationals).[180] AI tools such as the Automatic Fingerprint Identification are already allowed under the current rules. When it comes to the use of Facial Recognition Technology, border authorities are allowed to use the fingerprint data combined with the facial image collected for identifying any third-country national who may have been registered previously in the EES under a different identity or who does not fulfil or no longer fulfils the conditions for entry to, or for stay on, the territory of the Member States. In 2019, the Commission adopted specifications for the quality, resolution and use of fingerprints and facial images for biometric verification and identification in the EES.[181]

2.2.6 Databases become interoperable

In 2019, the EU adopted two Regulations putting in place a legal framework mandating the interoperability of the six databases described above.[182] The goal is to implement this overarching EU system that interconnects data from the six existing databases by the end of 2023.[183] However, even though the European Commission attempts to present interoperability as the ultimate component of already fully functioning databases, this is not the case since many of these databases are not yet fully functional. [184] As noted above, the updated version of SIS II was implemented in March 2022, the EES is expected to be implemented by the end of May 2023, ECRIS-TCN and ETIAS will become fully operational by the beginning of 2024,[185] the new rules on VIS are expected to be applied only from 2024,[186] while the EURODAC regulation is currently under a legislative revision process.[187] Moreover, as the Council of the EU notes, some Member States still face considerable risks of delays compared to the agreed implementation timeline,[188] while further delays could be triggered by the ongoing legislative reforms.[189]

The interoperability Regulations build upon the AI tools used in the context of each EU database, enabling further the automated comparison between personal data recorded in these databases with a person's biometric and/or biographic data. There exist four technical interoperability components:

a. The European search portal (ESP): When competent national and EU authorities are unable to identify a person or have doubts about the identity provided, they will be able to launch a query by submitting biographic or biometric data to the ESP. Once a query has been launched, the ESP will search all the six databases simultaneously to obtain a match-flag type of response indicating whether data related to the query are recorded in the aforementioned information systems. The use of the ESP is reserved for Member State's authorities and EU Agencies that already have access to at least one out of the six EU databases.[190] In this way, data from the existing databases will become searchable for a wider number of authorities, many more than those originally mandated to process the data by the existing legal frameworks.[191] For example, police authorities that had access to SIS II or ECRIS-TCN will now be able to make queries and search other databases too (that were not originally established for purposes of prevention, detection or investigation of crime), expanding their powers and control over vulnerable populations such as migrants, refugees and asylum seekers.

b. The multiple-identity detector (MID): MID creates and stores identity confirmation files, containing links between data in the six databases allowing detection of multiple identities in these systems.[192]

c. The common identity repository (CIR): CIR creates an individual file for each person that is registered in the EES, VIS, ETIAS, EURODAC or ECRIS-TCN. The file contains an individual's full name, date of birth, place of birth (town and country), nationality, gender, previous names, and travel document information.[193] CIR enables queries via ESP by using the biographic information of a person,

d. The shared biometric matching service (sBMS): The sBMS stores biometric templates, a reference to the EU information systems in which the corresponding biometric data are stored and a reference to the actual biometric records in those EU information systems. The sBMS enables queries via ESP by using the biometric information of a person.

Irrespective of the abovementioned delays, the interoperability framework of the EU databases constitutes another building block towards the internalisation of EU border checks. One of the main official objectives of these Regulations is to contribute to the prevention, detection, and investigation of terrorist offences and serious crime. However, most of the people that are included in these databases, such as VIS, ETIAS, EURODAC, and EES have no established connections to illegal activities. The only common denominator of these individuals is that they are third country nationals.[194]

The European Data Protection Supervisor (EDPS) has stated that these developments pave the way to the "point of no return". That is, the ongoing attempts to create streamlined and interoperable databases to collect, store and process third country national's data, alongside the use of AI enabled automated profiling and identification, see the creation of new centralised mega databases which poses serious risks to fundamental rights that will not be easy to undo. The centralised storage and sharing of millions of migrants' biographic and biometric data can be used to identify, profile, detain, and deport people. Not only do these developments further expand control over migrant populations through a high level of technological surveillance, but the EDPS has highlighted that they risk becoming *"a dangerous tool against fundamental rights"*, with potential for misuse, and ultimately demonstrates political as opposed to merely technical choice.[195]

In addition, the EU Agency for Fundamental Rights (FRA) has highlighted that the interoperability framework raises important challenges for data protection, such as the principles of purpose limitation and data minimisation, while it blurs the boundaries between migration management and the fight against serious crime and terrorism.[196] Moreover, FRA has underlined that the data protection authorities of the Member States are gaining more and more responsibilities in the context of the interoperability framework, but their budget remains limited. This could challenge the successful conduct of their supervision powers, undermining the principle of lawfulness of the processing of personal data.[197] Another EU expert body, the then Article 29 Working Party on Data Protection (A29WP),[198] had sounded the alarm about this interoperability framework, too. Specifically, the A29WP underlined that this framework raises fundamental questions regarding the purpose, necessity and proportionality of the data processing activities involved as well as concerns regarding the principles of purpose limitation, data minimization, data retention and clear identification of a data controller.[199] Furthermore, civil society organisations, such as the European Digital Rights (EDRi) network and the Refugee Lab have highlighted that the interoperability framework provides an enabling infrastructure for many automated decision-making projects with harmful implications, while the development and deployment of migration management is ultimately about decision-making by powerful actors on communities with few resources and mechanisms of redress.[200]

2.2.7 The externalisation of fortress Europe

The EU has a wide array of migration deals with third countries, including deals with Niger to Morocco, Libya, Turkey, Bosnia and Herzegovina[201] all geared to the prevention of migration from those countries to the EU. Conceived as "buffer States" to a "Fortress Europe" approach, these initiatives now stretch much further afield to countries of origin and transit of migrants in Southern Africa and Europe's "Far East".[202]

The European Border and Coast Guard Agency (Frontex) has signed more than two dozen working arrangements with non-EU states, regional bodies and international organisations, permitting cooperation on training, information-sharing, joint operations and assistance in the implementation of border control strategies and technologies.[203] The New EU "Neighbourhood, Development and International Cooperation Instrument – Global Europe" (NDICI) establishes priority areas and specific objectives for most neighbourhood partners, countries and regions of the EU, merging several former EU external financing instruments together.[204] For the period 2021-2027, some €8 billion, will be allocated to actions supporting management and governance of migration.[205] Billions more will come from the EU Trust Fund for Africa (EUTF for Africa, further described below), which allocate national development funding to migration management needs in EU partner countries.

All of this funding should also address "the root causes of irregular migration and forced displacement",[206] and be "implemented in full respect of international law, including international human rights and refugee law".[207] Despite these pledges, these programmes are steadfastly predicated on migration control, and have frequently been associated with push backs, border violence and internal repression perpetuated by national State agencies, and shrouded in complexity and secrecy.[208] The EU has also invested heavily in security research and migration control technology, and a number of its Member States are among the world's largest security technology exporters. According to *Privacy International,* Europe's "war on migration" is now firmly driving the spread of surveillance technology around the world.[209]

One of the key trends in the externalisation of the EU's borders is the redirection of development funding towards migration control.[210] The EU Emergency Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa (EUTF) was established in 2015 to support the implementation of the Joint Valetta Action Plan (JVAP) on enhancing collaboration and exchange of technologies between African and European countries in the field of migration.

The key priorities of the EUTF include, *inter alia*: the prevention of irregular migration through capacity building and provision of relevant equipment to law enforcement and border management authorities in African countries; the improvement of border management systems, including intelligence gathering and sharing; and the establishment of civil registry and biometric identification systems.[211] Although not an explicit priority, discussions among EU Member States suggest that Trust Fund budgets should be aimed to those countries and regions most closely associated with irregular migration via the Mediterranean.[212] To date the EU has pledged €5 billion in funding to projects in 26 partners countries across North Africa, the Sahel and Lake Chad and the Horn of Africa.[213]

Because the EUTF is a crisis funding instrument, normal EU public tendering rules are circumvented, with financing going directly from the 26 EU Member States to the projects in the target countries.[214] As well as repurposing development funding to migration control[215], the structure of the EUTF diminishes transparency and accountability, with in-depth investigations at national level required to understand what has been funded where. A study commissioned by the European Parliament recommended wholesale changes to the operation of the EUTF, including improvements in "democratic accountability, fundamental rights and rule-of-law impact assessments".[216]

Projects funded by the EUTF include €28 million for a biometric identity system in Senegal,[217] a collaboration between the Belgian Development Agency and the French company Civipol (see Section 6).[218] The same company is involved under the EUTF in projects for the establishment of civil status registry systems in African countries such as The Ivory Coast (€5 million)[219] and Mali (€25 million),[220] as well as in training/capacity building programs in Senegal, Burkina Faso, Mali, Mauritania, Niger and Chad (more than €100 million in total).[221]

The long-term goal of some EUTF projects involving biometrics and digital identity appears to be to establish systems that allow for some level of interoperability with EU databases,[222] which would in turn facilitate the return of unwanted migrants from Europe to Africa.[223] If this goes ahead it might mark a significant expansion of the border externalisation of the EU and a change in the nature of the migration control regime. Notably, coup d'états have taken place in Burkina Faso[224] and Guinea,[225] major EUTF recipients, as well coup attempts in other recipient countries. It is currently unclear what this has meant for EUTF funding, but it does underline the dangers of this strategy, as new regimes come into power that might use the biometric digital identity and surveillance technologies for suppressing their own populations.

