Forum Tunisien pour
les Droits Economiques et Sociaux

# THE NEXUS OF TECHNOLOGY AND MIGRATION

## TECH-FACILITATED BORDER CONTROL AND IMPLICATIONS FOR TUNISIA

**Supported by**

Mozilla Foundation

# TABLE OF CONTENTS

# ABOUT FTDES

The Tunisian Forum for Social and Economic Rights (FTDES) is a Tunisian civil society organisation, recognised by the state in 2011. FTDES is non-governmental, neutral, and independent from any political party or religion. It was established in 2011 to fight and advocate for people's economic and social rights at the national, regional and international level. FTDES is working on labour rights, women rights, environmental justice and migrant rights. It has its head office in Tunis and local branches in the governorates of Kairouan, Monastir and Gafsa.

# ABOUT MOZILLA FOUNDATION

Mozilla Foundation is a global nonprofit dedicated to ensuring the internet remains open, inclusive, and equitable. Founded in 2003, it supports people-first technology through funding, advocacy, education, and research. Although the present research was supported by a grant from the Mozilla Foundation, it does not necessarily reflect the views of the Mozilla Foundation.

Rooted in the open-source movement and guided by the Mozilla Manifesto, Mozilla Foundation focuses on critical issue areas like ethical data practices, healthy digital ecosystems and shifting digital power toward individuals and communities. Its work connects technologists, researchers, policymakers, and activists with the aim of reimagining and rebuilding systems that serve the public good. With over two decades of global impact, Mozilla Foundation continues to lead the movement for a better technology future—powered by people, and open by design.

# ABSTRACT

The policy paper examines the strategies and methods underlying the deployment of emerging technologies along the Italian Tunisian migration borders in the broader context of migration management in the Mediterranean. It investigates the measures needed for transparent, rights-based AI and tech applications by border security agencies and the relevant governmental institutions and subsequently explores civil society's role in protecting migrants encountering tech-facilitated border operations. The research analyzes existing literature and information provided by targeted key informants and stakeholder interviews. The research aims to identify policy-practice gaps and develop targeted recommendations for both governmental and civil society actors.

The findings will contribute to a broader understanding of how technology is deployed in the migration context of Tunisia, Italy and the EU as main parties. It will also shed light on frameworks that prioritize human dignity in border management across the Euro-Mediterranean region.

# EXECUTIVE SUMMARY

Migration control and pushbacks in the Mediterranean Region have become increasingly facilitated by technology in the recent years of digital evolution along with migration flows. The implications of technological advancements in determining the fate of migrants are now more significantly present across the region. Subsequently, this elaborated policy paper aims at shedding light on this phenomenon for civil society actors as well as people on the move, who are either affected by it or addressing it, all the while putting more pressure on the governmental entities and regional institutions that are complicit in it.

The paper builds on past discoveries in the intersection of technology and migration between Tunisia and Italy and between North Africa and the EU. It reflects on the evolution of technological deployment for border control and externalization while examining recently surfaced cases and events. The key findings of the paper are as follows:

### TECH-FACILITATED BORDER EXTERNALIZATION IS FUNDED BY THE EU AND MEMBER STATES

The pushbacks of migration flows, especially in the last few years, has been financially fuelled by the EU, governed by leading governments in the border control regime such Italy and operationalized by North African countries and their coast guards such as Tunisia, which continues to take advantage of the resources it is given, in order to perform as expected.

### DRONE SURVEILLANCE AND THE TECH INDUSTRY ARE FRONTEX'S MODERN BORDER CONTROL STRATEGY

The tech industry has become an important accomplice with FRONTEX in the weaponization of technology, drones, information systems and data, causing further surveillance and injustice towards migrants whose fates are being determined by machines.

### STATE-SPONSORED SPYWARE ATTACKS ARE TARGETING MIGRANTS' RIGHTS ACTIVISTS AS SECURITY THREATS

Targeting civil society actors with advanced military technology demonstrates that Italy and other EU member states are excessively reshaping migration as a security issue, invading privacy and deliberately labelling resistance as a threat, therefore targetable for cyber-attacks.

### DATA EXCHANGE & MIGRANTS' CRIMINALIZATION

Unlawful data transfer and misuse out of context is the most recent unravelling between FRONTEX and EUROPOL. This highlights the systemic collection and use of migrants' data for discriminatory and criminalization purposes and sheds light on the lack of legal basis to sharing sensitive data from migrants with other entities.

# METHODOLOGY

This is a policy-oriented research paper with a multi-stakeholder approach, addressing multi-disciplinary actors; thereby, it derives information from interviews conducted with activists, researchers, journalists and other stakeholders. These interviews are an addition to existing literature about the tech-migration nexus within context-relevant cases and settings along with open-source intelligence, recent investigative reports, public statements and evidence. The interviewees are journalists, human rights defenders and sea rescue members. They also include individuals directly affected by the systemic use of digital technologies for border control by Italy, the EU and its allies. Some remain under constant threat of surveillance, targeting and/or criminalization. Others bring firsthand field experience with migrants and asylum seekers facing tech-induced challenges including pushbacks and human rights violations along the Tunisian-Italian migration routes. These diverse lived experiences and evidence-based insights are analyzed in the present policy paper to understand the struggles and contribute to change.