3. Funding and profiting from smart borders

Private military and security companies have come to play an essential role in shaping EU policy and in providing a variety of surveillance tech and risk assessment services.[226] The Border War Series produced by TNI has provided detailed research and analysis on how immigration and border management have become a multibillion-dollar business in the EU and other parts of the world.[227] Market research agencies predict annual growth of the border security market of between 7.2% and 8.6%, reaching a total of $65–68 billion by 2025. The largest expansion is in the global Biometrics and Artificial Intelligence (AI) markets. The biometric systems market itself is predicted to double from $33 billion in 2019 to $65.3 billion by 2024, with biometrics for migration purposes being a significant sector, while the AI market will equal US$190.61 billion by 2025.[228] As people are pushed towards ever-more deadly routes to reach Europe and avoid detection, military and security companies continue to win contracts to provide 'smart' equipment to border guards, the surveillance technology to monitor population movements, and the database infrastructure to register, identify and track migrants.[229]

According to the United Nations Working Group on the use of Mercenaries, a large number of EU and non-EU corporate actors have strategically positioned themselves to benefit from the aforementioned security approaches to migration and the corresponding hikes in public budgets for border security.[230] By taking advantage of their expertise on new technologies, these for-profit private actors significantly influence the design and implementation of EU policies in the field of border management, creating a self-fulfilling loop of public demand and private supply of 'smart' tools funded with EU money, a *"spider's web of trust and influence"*.[231]

A recent investigation conducted by the Corporate Europe Observatory on the European Border and Coast Guard Agency (Frontex) reveals a trend by which security and defence companies are being given an *"outsized role – unmatched by other voices – in shaping EU's border control regime".*[232] These corporate actors do not participate as neutral parties in the respective policy debates but aim, by default, to influence EU's approach to border control based on their own interests in order to benefit from procurement contracts, while at the same time civil society organisations working to defend human rights are left out of these discussions.[233] Moreover, revolving door scandals are emerging, with ex senior EU officials recruited to key positions by private security and defence companies, such as the case of the European Defence Agency (EDA) Chief Executive, Jorge Domecq, who left EDA to join Airbus Defence and Space six months later as Head of Public Affairs and Strategic Advisor.[234] As the European Ombudsman ruled in this case, when a senior public official moves to the private sector this could give rise to: "*(i) risks of a conflict with the legitimate interests of the EU; (ii) risks that information that is not public may be disclosed or misused; or (iii) risks that former staff members may try to influence ex-colleagues, who, in the case of departing senior staff are likely to have been their subordinates, in favour of their new employer".*[235]

Revolving doors cases happen in reverse too, when senior officers of companies join EU bodies. For example, the current European Commissioner for the Internal Market, Thierry Berton, who holds a key position when it comes to policy decisions around the EU industries, was working until his nomination as a CEO of Atos with a broad portfolio, including significant work in the field of defence and border security.[236] The Corporate Europe Observatory, further reflects upon revolving-door cases by noting that private actors are trying to benefit from insider access and know-how in order to gain more influence and contracts with EU in the field of border management, among others.[237] Compounding on that has been the numerous criticisms on Frontex itself, with director Fabrice Leggeri stepping down in April 2022 amid widespread criticisms of Frontex complicity in, and cover-up of, illegal pushbacks in the Aegean Sea, the incorrect use of funds, preventing the hiring of 40 fundamental rights officers and misleading the European Parliament.[238]

The EU has several funding mechanisms for research relevant to borders, the largest beneficiaries of which are security and military companies. A recent report from Statewatch identifies that between 2014 and 2022 alone, more than €250 million of EU funds was given to research and develop technologies for border control, with the next funding cycle (between 2021 and 2027) seeing a 94% increase in allocated funds the development of border technologies[239]. Within these funding streams, two trends are clearly discernible: One, a growing focus on research concerning the securitisation, militarisation, and externalisation of borders that mirrors the policy trends described above, and two, an increasing share of funding going to research concerning 'smart' border technologies. The first trend is exemplified by the €8bn European Defence Fund (EDF), a military research funding for the period 2021-2027. It replaces the Preparatory Action on Defence Research and European Defence Industrial Development Programme (2018-2020), albeit with a budget that has grown by 1490%. In 2017, the Transnational Institute reported on the development of the EU security-industrial complex and the market forces at the core of the increasingly central lens of 'security' as *"default response to complex social and ecological crises"*.[240] The report noted how in research funding the lines between civilian and military technologies are deliberately blurred. The same is true for research on smart technology. These trends are exemplified in the six case studies of Horizon 2020 and Horizon funded EU research projects which we explore below.

ROBORDER

The project ROBORDER (autonomous swarm of heterogeneous RObots for BORDER surveillance)[241], completed in 2021, received around €9 million in EU Horizon 2020 funding. The project *"aims at developing and demonstrating a fully-functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles, capable of functioning both as standalone and in swarms, which will incorporate multimodal sensors as part of an interoperable network."*[242] In 2019, the Intercept reported that the project's developers *"say the robots will be able to identify humans and independently decide whether they represent a threat"* and that *"Roborder's developers acknowledge that parts of their proposed system involve military technology or could easily be converted for military use."*[243] This conversion to military use is not difficult to imagine; beyond apparent plug-and-play surveillance capabilities of the project, the technologies developed under ROBORDER are an EU-funded first stepping stone towards developing 'killer robots'.

There are several AI-aspects to the project, but most directly it concerns AI-based decision-making in detection capabilities and the autonomous differentiation between 'friend' and 'foe', as well as the ability to operate in 'swarms'. Swarms are defined by *"the ability of drones to autonomously make decisions based on shared information"*[244]. As increasing numbers of unmanned vehicles appear in warfare and beyond, it becomes challenging to let humans operate them. Autonomous swarms allow for increasing the use of unmanned vehicles further and developing novel strategies. One of the three pilot use cases of the project is the 'Early identification and tracking of illegal activities', including detecting unauthorised sea and land border crossings. The project website strongly emphasises 'illegal smuggler' activity, in other words – refugee and migrant crossings of the Mediterranean and EU external borders are likely to be the main future use case. While the project's trials took place at the borders of Portugal, Hungary and Greece, its outcomes will reach far beyond borders, with (parts of) the technology being sold in- and outside Europe.[245] An EP requested study noted that deliverables surrounding ethics are 'fully confidential' and are not accessible even partially,[246] questioning democratic oversight.

While the stated aim of the ROBORDER project is to enable better surveillance of borders and the robots are not equipped with weapons, the lines between ROBORDER's goals of developing technology that is nonlethal and 'killer robot' applications are not set.

Once autonomous border surveillance is a reality, adding weapons will not be difficult. Borders are by no means the only intended contexts these technologies are developed for; they are the context in which the EU funds their development. The 2014 TNI report Eurodrones Inc. noted the drone industry's controversial rise within the EU, finding that 314 million euros in research funding was awarded to military and defence contractors for border surveillance and law enforcement and that drones were the direction of travel in border control, particularly for Frontex. [247]

REACTION: *Specific Action REACTION: REal-time ArtifiCial InTelligence for BOrders Surveillance via RPAS data aNalytics to support Law Enforcement Agencies*

The legacy of the ROBORDERS project, which ended in 2021 is the continued investment in the ever prophesised completely automated and impenetrable border. We see this in the continued EU and corporate funding for the project REACTION. The project has received €3.716.100 funding from the European Commission's Migration and Home Affairs Fund, and is coordinated by the Information Technologies Institute at the Center for Research and Technology Hellas (CERTH), just outside of Thessaloniki[248]. REACTION once again proclaims to allow for a "fully functional, next-generation, holistic border surveillance platform, providing situational awareness from remote areas as an effective means of early detection of critical situation"[249]. REACTION will see the technology developed as part of the ROBORDERS project, namely an unmanned 'swarm' of drones, alongside tech developed in the projects AIDERS and CERETAB, brought into the hands of the Greek police to use at Europe's external borders alongside thermal sensors, motion detectors and cameras.[250] CERETAB (the Collaboration for the establishment of increased awareness of the situation) was a project that worked to deliver a detailed and accurate picture of what happens at the borders between Greece and Cyprus. Specifically, it developed platforms for the sharing of information and the development of a "Common Information Exchange Platform" related to border surveillance data and systems[251]. The project ran for 51 months, ending in February 2023, and received €1,023,990, 95% of which came from the EU. The AIDERS project on the other hand, developed an "application-specific algorithms and novel mapping platform" used to process data collected through visual, thermal and multispectral cameras deployed at the land border of Evros in Northern Greece[252].

Speaking to attendees at the Arms Fair in Thessaloniki in November 2022 where the drones were on show, Notiris Mitarachis, the then Minister for Migration in Greece, described how the drones will automatically identify 'people of interest' in the border areas and alert police to approach and apprehend the travellers[253].

As demonstrated on the Greek government page for the project, the pre-determined risk and criminality of those to be identified through the automated drones is clear, where the technology will facilitate the process of gathering information on dangerous incidents involving migrants[254]. The drones, using AI and algorithms to identity and categorise risk or 'threat' assessments, relaying information to command-and-control centres, including those at the Reception and Identification centres in Greece, and the Evros Police Station at the Northern land borders, where information systems are already installed. Furthermore, the data collected will be shared with EUROSUR and other surveillance and information databases such as CISE, allowing access to border guards, police, and coastguards in Greece.

The language used to justify the use of such technology speaks to the "significant pressures" and challenges of securing the EU's external borders, claiming to tackle "smuggling, people -trafficking and other illegal activities", i.e., illegalised travellers who have no recourse to safe and legal routes into Europe. AI technology and high-tech automated surveillance systems are then positioned as an answer to these issues in a landscape with "vast sea, mountainous and densely forested areas with rough terrain", which limits the ability for humans to monitor the area without the support of technology.

MIRROR: *Migration-Related Risks caused by misconceptions of Opportunities and Requirement*

AI can also be applied to interpret large amounts of (social) media data and to influence public opinion. This is the case with ongoing, €5.1 million heavy project 'Migration-Related Risks caused by misconceptions of Opportunities and Requirement' (MIRROR), which aims to influence perceptions of the EU abroad: *"The perception of Europe and individual European countries has a high impact on expectations and decisions of citizens from outside Europe (considering) coming to Europe, especially from countries of origin (COO) for migration. Misperceptions and targeted misinformation campaigns can lead to security threats. It is therefore crucial for border control and other relevant security agencies and policy makers to better understand how Europe is perceived abroad, detect discrepancies between image and reality, spot instances of media manipulation, and develop their abilities for counteracting such misconceptions and the security threats resulting from them."* [255] [256]

AI plays a limited role in the project, mainly in the technologies used to collect and process information, e.g., the detection of computer-generated content[257] and automatic speech recognition.[258] The project purports to respond to both 'wrong' perceptions of prospective migrants' opportunities in the EU and deliberate 'media manipulation'. MIRROR's potential implications of programs like it are worth considering. Concretely, the project aims to find potential narratives that could be used to discourage people from migrating to Europe, based on the (social) media in their countries of origin.[259] [260] MIRROR is mainly analytical and interpretative, but its objective of establishing 'actionable insights' intends to, as the quote above demonstrates, provide theoretical findings to be used as a base for practical actions. Unsurprisingly, migrants are once again reduced to 'security threats'. While the proclaimed action of 'counteracting such misconceptions' might sound benign, publications by the Transnational Institute have demonstrated how policies for countering violent extremism have undermined human rights and can instrumentalise civil society to do so,[261] noting the rise of online content moderation and content removal.

iBorderCtrl

A project which is seemingly navigating itself in between the worlds of actual technology and false promises is the Intelligent Portable Border Control System (iBorderCtrl). The iBorderCtrl project ran from 2016-2020, also funded by Horizon 2020.[262] Scientists at Manchester Metropolitan University conducted the project and sold the technology commercially through their firm Silent Talker Ltd.[263] The EU contributed 100% of the funding, just over 4.5 million euros.[264] The testing took place at the Serbian-Hungarian border and the project's aim was to enable more rapid border crossings through a number of modalities, including an 'AI lie detector'; *"Multiple technologies check validity and authenticity of parameters (e.g. travel documents, visa, face recognition of traveller using passport picture, real-time automated non-invasive lie detection in interview by officer, etc.)."* [265] The 'officer' in question is an animation, questioning people on their own devices prior to their journey. The Intercept reported how, upon uploading a passport copy, the avatar requires people to verbally answer questions about their biographic data and trip purpose. Meanwhile, *"the virtual policeman uses your webcam to scan your face and eye movements for signs of lying. At the end of the interview, the system provides you with a QR code that you have to show to a guard when you arrive at the border. (…). The guard's tablet displays a score out of 100, telling him whether the machine has judged you to be truthful or not."* [266]

Travellers can and might already have been denied access to the EU without knowing the reason was the AI's assessment. Furthermore, the project has been criticised as scientifically dubious. Researchers from the Data Justice Lab at Cardiff University found the statistical premises and assumptions iBorderCtrl was based on included statistical fallacies and concluded it is *"very unlikely that the model that iBorderCtrl provides for deception detection would work in practice"*.[267]

IBorderCtrl is illustrative of several problematic dimensions of research projects impacting human lives and the way AI technologies are approached. Beyond the questionable efficacy of the science informing the technology, it was shrouded in secrecy, as commercial interests and the competitive advantage of private companies trump democratic control and oversight in EU research funding. In January of 2019 German MEP Patrick Breyer's request to access documents on iBorderCtrl was denied due to the commercial nature and value of the private companies involved, the biggest of which is European Dynamics.

In response he sued the EC, with the Court of Justice of the European Union ruling in December 2021 that the documents get released, with some further conditions.[268] Meanwhile, a follow-up project has been launched: "robusT Risk basEd Screening and alert System for PASSengers and luggage" (TRESSPASS). TRESSPASS includes more modalities, but still offers real-time behavioural analysis [269], pilots for which are being held at a Dutch airport, a Polish land border and a Greek seaport border crossing.[270]

The iBorderCtrl website lists FAQ's[271] notes that iBorderCtrl was a research project and there are several hurdles to implementing the technologies at the European borders. These hurdles include there currently being no clear legal basis and tensions with the rights to due process, non-discrimination, "*human dignity, etc.*"[272] It is worth noting, that the roll out of AI such as iBorder Ctrl would likely be banned under the AI act with updated unacceptable uses of AI that now include emotion recognition in the areas of law enforcement and border controls, changes brought in thanks to the campaigning of a coalition of digital rights organisations as we explore further below.

NESTOR *- aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders*

NESTOR makes the bold promise to the deliver "an entirely functional, next-generation, comprehensive border surveillance system offering pre-frontier situational awareness beyond sea and land borders".[273] It states it will offer a "new border surveillance system"[274]. Specifically, NESTOR will use *"thermal imaging and radio frequency spectrum analysis technologies fed by an interoperable sensors network"* to find people trying to cross the peripheral borders of Europe. The project ran from 11/1/2021- 30/4/2023, and received € 4 999 578,13 from the EU as part of the Secure societies – Protecting freedom and security of Europe and its Citizens funding programme[275] and was coordinated by the Hellenic Police.

The project again alludes to the ever-sought after yet ever-elusive *"real-time border surveillance"* that allows for a pre-frontier that becomes impenetrable. Sharing data with both CISE and EUROSUR, the project aims to use "state of the art sensory devices" to *"form an interoperable network to detect, assess and respond to illegal activities in border surveillance missions".* Further, the project website incites ideas of a "holistic" approach to border surveillance that is so often invoked, using "existing mixed reality and sensing technologies based on intelligent radar systems, RF localisation and wide-area visual surveillance services along with unmanned assets". Here, as the website states *"NESTOR will enrich its border surveillance system with accurate detection capabilities to optimally monitor the required border territory. Multimodal data feeds from numerous off-the-shelf devices will be fused and processed by employing AI techniques for enhancing the situational awareness and decision-making capacity of border control authorities".*

There have been three trials of the NESTOR platform to test is the technologies function as a means of detecting illegalised activities and people across border regions. The first of these took place at the Lithuanian border in November 2022, the second in February 2023 at the Cyprus/Turkey maritime border, and the third at the Greek/Bulgarian land border in March 2023. All three trials have been considered as successful[276], enabling "remote surveillance of the monitored border areas" to allow for an "early warning system"[277].

EURMARS *- An advanced surveillance platform to improve the EUROpean Multi Authority BordeR Security efficiency and cooperation*

The EURMARS project speaks of a "ground-breaking vision[278]" it "expand the common risk assessment practices" used by authorities at Europe's borders, furthering enhancing and developing the "deployment and evaluation of a secure multitasking surveillance platform". The aim of this, according to the projects webpage, improve "sensing capabilities for a wide range of security risks and threats in wider border areas by clustering high altitude platforms technology, satellite imagery, UxVs and ground-based sensors into a novel joint surveillance capability" through creating a unified surveillance system. The objective of the project is to enhance the security and risk assessment performance of border surveillance solutions. The project duration is from October 1, 2022, to September 30, 2025, with a total budget of €7,085,214.75, receiving funding from the Horizon Europe fun. Within the project's consortium is groups such as European Dynamics – who was also involved in iBorderCtrl, and the French company Thales.

The projects page remains particularly vague about specifics of what exactly will be developed, speaking of a platform only, but states it will enable a high level of surveillance and efficient risk assessment through creating a "closer collaboration between authorities at national, regional and EU levels". The project promises once again to build upon "the lessons learnt of previous initiatives, assimilate the knowledge of the stakeholders and their practice on CISE and other relevant systems, exploit the latest AI, risk assessment and visualization innovations". The language of "exploiting" AI suggests again that AI offers novel means of furthering securitisation policies at the border, that rely upon high levels of surveillance and risk assessment.

4. Regulation, Marketisation and the Future of AI in Europe

In April 2021, the European Commission published its long-anticipated AI package,[279] with one important part of this legislative reform being the proposal for a regulation on AI (the AI act).[280] This began a long legislative process that remains ongoing at the time of writing, before the European Commission, the European Parliament and the Council of the European Union (composed of the governments of the EU Member States) will agree on a common text and adopt the proposed rules.[281] Despite the recent vote from the Internal Market Committee and the Civil Liberties Committees of the European Parliament who voted on May 11th 2023 to ban the use of many emotion recognition AI, predictive policing, biometric categorisation and the use of biometric identification in public space – following an ongoing and widespread campaign consisting of 123 civil society groups – it is still the case that there is not sufficient protections for migrants and refugees from potential harm caused by the use of AI at and beyond the borders. The current version of the EU's upcoming AI act has a number of substantial shortcomings in relation to these vulnerable groups. Individual AI-based risk-assessments are nearly always incompatible with the right to due process, even if it is designed only to inform human decision-making. AI risk assessments used in the context of migration and border control must be classified as high-risk or unacceptable risk applications to ensure the same safeguards are necessary as with other high-risk applications.[282] These and a number of other recommendations were made in November 2021 by over 100 (digital rights) organisations[283], Members of the European Parliament (MEPs) seemingly paid heed to some of these recommendations and voted to restrict the use of biometric mass surveillance (BMS) and classify biometric systems as high risk in the context of the AI act in proposed amendments to the act in May 2023, as we shall see below[284]. However, there remains serious gaps and loopholes in the safeguards for AI technologies deployed at the external borders of Fortress Europe. Importantly also, Statewatch has found that since 2007, over 340 million euros has been spent on technologies that would be either high-risk or underregulated by the new AI Act.[285]

4.1 Risk vs Security; priorities within a risk-based approach

Through the AI act, the European Commission attempts to horizontally regulate AI systems, providing for differentiating requirements and obligations by risk level.[286] More precisely, the proposed regulation follows a risk-based approach, differentiating between uses of AI that create (i) an unacceptable risk, (ii) a high risk, (iii) a limited risk, and (iv) minimal or low risk. [287]

In Title II, the proposed rules list the prohibited practices that comprises all those AI systems whose use is considered as an unacceptable risk because it contravenes Union values, for instance by violating fundamental rights. This list was previously closed but was expanded in May 2023 to include *"real-time and most post remote biometric identification (RBI) in public spaces, discriminatory biometric categorisation and emotion recognition in unacceptably risky sectors"* [288]. Furthermore, Title III (with references also to Annex III) lists the *high-risk* AI systems that could impact people's health, safety or fundamental rights. The use of such systems is permitted in the EU subject to compliance with certain mandatory requirements and an ex-ante conformity assessment listed in Articles 8 to 15.[289] Such requirements are related to risk management, data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and cybersecurity[290]. Next, Title IV provides for some transparency obligations with regard to AI systems of limited-risk, including systems intended to interact with natural persons or to generate content.[291] Finally, the proposal allows the free use of *minimal or low risk* AI systems in the EU.[292]

Unacceptable Risk	AI systems viewed as harmful or that could pose a threat to a person's wellbeing, including "Cognitive behavioural manipulation of people or specific vulnerable groups", "social scoring" and "Real-time and remote biometric identification system".	These technologies are banned under the act.
High Risk	Ai systems viewed as potentially harmful to a person's safety and fundamental rights, to be divided in to two categories – those which fall within product safety legislation; and those that relate to the eight specific areas, namely of biometric identification and categorisation; critical infrastructure, education and training; employment; management and work; access to private and public services and benefits; law enforcement; migration, asylum and border control; assistance in the application of the law.	These technologies will be subject to "strict obligations" and assessments under the act, with exceptions set out for AI used for security and criminal purposes.
Limited Risk	AI systems viewed as posing a limited risk to users, where information, transparency and informed consent are robust enough safeguards to prevent harm. These include interactions with generative AI systems such as chatbots.	These technologies will have to comply with transparency obligations to enable people to make informed decisions about using the technology.
Minimal or Low Risk	AI systems that are already widely used, which are seen as safe for those who use them. This includes technology such as spam filters.	These technologies are allowed to be freely used under the act.

Data taken from the European Parliament, EU AI Act: first regulation on artificial intelligence *and the European Commission* Regulatory framework proposal on artificial intelligence

A coalition of 123 civil society organisations is criticizing this risk-based model as "dysfunctional" and has been instrumental in making the issue public, and campaigning for changes to the act, many of which were adopted in May 2023, as noted above. The coalition makes clear that this approach of ex ante designating AI systems to different risk categories does not consider that the level of risk also depends on the context in which a system is deployed and cannot be fully determined in advance.[293] This is because the deployment of AI systems can be of a dynamic nature, and therefore this risk-based approach is not suited for assessing unpredicted, long-run challenges and harms.[294] Thus, such a risk-based model could exclude from legal scrutiny a vast range of AI systems generally perceived to be of limited or minimal risk.[295] Moreover, the coalition underlines that the use of closed lists for certain categories, which cannot be amended easily in the future undermines the lasting relevance of the proposed regulation, and in particular its capacity to respond to future developments and emerging risks for fundamental rights.[296] These organisations support a shift of the current risk-based approach to a case-by-case, ex ante assessment of all AI systems. This would ensure that the burden of proving an AI system causes or risks harm falls upon the AI provider or user and prevent a situation where systems that are not classified as high-risk still have a detrimental impact because of their real-world use.[297] It should be noted that the vote that took place on the 11th of May, 2023, also proposed amendments to what should be considered as high-risk, providing further details on limits to "biometric identification, categorization and relating surveillance and policing purposes"[298]. However, despite these changes, the commission has stopped short of requiring that actors developing and implementing any high-risk AI be fully transparent and accountable – a core demand from the civil society coalition. Whilst MEPs have proposed that a fundamental rights assessment be conducted prior to the implementation of AI technologies, not everyone will be required to publish the findings of their assessments – only public authorities and large corporations and actors will have to do so[299].