# ACRONYMS

| | |
|---|---|
| AI | Artificial Intelligence |
| ADAS | Airbus DS Airborne Solutions |
| AFIS | Automated Fingerprint Identification System |
| BMP | Border Management Programme |
| BMVI | Border Management and Visa Instrument |
| CMRCC | Civil Maritime Rescue Coordination Centre |
| EEAS | European External Action Service |
| EDPS | European Data Protection Supervisor |
| EU | European Union |
| EU-LISA | European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice |
| EURODAC | European Dactyloscopy |
| EUROPOL | European Union Agency for Law Enforcement Cooperation |
| EUROSUR | European Border Surveillance System |
| EUTF | European Union Trust Fund for Africa |
| FRONTEX | European Border and Coast Guard Agency |
| FTDES | The Tunisian Forum for Social and Economic Rights |
| GDPR | General Data Protection Regulation |
| GPS | Global Positioning System |
| IAI | Israel Aerospace Industries |
| IBM | Integrated Border Management |
| ICMPD | International Centre for Migration Policy Development |
| ISMaris | Integrated System for Maritime Surveillance |
| ITU | International Telecommunication Union |
| SARI | Sistema Automatico Riconoscimento Immagini |
| SAR | Search and Rescue |
| VHF | Very High Frequency |
| UN | United Nations |

# INTRODUCTION

In recent years, EU member states, including Italy with the Mediterranean borders, have been leveraging more innovative technology and AI applications in their border control strategy and border management operations. The Italian government, along with several EU border control agencies have shown their commitment to using these tools through a growing flow of investments where Statewatch (2023) asserts that the EU allocated at least €250 million for border high-tech development between 2014 and 2022 with Italy as the most funded state for border policies' implementation within the 2014-2020 period (Rijtano, 2023).

As for the BMVI funding allocation for 2021-2027, Italy has shown an increase of investment in tech-powered surveillance and identification equipment including drones, aircrafts, vehicles equipped with satellite and thermal imaging and other digital tools serving for stemming migration flows to Italy and the EU at any cost (Catelli, 2024). These tech-facilitated approaches of border control in the Mediterranean, not only come with financial and logistical costs but also with human costs. This is where the adopted EU Council's migration and asylum pact does not clearly highlight the line between security and targeting in the nexus of technology and migration (EU Council, 2024).

# LITERATURE REVIEW

Along with the European Union, some of the key actors involved in the utilization of technology for implementing the EU's Mediterranean border control policies and the 2024 migration and asylum pact include EU-LISA, FRONTEX, EUROPOL, EU-Mediterranean States such as Italy and Greece and other agencies such as EEAS that shape EU's foreign policy. Although technology plays a central role in these policies, EU institutions and associated agencies have faced ongoing criticism for lacking clear and independent measures tailored for the use and deployment of border technologies. Similarly, the EU AI Act ("EU AI Act," 2024) —or the EU's most crucial AI governance legislation— has been criticized for lacking a human rights-based approach at borders and for experimenting high-risk technology and AI on migrants (Molnar, 2023).

Since before the emergence of AI and technology procurement in recent years for border control and management, the Italian government has been gathering migrants' data —including biometric data— in two key databases. The first is EURODAC, a database managed by the EU-LISA agency, mainly in asylum seeking processes but was consequently serving law enforcement and border security institutions, hence the adoption of EURODAC in EU criminal law, including at the borders (Vavoula, 2024). The second is the AFIS, generating a biometric database by the Italian ministry of interior that is also serving a dual use in law and in migration.

**EU-LISA**

EU-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems, is an EU agency that managed the IT systems and relevant databases for the EU's security including border security, migration monitoring and asylum-seeking processes. It is governed by board members who are representatives of EU Member States and the European Commission.

These databases have been utilized by the Italian government in the deployment of an AI-driven facial recognition system "SARI" procured in 2017 which has been abused in its applications and has slowly led to a growing pattern of African migrants' criminalization, particularly during the reception and disembarking processes across the Italian-Mediterranean borders (Carrer & Coluccini, 2022).

The AI system not only relies on migrants' biometric data and imagery—some of which reportedly collected without the consent of the migrants— but is also lacking transparent governance, cross-verification and protection in the limited legal frameworks of the EU's GDPR and AI Act which do not foster safety measures in the context of migration due to the extra-territorial span despite being deployed in Italian and EU territory (Soverino, 2024).

This proves significant contextual and policy gaps in these frameworks allowing the continuous use of automated image and facial recognition in critical decision-making processes by the Italian Ministry of Interior, when it comes to the fate of migrants and asylum seekers.