Another inherent problem with the adoption of a risk-based approach, is where different categories of risks are played against each other, leading to the undermining of fundamental rights for any individual who is deemed a risk to Europe. For example, the failure to include AI used at and beyond the border to prevent entry to European territory demonstrates clearly how illegalised migrants are portrayed as a security threat and risk to Fortress Europe. As such, the risk of harm to them, or violation of their fundamental rights, is seen as less important as the supposed 'risk' they pose to Europe. So, we see how AI systems as well as individuals are constructed as risk points, especially within the context of migration or policing, that leaves them outside of safeguards within the AI act. Below, we explore each category of risk within the act to further outline the tensions within a risk-based approach.

4.2 Unacceptable use of AI Systems & the interplay with border management

As mentioned above, the European Commission provides outright or qualified prohibitions for a closed list of AI Systems that are perceived to pose an unacceptable risk. This list was initially composed of: (1) AI systems that deploy subliminal techniques, (2) manipulative AI systems, (3) social scoring systems, and (4) 'real-time' remote biometric identification systems used in publicly accessible places.[300] For categories 1 to 3, the prohibition for the use of such AI systems is broad and unconditional, and therefore directly applies to a border management context too.[301] The fourth category refers to a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay.[302]

Proposed amendments to the act that were the focus of the vote in May 2023 and the redrafting of the act for the "Compromise Amendments", will expand the list of unacceptable use of AI systems to all *"real-time and most post remote biometric identification (RBI) in public spaces, discriminatory biometric categorisation and emotion recognition in unacceptably risky sectors".*[303] This includes biometric categorisation that uses "sensitive characteristics" such as gender, race, ethnicity, citizenship status, religion or political orientation[304]. According to the European Digital Rights (EDRi) network, such systems are historically rooted in systems of oppression, colonialism, and injustice, making their use in a rule-of-law-respecting society hard to justify.[305] This follows following ongoing campaigns by groups such as the European Citizens Initiative "ReclaimYourFace"[306] composed of a large number of civil society organisations

It remains important to acknowledge that whilst most "post" remote uses of biometric identification will now be classed as unacceptable, the proposed rules of the AI Act continue to provide for a distinction between "real-time" and "post" uses of remote biometric identification, meaning there is not an outright ban on all remote biometric identification. As European Digital Rights highlight, this differentiation is irrelevant in human right terms, because the "post factum" use of biometric identification can be equally invasive as the "real-time" use.[307] Both uses are intrusive due to the increasing amount of video footage and digitised photographs posted online, allowing for biometric identification tools to be deployed in connection with big-data ecosystems that combine large datasets from multiple sources, such as social media or EU and national datasets storing biometric information.[308]

The amendments will also see the banning of AI used for predictive policing systems that profile people based on location or historical criminal record, as well as banning the use of emotional recognition AI systems used for law enforcement, border controls, the workplace and within education[309]. Furthermore, MEPs voted to enforce fundamental rights impact assessments be conducted before using high-risk AI systems.

These assessments should include an assessment of the following impacts, as per Article 29a of the compromise amendments to the act:

a. a clear outline of the intended purpose for which the system will be used;
b. a clear outline of the intended geographic and temporal scope of the system's use;
c. categories of natural persons and groups likely to be affected by the use of the system;
d. verification that the use of the system is compliant with relevant Union and national law on fundamental rights;
e. the reasonably foreseeable impact on fundamental rights of putting the high-risk AI system into use;
f. specific risks of harm likely to impact marginalised persons or vulnerable groups;
g. the reasonably foreseeable adverse impact of the use of the system on the environment;
h. a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated.
i. the governance system the deployer will put in place, including human oversight, complaint-handling and redress.[310]

However, only public authorities and large corporations are required to make the results of these assessments public, failing to provide a high level of transparency and accountability. Notably, as made clear by EDRI in their statement on the vote, MEPs have not included much of the AI used at and beyond the border for high levels of surveillance inherent to the securitisation, militarisation and externalisation of the border as discussed in the previous chapter.

4.3 High-Risk systems & Fortress Europe

The European Commission acknowledges, even within the proposed amendments to the act, that "AI systems used in migration, asylum and border control management affect people who are often in a particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities", while their use should always "guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration"[311]. In the proposed AI Act, the European Commission provides a list of AI systems that are considered to be of high-risk in a border management context. As mentioned already, the use of such systems is permitted in EU subject to compliance with certain mandatory requirements and an ex-ante conformity assessment.[312] The list as published in the current is composed of the following AI applications:

a. AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies as polygraphs and similar tools insofar as their use is permitted under relevant Union or national law

b. AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

c. AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

d. AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies to assist competent public authorities for the examination and assessment of the veracity of evidence in relation to applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

e. AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management to monitor, surveil or process data in the context of border management activities, for the purpose of detecting, recognising or identifying natural persons

f. AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management for the forecasting or prediction of trends related to migration movement and border crossing

EU watchdogs, such as the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) have already heavily criticised the European Commission's proposal.[313]

With regard to the AI systems provided under point (a), namely polygraphs and similar tools detecting the emotional state of a natural person, the EDPB and EDPS highlight that the scientific validity of such systems "is not proven", while their use can have a *"direct conflict with essential values of the EU",* adding that their use should be banned, instead.[314] Of note in the amendments is the adding of *"or on behalf of"* public authorities, suggesting agencies such as Frontex, the European border and coast guard agency, or the UNHCR, would also be authorised to use high risk AI technologies. Furthermore, the amendments add that high risk systems can be used in situations where risks are weighed against the *"potential benefits and intended goals of the system"*. In the case of border controls, the benefits of using AI systems for the prevention of illegalised migrants through irregular and illegalised means are thus likely to be considered as necessary to fulfil the goals of border control measures. Whilst the list of high-risk AI systems has been expanded to include systems used for detection and identification in point (e), and prediction of movement in point (f), it is noteworthy that these systems are not included in the use of unacceptable AI systems, despite using biometric categorisation and emotional detection AI technologies. Whilst the amendments add that such technologies should not be used to *"circumvent their international obligations under the Convention of 28 July 1951 relating to the Status of Refugees as amended by the Protocol of 31 January 1967, nor should they be used to in any way infringe on the principle of non-refoulement, or or deny safe and effective legal avenues into the territory of the Union, including the right to international protection"*, it is hard to see how technologies that fortify Fortress Europe and enable pushbacks of people from European territory at land and sea could ever not contravene the right to claim asylum. For example, the use of AI technologies such as radar or drone technologies in the Evros region in Greece, or in the Mediterranean Sea between Libya and Italy, where people are identified as illegalised migrants and forcibly intercepted or denied rescue when in distress, demonstrates how their deployment is fundamentally at odds with the right to claim asylum[315].

In chapter 2 we provided a detailed description of the EU databases in the field of border management, which constitute a key part of the virtual walls of Fortress Europe. Such databases incorporate the use of AI tools, for example in the context of automated profiling or automated biometric identification/ verification tasks, as explained in detail. The proposed amendments of the AI Act, in Article 83, states that where large IT-systems such as the interoperable databases of VIS, Eurodac, ETIAS, or SIS, have been deployed prior to the implementation of the AI act, they will have four years after the act comes into force to comply with the regulation, and two years where they fall under a high-risk category as listed above[316]. Whilst this is a significant amendment to the previous proposed regulation that states that it shall not apply to the AI systems which are components of all the EU databases in the field of border management that have been placed on the market or put into service before 12 months of the final date of application of the proposed rules[317], there are still important questions about the immediate harm of identification and categorisation through biometrics, where risk assessment of individuals continues to be central to the use of such systems.

4.4 Lobbying in the context of the AI legislative initiative

The AI act proposal is the product of a long process that started at the very beginning of the term of office of the new College of Commissioners in December 2019. The current President of the European Commission, Ursula von der Leyen, began her term with plans to propose legislation on the human and ethical implications of Artificial Intelligence in her first 100 days in office.[318] However, the legislative process was delayed offering the opportunity to various actors, including private technology and defence companies and their lobby organisations, to meet with key cabinets within the European Commission in order to promote their interests and strategically position themselves in the related policy discussions from the early beginning.

As our research shows, lobby groups targeted van der Leyen, key Commissioners for the proposed AI Act, such as Margrethe Vestager, the Executive Vice-President and Commissioner for A Europe fit for the Digital Age, and Thierry Breton, the Commissioner for the Internal Market, as well as Senior Officials of their cabinets. The presented findings are based on the transparency register of the European Commission, indexing all meetings of Commissioners and their cabinets with lobby organisations on topics such as digital policy and Artificial Intelligence from December 2019 to May 2023.[319]

Within these 31 months, 18 organisations related to the field of security and defence met with key representatives of the European Commission at least 80 times to discuss agendas related to technology, digital policy and Artificial Intelligence. The entity that managed to attend the most meetings (17) with the Commissioners and their cabinets is DIGITALEUROPE, a lobby organisation representing 78 corporate members, including big defence and security companies such as Accenture, Airbus, and Atos.[320] Other lobby groups such as the European Roundtable for Industries (ERT), representing also defence and security companies like Leonardo and Airbus,[321] attended 16 meetings, while the Information Technology Industry Council (ITI), also representing some security companies like Accenture or IBM,[322] managed to meet with the Commission 9 times. Another lobby group worth mentioning is the European Association of Research & Technology Organisations (EARTO)[323] which met with the European Commission 3 times. EARTO represents research centres that are big beneficiaries of EU research projects in different fields, including security, such as KEMEA (awarded approximately 40 million euro for 68 EU-funded research projects, including iBorderCtrl and NESTOR),[324] Fraunhofer-Gesellschaft (awarded approximately 80 million euro for 140 EU-funded research projects, including ROBORDER)[325] or the Austrian Institute of Technology (awarded approximately 25 million euro from 37 EU-funded research projects, including FOLDOUT (Through-foliage detection, including in the outermost regions of the EU), employing various sensors combined with machine learning analysis).[326] Large security and defence companies met also with the Commission without being represented by lobby groups: Airbus (13), Dassault Systemes (6), IBM Corporation (4), Leonardo (3), INDRA (2), OHB (2), Saab (2), THALES (2), Atos (3), Bundesdruckerei (1), IDEMIA (1), MBDA (1), Palantir Technologies (1), and TERMA A/S (2).

Our research into the meetings between EU commissioners throughout the course of negotiations over the AI act and the drafting of the proposed legislation demonstrates that there has been ongoing and expansive involvement of leading private companies within the field of security and defence. This is significant in the context of EU's priority to advance "innovation in the market", "investment", "improving the functioning of the internal market", "making Europe a leader in the field"[327]. Indeed, innovation and investment are set out in the guiding principles of the AI act, and Title V is dedicated to "measures in support of innovation".

Table 1: *Meetings of companies and lobby groups related to the field of security and defence with the European Commission on files related to digital policy and AI from December 2019 to May 2023.*

Entity name	Meetings with the President and/or her cabinet	Meetings with the Commissioner for 'A Europe fit for the Digital Age' and/or her cabinet	Meetings with the Commissioner for 'The Internal Market' and/or his cabinet	Number of Total Meetings for AI & digital policy
Airbus	7	1	5	13
Atos	1	0	2	3
Bundesdruckerei	1	0	0	1
Dassault Systemes	2	0	4	6
DIGITAL EUROPE	3	7	7	17
European Association of Research & Technology Organisations (EARTO)	0	2	1	3
European Roundtable for Industries (ERT)	6	4	2	12
IBM Corporation	1	3	0	4
IDEMIA	0	1	0	1
INDRA	0	1	1	2
Leonardo	2	1	0	3
MBDA	0	0	1	1
OHB	0	0	2	2
Palantir Technologies	1	0	0	1
Saab	1	1	0	2
TERMA A/S	0	2	0	2
THALES	0	0	2	2
The Information Technology Industry Council (ITI)	2	2	1	5
Total number of Meetings				80

Source: European Commission, The Commissioners

4.5 AI-enabled surveillance tools: Made in Europe, sold abroad

The proposed rules, under the current form, apply to the placing on the market, the putting into service and the use of AI systems in the EU.[328] Thus, they do not cover research and development activities for AI tools within the EU. However the amendments do include a caveat that the "testing in real world conditions shall not be covered by this exemption"[329]. Indeed, the proposed rules continue to safeguard the freedom of the arts and sciences as provided in Article 13 of the EU Charter for Fundamental Rights which outlines that keeping research and development practices free of constrain is undoubtedly of outmost important for a democratic society.[330] Yet, arguments have been made that this freedom should be subject to necessary and proportional limitations that aim at protecting the rights and freedoms of others.[331] Without such safeguards in place, the AI act will enable the ongoing investment in research projects that could lead to scientific breakthroughs in the development of surveillance-oriented AI systems that stand to be in conflict with the EU's human-centric vision of AI. In fact, the vote on the 11th of May 2023, MEPs also added additional exemptions to the act to cover research activities to promote "innovation" in the sector[332].

Further to this, there remains a failure to include AI used for national security and defence within the scope of the act (as set out in Article 2 of the act), as well as the failure to protect "the rights of migrants from discriminatory surveillance"[333] when voting on the draft mandate for the act in May 2023. Accordingly, private actors continue to benefit from research and development projects for intrusive AI technologies in a border management and national security context – often funded with EU money as part of the Horizon Europe and previous Horizon2020. As has been described in detail above, such EU-funded research projects already exist, further promoting the securitisation of immigration and the militarisation of border management activities. Importantly, the categorisation, as we shall see below, of AI tools for border control as high-risk opposed to unacceptable risk, means that the testing of experimental AI technology at the border in real world conditions continues to be permitted even when the act comes into force.

Moreover, the proposed rules of the AI Act provide significant loopholes to the deployment of AI tools outside of the EU. Specifically, whilst the amendments add that providers may not deploy AI technology prohibited as unacceptable under article 5 of the act outside of the EU whilst the providers or distributers of the system is located within the EU, it does not mention whether high-risk systems would be subject to any risk assessments if used outside of the union. Thus, the consortiums of EU-funded research projects developing intrusive AI tools could still sell the fruits of their research to third countries, exporting AI systems and "know-how" to the rest of the world.[334] In this way, surveillance-oriented AI systems could be designed and developed in the EU without limitations and then sold to third countries for border management and surveillance practices, strengthening the externalisation of EU borders even further.

Of note is that where authorities in third countries *"use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member State",*[335] and where they are assessed to have safeguards in place, the AI act regulations and safeguards shall not apply.

This is highly relevant to the exporting of technologies noted in the previous section that looked at externalisation practices such as the EUTF and agreements with countries such as Libya, or the exporting of surveillance tech in Niger and Western Sahara, to tackle migration before it reaches Europe. Thus, the provisions of the AI act would need to provide specific safeguards related to research and export activities taking into consideration the existing EU rules on similar matters.[336]

5. Conclusion

In the previous sections of this report, we have presented an overview of the expansive 'smart borders' of Europe. We framed these technologies along different points of the migratory journey: before leaving, along the route, at the border, and beyond the border where surveillance and practices of control continue to present themselves on the streets and in the camps of Europe. We explored how these structures work to categorise ad identify people as 'illegal' and 'risky' individuals and populations, perpetuating and entrenching unequal and harmful migration controls that ultimately exclude, stigmatise and marginalise people on the move, portraying them as a risk to the safety and security of European member states. We looked at the internalisation of border policies onto the human body through the use of biometrics for identification by border guards, police, and within EU wide interoperable migration databases, heartbeat detection at the border, as well as facial recognition and emotional detection AI technologies. We also discussed the externalisation of borders through hi-tech surveillance apparatus alongside data scraping and analysis to detect, predict and prevent people entering European territory. The involvement of private actors selling data infrastructures, technologies and AI equipment is integral to these processes, as well as migration pacts and funds for deals with third countries to try and stop people from being able to start the journey to Europe. The onus on AI technologies beyond the border, used to surveil, detect, and prevent people reaching European shores suggests that we are likely to see further externalisation policies and militarisation of peripheral borders (such as the Mediterranean Sea and Greece, as well as Libya, Niger, etc).

Focusing not only on how smart borders impact upon longstanding policies of securitisation, militarisation and externalisation as core logics of Europe's border regime, we also explored the interplay between governmental and private entities within the field of security and migration politics and policies. Security and border management companies are a multibillion-dollar industry, and the field of AI offers even further avenues to expand profit, with the market expecting to grow to $65.3 billion by 2024. Private companies have strategically positioned themselves to benefit and influence ongoing development of smart border technologies and AI for security and migration, whereby they create a self-fulfilling loop of public demand through providing infrastructure and expertise, nurturing strategic priorities relating to EU's creation of a leading AI market. Playing on narratives of illegality and risk vs security, private interests thus play a pivotal role in the ongoing development of smart technologies within the context of borders and migration. Our analysis in the final sections of the report show that the amendments within the AI act made in May and June 2023 go some way to address key concerns about AI technologies, but ultimately do not challenge the core components of Fortress Europe. The act will enable the ongoing use of AI technologies within migration controls that have been ruled as unacceptable within other contexts, such as the use of polygraphs and emotion detection AI technologies. In this sense, AI is both embedded within and entrenching particular policy directions of migration management.

Through exploring the development of Fortress Europe, the data infrastructures and AI that make up the 'smart' borders of Europe, and the future outlook of AI within border controls we can therefore see how security and private interests intersect with narratives of risk across migration policies and border politics. Understanding the objectives and mechanics of these policies, as well as the actors involved and those who stand to benefit from the advancement of AI and data-driven governance across the external and internal borders of the EU shows how the use of smart borders complements and reinforces restrictive border policies as well as industrial policies on AI. Smart technology is positioned as both an avenue for developing the EU as an innovator in the market and as a potential solution to the risk of migration. Yet there is little to suggest that any of this will actually help those who stand to be the most impacted by its harmful effects.

6. Endnotes

1 Politico Greek prime minister renews call for EU cash for border fence. 2023

2 The Guardian, Greece fortifies border to block refugees from Turkish-Syrian earthquakes. 2023.

3 M Akkerman, Expanding the Fortress Transnational Institute and Stop Wapenhandel Amsterdam,, 2018.

4 Countries attending the conference: Austria, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Greece, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia

5 The Greek Reporter, Contract For Greece's Evros Border Fence Extension Signed. 2023.

6 European Council on Refugees and Exiles, Greece: Further "Fortification" of Borders and More Vessels for Hellenic Coast Guard as Situation for Refugees in Türkiye Worsens Following Earthquakes, Series of Reports on Systematic Detention and Abuse. 2023.

7 Proposal for a Regulation of the European Parliament and od the Council. Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,

8 The Schengen acquis – Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders., 1985.

9 M Akkerman, Expanding the Fortress Transnational Institute and Stop Wapenhandel Amsterdam, 2018.

10 European Council: European Security Strategy – A secure Europe in a better world. 2009.

11 EEAS, A Global Strategy for the European Union's Foreign and Security Policy,, 2016.

12 More information on the shift towards securitisation can be found in Akkerman M. Expanding the Fortress Transnational Institute and Stop Wapenhandel Amsterdam, 2018.

13 Council of Europe, Media coverage of the "refugee crisis": a cross-European perspective: Council of Europe report DG1(2017)03. 2017.

14 Market Research Global Border Security Market Growth (Status and Outlook) 2021-2026,, 2021.

15 Der Spiegel, Europe's Violent Shadow Army Unmasked. 2021.

16 SIPRI World military spending rises to almost $2 trillion in 2020, 2021.

17 A Fotiadis. & N Ní Bhriain Smoking Guns: How European arms exports are forcing millions from their homes Transnational Institute, 2021.

18 A R Benedicto & P Brunet, Building Walls: Fear and Securitisation in the European Union, 2018.

19 European Union, EU's Next Long-Term Budget & Next Generation EU: Key Facts And Figures, 2020.

20 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624,

21 M Akkerman. Expanding the Fortress Transnational Institute and Stop Wapenhandel Amsterdam, 2018,

22 M Akkerman: Outsourcing Oppression, Transnational Institute, 2021.

23 Ibid.

24 UN High Commissioner for Refugees (UNHCR), UNHCR Position on the Designations of Libya as a Safe Third Country and as a Place of Safety for the Purpose of Disembarkation Following Rescue at Sea, 2020.

25 Human Rights Watch No Escape from Hell: EU Policies contribute to abuse of migrants in Libya, 2019.

26 Border Forensics, Mission Accomplished? The Deadly Effects Of Border Control In Niger. 2023.

27 UNITED. List of 52.760 documented deaths of refugees and migrants due to the restrictive policies of "Fortress Europe", 2023.

28 IRC. Greek shipwreck: Everything you need to know. International Rescue Committee. 2023.

29 Data available at the Missing Migrants Project, International Organisation for Migration

30 A R Benedicto & P Brunet, Building Walls: Fear and Securitisation in the European Union, 2018.

31 Bircan, T. & Korkmaz, E. Big data for whose sake? Governing migration through artificial intelligence, Humanities and Social Sciences Communications, 2021.

32 See for example A R Benedicto & P Brunet, Building Walls: Fear and Securitisation in the European Union, Transnational Institute, 2018.

33 Science for Humanity, Human presence, Movement & heartbeat Detection System (MDS), N.D.

34 Human Rights Watch and Homo Digitalis, Greece: New Biometrics Policing Program Undermines Rights, 2022.

35 Homo Digitalis, The Hellenic DPA is requested to take action again the deployment of ICT systems IPERION & KENTAUROS in facilities hosting asylum seekers in Greece. 2022.

36 European Asylum Support Office (EASO), Asylum Report, 2020.

37 Ibid, p.57.

38 International Organisation for Migration, 'Using big data to estimate migration "push factors" from Africa in Migration in West and North Africa and across the Mediterranean, 2020.

39 European Parliamentary Research Service, Artificial Intelligence at EU Borders: Overview of applications and key issues, 2021.

40 European Data Protection Supervisor (EDPS), Formal consultation on EASO's social media monitoring reports (case 2018-1083), 2019.

41 European Asylum Support Office (EASO), Record of data processing activity for EASO's Social Media Monitoring Reports, p.1, 2019.

42 Ibid.

43 European Data Protection Supervisor, Letter concerning a consultation on EASO's social media monitoring reports, 2019,

44 Ibid.

45 Ibid, p.3.

46 Ibid. p.5.

47 See Greek Ministry of Digital Governance, Upgrade/maintenance of the computer room of the Directorate of Maritime Border Security and Protection (EL), 2022.

48 Homo Digitalis, The Hellenic Coast Guard wants to acquire social media monitoring software: The Hellenic DPA is urged to exercise its investigative and supervisory powers, 2022.

49 Homo Digitalis, The Hellenic DPA is investigating the Greek Coast Guard for social media monitoring, 2023.

50 Frontex, Service contract for the provision of social media analysis services concerning irregular migration trends and forecasts (as part of pre-warning mechanism): Tender Specifications, 2019.

51 Frontex, Service contract for the provision of social media analysis services concerning irregular migration trends and forecasts (as part of pre-warning mechanism): Tender Specifications, 2019.

52 Privacy International, #PrivacyWins: EU Border Guards Cancel Plans to Spy on Social Media (for now), 2019.

53 M Latonero & P Kift, On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control, 2018.

54 Common Information Sharing Environment (CISE), European Maritime Safety Agency https://www.emsa.europa.eu/cise.html

55 European Commission, Report on the evaluation of the European Border Surveillance System (EUROSUR), 2018.

56 Statewatch, Kopernicus – what's in it for Joe Public?, 2008.

57 European Commission, European space capacities support responses to the refugee crisis, 2016.

58 Frontex, Migratory Map,

59 M Monroy, WhatsApp to Libya: How Frontex uses a trick to circumvent international law, 2021.

60 REGULATION (EU) 2021/1232 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. 2021.

61 Commission Implementing Regulation (EU) 2021/581 of 9 April 2021 on the situational pictures of the European Border Surveillance System (EUROSUR).

62 Ibid, Article 15.

63 Fallon, K., Christides, G., Busch, J., and Emmanouilidou, L. Greek shipwreck: hi-tech investigation suggests coastguard responsible for sinking. 2023.

64 European Commission, Coordinated Plan on Artificial Intelligence, 2018.

65 Intelligence Online, Frontex forges ahead with GEOINT and AI initiatives, 2021.

66 Özlem Demirel, Parliamentary Questions: Use of artificial intelligence for Frontex risk analysis, 2021.

67 Common Information Sharing Environment (CISE), European Maritime Safety Agency https://www.emsa.europa.eu/cise.html

68 L Taylor & F Meissner, A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk, 2020.

69 B Bathke, In post-pandemic Europe, irregular migrants will face digital deterrents, 2021.

70 European Commission, More Snapshots from the EU Asylum, Migration and Integration Fund and the EU Internal Security Fund, p. 30, 2020.

71 Hellenic Police, Announcements on Public Procurement Contracts. See also, Hellenic Government, National Programme ISF,

72 Onex SA, ONEX SA provides the Hellenic Police with high-end heartbeat detectors system for preventing illegal migration, 2018, European Commission, More Snapshots from the EU Asylum, Migration and Integration Fund and the EU Internal Security Fund, p. 30, 2020, and Hellenic Police, Announcements on Public Procurement Contracts.

73 Onex SA, ONEX SA provides the Hellenic Police with high-end heartbeat detectors system for preventing illegal migration, 2018.

74 Bulgarian National Television, The Illegal Migrants Detained at Kulata bordcr crossing were found by means of Heartbeat Detectors, 2016

75 Statewatch, Border guards, planes, "thermal vision vans" and heartbeat detectors – who is equipping Frontex?, 2014.

76 Frontex, Framework Contract for the Supply of Heart Beat Detectors (HBD) for Border Checks, 2019.

77 Water, N. & Freudenthal, E. Frontex at Fault: European Border Force Complicit in 'Illegal' Pushbacks, Bellingcat 2020, available at https://www.bellingcat.com/news/2020/10/23/frontex-at-fault-european-border-force-complicit-in-illegal-pushbacks

78 Border Violence Monitoring Network, BVMN join Statewatch in a Letter of Concern to Frontex, 2021.

79 Border Violence Monitoring Network, Frontex ignore rights violations at the Evros border, 2020.

80 Frontex, Artificial Intelligence Based Capabilties for the European Border and Coast Guard, 2020.

81 EDRI, Chilling use of face recognition at Italian borders shows why we must ban biometric mass surveillance, 2021.

82 Ibid.

83 Digwatch, Italian data protection authority: Sari facial recognition system proposed by Ministry of Interior could lead to mass surveillance, 2021 and Italian Data Protection Authority (Garante per la Protezione dei Dati Personali),Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy, 2021.

84 European Data Protection Board, EDPB response to MEP Sophie in't Veld regarding the use of Automatic Image Recognition System on migrants in Italy, 2021.

85 Ibid and European Data Protection Board and European Data Protection Supervisor, Call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination, 2021.

86 Carrer, L. & Coluccini, R. Technologies for Border Surveillance and Control in Italy, Hermes Center for Transparency and Digital Human Rights, N.D.

87 Reuters, Italy outlaws facial recognition tech, except to fight crime, 2022.

88 M Latonero & P Kift, On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control, 2018.

89 P Metcalfe & L Dencik, The politics of big borders: Data (in)justice and the governance of refugees, 2019.

90 European Commission, Snapshots from the EU Asylum, Migration and Integration Fund and the EU Internal Security Fund, p. 87, 2017.

91 Hellenic Ministry of Citizen's Protection, Approval of an extension for the delivery of the smart policing systems (EL), 2021.

92 E Chelioudakis, Greece: Technology-led policing awakens, 2020.

93 The devices will be linked to 20 databases held by national and international authorities. They include the Greek ministries of Transport, of the Interior, and of Foreign Affairs, Europol, Interpol and the FBI, though exactly which databases are included is unclear. Moreover, Teiresias, a credit bureau owned by Greek banks, is also among the databases listed in the document. See more in p.11 and p.140 of Hellenic Police, The technical specifications of the smart policing contract, 2018.

94 Hellenic Police, The technical specifications of the smart policing contract, 2018.

95 European Digital Rights, Facial recognition: Homo Digitalis calls on Greek DPA to speak up, 2020.

96 See more in Hellenic Data Protection Authority, Request for Information with regard to the smart-policing contract between the Hellenic Police and Intracom-Telecom (EL), 2020.

97 Ibid.

98 AlgorithmWatch, Flush with EU funds, Greek police to introduce live face recognition before the summer, 2021.

99 K L Jacobsen, Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees, 2015.

100 P Metcalfe & L Dencik, The politics of big borders: Data (in)justice and the governance of refugees, 2019.

101 M Latonero et al, Digital Identity in the Migration & Refugee Context analyzes the challenges of continually collecting identity data from migrants & refugees, 2019.

102 M Latonero & P Kift, On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control, 2018.

103 P Metcalfe & L Dencik, The politics of big borders: Data (in)justice and the governance of refugees, 2019.

104 Hellenic Government, Digital Transformation Bible 2020-2025, 2021

105 C Aradau & M Tazzioli M. Biopolitics multiple: Migration, extraction, subtraction. 2020.

106 V Squire & M Alozie, Coloniality and frictions: Data-driven humanitarianism in North-Eastern Nigeria and South Sudan. 2023.

107 M Madianou, Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. 2019.

108 Hellenic Government, IPERION IT System (EL), 2021.

109 Hellenic Government, REA IT System, 2021.

110 P Metcalfe & L Dencik, The politics of big borders: Data (in)justice and the governance of refugees, 2019.

111 Hellenic Government, KENTAYROS IT System, 2021.

112 Homo Digitalis, A major success for civil society in Greece: The Hellenic DPA launches an investigation into the Ministry of Immigration and Asylum re the YPERION and KENTAYROS IT systems, 2022

113 P Metcalfe & L Dencik, The politics of big borders: Data (in)justice and the governance of refugees, 2019.

114 M Latonero & P Kift, On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control, 2018. See also Privacy International, Wherever you go, they can follow: Modern surveillance technologies and refugees, 2014, available at https://privacyinternational.org/blog/1443/wherever-you-go-they-can-follow-modern-surveillance-technologies-and-refugees

115 Council of the European Union, Implementation of interoperability: state of play on the implementation of the Entry/Exit System and the European Travel Information and Authorisation System, 2021.

116 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1505

117 Ireland is fully connected since 2021, See more in Republic of Ireland, Minister McEntee and Commissioner Harris welcome Ireland's connection to Schengen Information System (SIS II), 2021.

118 European Commission, SIS II – Second generation Schengen Information System, 2021.

119 TNI, Building Walls: Fear and securitization in the European Union, 2018.

120 Regulation 2018/1860 (return decisions- consolidated version),

121 Regulation 2018/1861 (border checks for refusing entry or stay – consolidated version).

122 Regulation 2018/1862 (police & judicial cooperation – consolidated version).

123 See more details in Article 4 of Regulation 2018/1860, Article 32-33 of Regulation 2018/1861, and Articles 42-43 of Regulation 2018/1862.

124 Statewatch, Counter-terrorism and the inflation of EU databases by Heiner Busch and Matthias Monroy, 2017.

125 See more in European Union Agency for Fundamental Rights (FRA), Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019.

126 M Monroy, Schengen Information System: Fingerprint matching now obligatory throughout the EU, 2021.

127 European Commission, Automated Fingerprint Identification System (AFIS)

128 See more in European Union Agency for Fundamental Rights (FRA), Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019.

129 M Monroy, Schengen Information System: Fingerprint matching now obligatory throughout the EU, 2021.

130 Article 33 par 4 of Regulation 2018/1861 states that "As soon as it becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person in the context of regular border crossing points. Before this functionality is implemented in SIS, the Commission shall present a report on the availability, readiness and reliability of the required technology."

131 G Herrero et al, Study on Face Identification Technology for its implementation in the Schengen Information System, 2019.

132 Ibid.

133 European Digital Rights & Refugee Lab, Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up, 2020.

134 26 countries, namely: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland.

135 Former VIS rules, i.e. Regulation 767/2008.

136 European Commission, Revision of the VIS Regulation and of the Visa Code,

137 European Parliament and Council, Regulation (EU) 2021/1134 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing , OJ L 248, 13.7.2021.

138 European Parliament and Council, Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other, OJ L 248, 13.7.2021

139 See Article 1 of Regulation 2021/1134.

140 See more in Article 5 of Regulation 2021/1134.

141 Eu-LISA, VIS Technical Report 2017-2019: Factsheet, 2020.

142 Eu-LISA, Report on the technical functioning of the Visa Information System (VIS), 2020

143 See Recital 12 of Regulation 2021/1134 and Article 2 of Amendments to Regulation (EC) No 810/2009.

144 European Commission, Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security, Volume 2: Addendum, 2020.

145 See more in Article 9j, para. 4 of Regulation 2021/1134.

146 See more in Article 9j, para. 5 of Regulation 2021/1134.

147 See more in the EURODAC Regulation 2013/603.

148 Find all the relevant latest information regarding the suggested revision process of EURODAC in European Parliament, Recast EURODAC Regulation, 2021.

149 EPRS, Secondary movements of asylum- seekers in the EU asylum system, 2017.

150 European Council on Refugees and Exiles, Transforming Eurodac from 2016 to the New Pact from the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration, 2020.

151 European Digital Rights (EDRi), Eurodac database repurposed to surveil migrants, 2021.

152 The Migrant Files, http://www.themigrantsfiles.com/

153 See all information in Article 11 of the EURODAC Regulation 2013/603.

154 European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), Eurodac-2020 Statistics, 2021.

155 European Parliament, Recast EURODAC Regulation, 2021.

156 Ibid.

157 European Parliamentary Research Service, Artificial Intelligence at EU Borders: Overview of applications and key issues, p.8, 2021.

158 See more in the ETIAS Regulation 2018/1240.

159 Ernst & Young, European Union to implement Entry and Exit System (EES) and European Travel Information and Authorisation System (ETIAS), 2022,

160 ETIAS Regulation 2018/1240., Article 1.

161 Statewatch, EU: One step closer to the establishment of the 'permission-to-travel' scheme, 2021.

162 European Commission, Lists of third countries whose nationals must be in possession of a visa when crossing the external borders and of those whose nationals are exempt from that requirement, 2020

163 See all information about the different categories of data collected in Article 17 the ETIAS Regulation 2018/1240.

164 Ibid, Article 33-34.

165 Ibid.

166 Consumer Financial Protection Bureau, Using Publicly Available Information to Proxy for Unidentified Race and Ethnicity: A Methodology and Assessment, 2014.

167 Cabrera et al, Investigating Socioeconomic Status Proxies: Is One Proxy Enough?, 2018.

168 B Ghosh, Managing Migration: Whither the Missing Regime? How Relevant is Trade Law to Such a Regime?, 2017.

169 See more information in European Commission, European Criminal Records Information System (ECRIS), Accessed July 2023, Statewatch, EU: Interoperability: Letter confirms delays in implementation of "complex and challenging" plan, 2022 and EU Agency for large-scale IT-systems, Large-Scale IT Systems – Evolution and Outlook, 2023.

170 See more in the ECRIS-TCN Regulation 2019/816.

171 Ibid, Article 2.

172 Meijers Committee, CM2104 Creating second-class Union citizenship? Unequal treatment of Union citizens with dual nationality in ECRIS-TCN and the prohibition of discrimination, 2019.

173 See more in Article of 5 the ECRIS-TCN Regulation 2019/816.

174 Council of the European Union, Implementation of interoperability: state of play on the implementation of the Entry/Exit System and the European Travel Information and Authorisation System, 2021.

175 European Commission, Entry-Exit System. (EES).

176 See more in Article 1 of the EES Regulation 2017/2226.

177 Ibid.

178 Ibid.

179 Statewatch, Deportation Union, 2020.

180 Ibid, Articles 15 to 17.

181 European Commission, Implementing decision laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the EES, 2019.

182 Council of the European Union, Interoperability between EU information systems: Council adopts regulations, 2019. Specifically, Regulations 2019/817 and 2019/818 ,

183 Council of the European Union, Implementation of interoperability: state of play on the implementation of the Entry/Exit System and the European Travel Information and Authorisation System, 2021.

184 European Data Protection Supervisor, Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 2018.

185 The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, Revised timeline for the implementation of Interoperability, 2021.

186 European Commission, Summaries of EU legislation: Visa Code,

187 Statewatch, EU: Tracking the Pact: Presidency compromise proposals on revamped Eurodac database, 2021.

188 European Data Protection Supervisor, Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 2018.

189 European Parliamentary Research Service, Artificial Intelligence at EU Borders: Overview of applications and key issues, 2021.

190 See more in Article 7 of Regulations 2019/817 and 2019/818.

191 C Blasi Casagran, Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU, 2021.

192 See more in Article 25 of Regulations 2019/817 and 2019/818.

193 See more in Article 17 of Regulations 2019/817 and 2019/818.

194 E Brouwer, Large-Scale Databases and Interoperability in Migration and Border Policies: The NonDiscriminatory Approach of Data Protection, 2021.

195 European Data Protection Supervisor, Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 2018.

196 EU Agency for Fundamental Rights (FRA), Interoperability and fundamental rights implications, 2018.

197 Ibid.

198 Now called European Data Protection Board (EDPB).

199 Article 29 Data Protection Working Party, Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration, 2018.

200 European Digital Rights & Refugee Lab, Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up, 2020.

201 C Jones,, R Lanneau, & Y Maccanico, Access denied: Secrecy and the externalisation of EU migration control. Heinrich Boll Stiftung and Statewatch, 2022.

202 TNI & Stop Wapenhandel Amsterdam,, Financing Border Walls: The border industry, its financiers and human rights, 2021.

203 The European Border and Coast Guard Agency, Frontex` Single Programming Document 2016 – 2019, 2015.

204 European Commission, Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI – Global Europe),

205 Statewatch and Transnational Institute, At what cost? Funding the EU's security, defence, and border policies, 2021–2027, 2022.

206 Recital 51, Regulation (EU) 2021/947 of the European Parliament and of the Council of 9 June 2021 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe, OJ L 209.

207 Recital 51, Regulation (EU) 2021/947 of the European Parliament and of the Council of 9 June 2021 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe, OJ L 209.

208 A European Parliament Resolution approved in May 2021 expressed "concern" that a "lack of sufficient and coherent oversight" of the European Commission's implementation of the NDICI could prevent the Parliament "exerting democratic scrutiny over the EU's external migration policy". European Parliament, Resolution of 19 May 2021 on human rights protection and the EU external migration policy, 2019.

209 Privacy International, Violence at the EU's borders: Tech and surveillance in Europe's Human Rights Crisis, 2022.

210 https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620936/bp-eu-trust-fund-africa-migration-politics-300120-en.pdf;jsessionid=A43214CD357B5732DE35A94B28A8A349?sequence=1

211 European Commission, EU Emergency Trust Fund for Africa: A virtual exhibition,

212 Minutes of the EUTF's Strategic Board, cited in Oxfam International, The EU Trust Fund for Africa: trapped between aid policy and migration politics, 2020.

213 European Commission, EU Emergency Trust Fund for Africa: A virtual exhibition,

214 M Vermeulen & G Zandonini, The EU bypasses public tenders in Africa. This is what the EU's financial watchdog has to say, 2019.

215 Please see, M Akkerman, Expanding the Fortress: The policies, the profiteers and the people shaped by EU's border externalisation programme, 2018. p. 36-37 and European Commission, Table II -EU contributions pledged, 2019.

216 European Parliament Policy Department for Budgetary Affairs, Oversight and Management of the EU Trust Funds Democratic Accountability Challenges and Promising Practices, 2018.

217 EU Emergency Trust Fund for Africa, Support program for the strengthening of the civil status information system and the creation of a national biometric identity file, 2017.

218 Privacy International, Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds, 2020.

219 EU Emergency Trust Fund for Africa, Support for the implementation of the National Civil Status and Identification Strategy of Côte d'Ivoire, 2020.

220 EU Emergency Trust Fund for Africa, Support program for the operation of civil status in Mali: support for the establishment of a secure information system, 2017.

221 EU Emergency Trust Fund for Africa, Sahel and Lake Chad

222 Privacy International, The Future of the EU Trust Fund for Africa: Policy Briefing, 2019.

223 Privacy International, Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds, 2020.

224 O Moderan & F, R, Kone, What caused the coup in Burkina Faso?, 2022.

225 E, M. Akuamoah, 2021 in Review: The Coup in Guinea: Causes and Consequences,, 2021.

226 Privacy International, UN experts report highlights role of private military and security companies in immigration management, 2020.

227 See submission by Transnational Institute to the report of the UNHRC Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, 2020

228 M Akkerman, Financing Border Wars: The border industry, its financiers and human rights, Transnational Institute 2021.

229 Transnational Institute, Border Wars: The arms dealers profiting from Europe's refugee tragedy, 2016.

230 United Nations Working Group on the use of mercenaries Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants: Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the e, p.5, 2020.

231 See more in J Rufanges, Military Spending and Global Security: Humanitarian and Environmental Perspectives, 2020, Statewatch & The Transnational Institute, Market Forces: The development of the EU Security-Industrial Complex, 2017, and G Hudson &I Atak, Migration, Security, and Resistance: Global and Local Perspectives, 2022

232 Corporate Europe Observatory, Lobbying Fortress Europe: The making of a border-industrial complex, 2021.

233 Ibid.

234 When public officials, especially senior officials, leave the public administration to take up positions in the private sector, they are described as a 'revolving door' case. See more in European Ombudsman, Recommendation on how the European Defence Agency handled the applications of its former Chief Executive to take on senior positions at Airbus (OI/3/2021/KR), 2021.

235 Ibid.

236 M Akkerman, Financing Border Wars: The border industry, its financiers and human rights, Transnational Institute , 2021.

237 Corporate Europe Observatory, EU Defence Agency under pressure to change rules after Airbus revolving doors scandal, 2021 and Corporate Europe Observatory, Corporate Europe Observatory, Thierry Breton, the corporate commissioner?, 2019

238 The Guardian, Head of EU border agency Frontex resigns amid criticisms, 2022.

239 Statewatch and EuroMed Rights. Europe's Techno-Borders. 2023.

240 TNI, Market Forces: The Development of the EU Security-Industrial Complex, 2018.

241 European Commission, autonomous swarm of heterogeneous RObots for BORDER surveillance (ROBORDER),

242 European Commission, autonomous swarm of heterogeneous RObots for BORDER surveillance (ROBORDER),

243 Z Campbell, Swarms of drones, piloted by Artificial Intelligence, may soon patrol Europe's borders, 2019.

244 Z. Kallenborn, The Era of the Drone Swarm is Coming, and We Need to be Ready for It, 2018.

245 Ibid.

246 European Parliament, Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights, p.95, 2020

247 B Hayes, C Jones, & E Töpfer, Eurodrones Inc., 2014.

248 Lulamae, J. Greece plans automated drones to spot people crossing border. Algorithm Watch, N.D. https://algorithmwatch.org/en/greece-plans-automated-drones/ See also, Specific Action REACTION: REal-time ArtifiCial InTelllgence for BOrders Surveillance via RPAS data aNalytics to support Law Enforcement Agencies,

249 Ibid.

250 Lulamae, J. Greece plans automated drones to spot people crossing border. Algorithm Watch, N.D.

251 See CoopERation for increased siTuational Awareness establishment

252 See AIDERS project,

253 J Lulamae, Greece plans automated drones to spot people crossing border. Algorithm Watch, N.D.

254 See Specific Action REACTION: REal-time ArtifiCial InTelllgence for BOrders Surveillance via RPAS data aNalytics to support Law Enforcement Agencies,

255 European Commission, Migration-Related Risks caused by misconceptions of Opportunities and Requirement (MIRROR),

256 Privacy International, MONITORYOU: the MilliONs beIng spenT by the eu on develOping surveillance tech to taRget YOU, 2020.

257 MIRROR. Deliverable D4.1: First Release of Text-analysis Technologies and Models, 2020.

258 MIRROR, Deliverable D7.1: MIRROR Architecture and Integration Plan, 2019.

259 European Commission, Strengthen security through border management,

260 European Commission. Support the Union's external security policies including through conflict prevention and peace-building.

261 Transnational Institute, The globalisation of Countering Violent Extremism policies: Undermining human rights, instrumentalising civil society, 2018.

262 European Commission, Secure societies – Protecting freedom and security of Europe and its citizens,

263 Biometric Update, Partial success in transparency lawsuit into EU's AI lie detector research. 2021

264 Open Security Data Europe, iBorderCtrl – Intelligent Portable Border Control System,

265 European Commission, Intelligent Portable Border Control System (iBorderCtrl),

266 Intercept, the, We tested Europe's new lie detector for travelers — and immediately triggered a false positive, 2019.

267 JS Monedero & L Dencik, The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl, 2020.

268 Biometric Update, Partial success in transparency lawsuit into EU's AI lie detector research. 2021

269 Tresspass Project, the Project

270 Tresspass Project, Pilots

271 iBorderCtrl, Frequently Asked Questions,

272 iBorderCtrl, Frequently Asked Questions,

273 See aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders,

274 NESTOR: Showcasing a new border surveillance system, Frontex. https://frontex.europa.eu/innovation/eu-research/news-and-events/nestor-showcasing-a-new-border-surveillance-system-NIV4SC

275 See aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders,

276 Nestor Project, Greek/Bulgarian trail, 2023.

277 Nestor Project , Lithuanian trial, 2022.

278 See Eurmars Project

279 See specifically, European Commission Communication on Fostering a European approach to Artificial Intelligence, 2021; European Commission, Coordinated Plan on Artificial Intelligence 2021 Review, 2021; and European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021.

280 See above.

281 Follow the legislative process of the EUAI Act in European Commission, Legislative train schedule: Proposal for a regulation on a European approach for Artificial Intelligence,

282 Statewatch, A Clear and Present Danger, 2023

283 Ibid.

284 EDRI, EU Parliament sends a global message to protect human rights from AI, 2023.

285 Statewatch, EU has spent over 340 million on border AI technology that new laws fail to regulate, 2022.

286 M Veale and FZ Borgesius, Demystifying the Draft EU Artificial Intelligence Act, 2021.

287 See in detail paragraph 5.2.2. of the explanatory memorandum in the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p.12, 2021.

288 https://edri.org/our-work/eu-parliament-committee-vote-strong-message-protecting-fundamental-rights-from-ai-systems/

289 See more in Section 5.2.3, p. 13-14 of European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts,

290 Statewatch, A Clear and Present Danger, 2023

291 European Commission, Regulatory framework proposal on artificial intelligence,

292 European Commission, Regulatory framework proposal on artificial intelligence, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

293 EDRI et al, An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement, 2021.

294 EDRI, Recommendations for a fundamental rights-based Artificial Intelligence Regulation: addressing collective harms, democratic oversight and impermissible use, 2020.

295 European Digital Rights, Submission to European Commission adoption consultation: Artificial Intelligence Act, 2021.

296 European Commission, Regulatory framework proposal on artificial intelligence, Accessed June 2022.

297 EDRI et al, An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement, 2021.See also AlgorithmWatch, Draft AI Act: EU needs to live up to its own ambitions in terms of governance and enforcement, p.4, 2021.

298 TaylorWessing, Draft of the AI Act gets on the home stretch, 2023.

299 EDRI, EU Parliament sends a global message to protect human rights from AI, 2023.

300 See Article 5 of the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021

301 There are civil society groups that have called for more clarifications in the text, especially for manipulative AI systems, in order to reassure that the prohibition of Article 5(1)(b) for the exploitation of a comprehensive set of vulnerabilities covers also migration status. See more in European Digital Rights et al, An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement, 2021.

302 See Article 3 of the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021

303 EDRI, EU Parliament sends a global message to protect human rights from AI, 2023.

304 See TITLE II PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES, Article 5 in https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf

305 EDRI, Submission to European Commission adoption consultation: Artificial Intelligence Act, 2021.

306 See more information in the related website of ReclaimYourFace European Citizens Initiative.

307 EDRI Submission to European Commission adoption consultation: Artificial Intelligence Act, 2021.

308 The Biometrics and Forensics Ethics Group (BFEG), Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology, 2021.

309 Mayson, Hayes & Curran,, MEPs Adopt Parliamentary Committee Amendments to EU AI Act, 2023.

310 European Parliament, DRAFT Compromise Amendments on the Draft Report, 2023,

311 European Parliament, DRAFT Compromise Amendments on the Draft Report, 2023,

312 See Article 7 of the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021 and Annex III paragraph 7 .

313 European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021.

314 Ibid, page 12.

315 Statewatch and EuroMed Rights. Europe's Techno-Borders. 2023.

316 European Parliament, DRAFT Compromise Amendments on the Draft Report, 2023,

317 See Article 83 of the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021 and Annex IX .

318 EDRI, Von der Leyen: An ambitious agenda for digital rights, 2019.

319 European Commission, The Commissioners,

320 See more in DIGITALEUROPE, Our Corporate Members,

321 See more in European Roundtable for Industries, Members,

322 See more in Information Technology Industry Council, ITI Members,

323 See more in European Association of Research & Technology Organisations, Members,

324 Open Security Data, KEMEA,

325 Open Security Data, Fraunhofer-Gesellschaft,

326 Open Security Data, Ait Austrian Institute Of Technology Gmbh,

327 European Parliament, DRAFT Compromise Amendments on the Draft Report, 2023,

328 Article1 of the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021.

329 See Article 2, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf

330 Article 13 of the Charter of Fundamental Rights of the European Union,

331 Article 52 of the Charter of Fundamental Rights of the European Union,

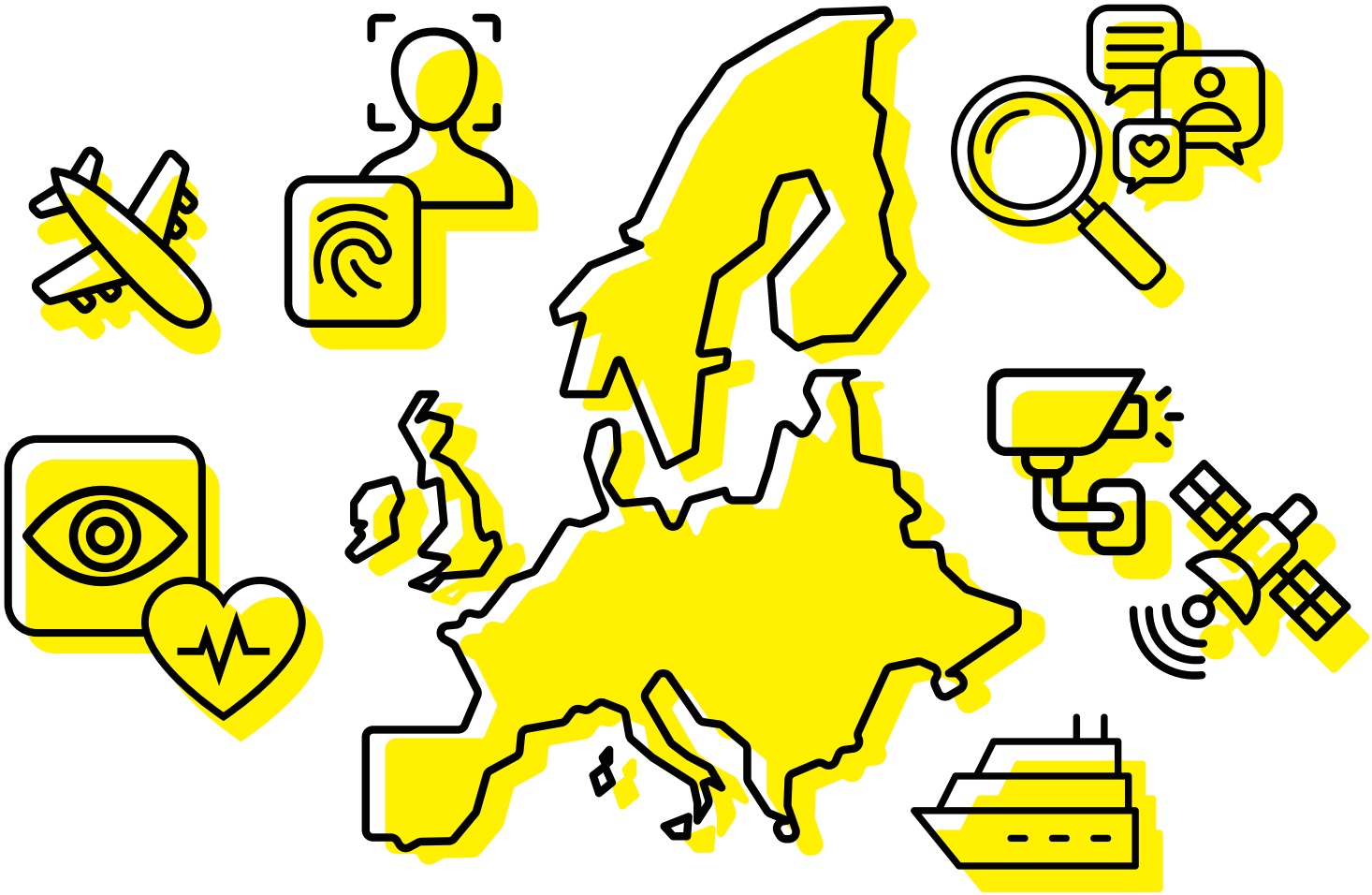
332 https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

333 EDRI, EU Parliament sends a global message to protect human rights from AI, 2023.

334 Article 2 of the European Commission Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021 and European Digital Rights (EDRi), Submission to European Commission adoption consultation: Artificial Intelligence Act, 2021.

335 See Article 2, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf

336 Such as for example the recently adopted rules on control of exports, brokering, technical assistance, transit and transfer of dual-use items, even though they are far from perfect. See more in Council of the European Union, Trade of dual-use items: new EU rules adopted, 2021.



datajusticelab.org

Data Justice Lab

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

erc