**GDPR**

**The General Data Protection Regulation, abbreviated GDPR, is a European Union regulation on information and data privacy in the European Union.**

**EU AI Act**

**The EU AI Act is a regulation that establishes legal rules for the development, marketing, and use of AI systems within the EU. It covers AI across many sectors except those solely used for military, national**

This automated process disregards the potential for bias and stigmatization in the labelled data collected as well as the migrants' right to epistemic justice and due process in cases of systemic criminalization during arrivals. For strategic purposes, Italy's role in employing AI-driven technology for border control and migration reception systems extends to employing it for border externalization through relations with North Africa. In particular, the Tunisian government has been deeply involved in Italy and the EU's scheme of migrants' pushback in the Mediterranean as well as arbitrary detention at arrival.

The Italian government has been the second highest ranking donor to the EUTF, the programme responsible for funding and implementing the €65 million-worth project Border Management Programme in partnership with the ICMPD (EUTF, 2018). Along with Morocco, Tunisia has been an implementation country of the BMP, one of many EUTF projects aimed at migration control, under the overall EUTF budget of €5 billion, to which Italy has contributed. (EUTF, 2024). Up until 2024, the BMP consisted mainly in providing the national coast guard with surveillance tools ranging from sensor-based radars and thermal and satellite imagery detection to remote surveillance vehicles and drones, along with intensive training and guidance for their deployment (Garavoglia, 2024).

The outcomes of this project and similar ones reveal yet another gap between EU migration policy and tech-driven practices — this time on the other side of the Mediterranean where Tunisia is exploiting Italy's technical resources and capacities, thereby jeopardising the privacy and digital rights of Tunisian and Sub-Saharan migrants.

**EUTF**

**EUTF, the European Union Trust Fund for Africa, is an EU-funded programme that operates in the Sahel region and Lake Chad, the Horn of Africa and North Africa regions. It aims at providing economic opportunities in these regions all while monitoring and managing migration flows towards Europe. It is managed by the European Commission, and its projects conclude at the end of 2025.**

**ICMPD**

**ICMPD, the International Centre for Migration Policy Development, is an international, inter-governmental organization that is funded by various sources including EU members states, UN agencies and the European Commission. It provides space for exchange of services between governments, for research, dialogue and capacity developments, to manage migration flows from Africa, Central Asia, Western Balkens are Turkey. It's decentralised structure and**

With the EU's support, the Italian ministry of interior invested € 4.8 million in patrol boats for the Tunisian coast guard as part of a memorandum of understanding signed by both governments in December 2023 and they are equipped with sensor-driven technologies (Abdul, 2024). The highly sophisticated patrol boats were transferred to Tunisian coast guard during the summer of 2024 under the condition that they'd be used for Tunisia's newly established maritime Search and Rescue mission (Abdelmoula, 2024). Nevertheless, past practices of the Tunisian coast guard have shown that intercepting migrants, boats and shipwrecks before the rescue boats by non-governmental organizations would often lead to further violence or deliberate boat wrecking, increasing death tolls, criminalization, deportation following interception, and other human rights violations at the Mediterranean Sea, in the context of SAR (Alarmphone, 2024).

The EU, the Italian ministry of Interior, the Tunisian government and its national coast guard are all involved in reinforcing strict and inconsiderate border control measures using AI, sensor-based technologies and surveillance tools. However, they are not the only ones creating tech borders. FRONTEX's use of emerging technologies has been present in both the interception and in the reception of migrants and asylum seekers in the Mediterranean.

In recent years, FRONTEX has prioritized the deployment of algorithmic surveillance using its own drones and facial recognition and sensor monitoring technologies such as radars and satellites. This allows gathering personal and biometric data that is being further shared with EUROPOL, the same agency that has shown in the past a pattern of unlawful data practices such as the collection, storage and treatment of large datasets leading to wrongful association to criminal activity (Napolitano & Barker, 2025). These unlawful practices by an EU agency show that algorithmic discrimination is only one out of many risks that EU agencies keep taking in the name of security and border control, especially as they follow a path of automation and intelligence surveillance without a rights-based approach (Gandhi, 2024).

**FRONTEX**

**Frontex, the European Border and Coast Guard Agency, is an agency of the EU established to coordinate and support EU member states in managing the external borders of the Schengen Area with significant operational powers at borders.**

**EUROPOL**

**Europol, the European Union Agency for Law Enforcement Cooperation, is the EU's law enforcement agency established to support member states**

For advocacy and for inducing change, civil society in the region has been shedding light on these policy-practice gaps across the Mediterranean Sea from the different perspectives of governments' respective agendas, the EU as a main funder and facilitator, the technologies' duality and limitations as well as the engagement of NGOs, activists and journalists involved. Civil society's commitment to advancing migrants' rights has been manifested beyond rescue missions and humanitarian aid, especially amid a fast-paced technological innovation.

Awareness raising, legislation suspensions and policy contributions have all been part of civil society's efforts in resisting tech borders and their impacts on migrants in the region. Nonetheless, civil society actors themselves have been affected by these tech borders and have been facing more challenges than ever in advocacy, rescue attempts, support giving and documentation efforts, hence, making it more difficult to influence policy and less safe for the entire community (Napolitano, 2023).

# CONTEXT OVERVIEW

In April 2025, Tunisia has been marked as a safe third country of origin in a unified list released by the EU commission despite recurrent activities by the Tunisian authorities and ministry of interior, particularly in the past 2 years, which have led to immense human rights violations towards Tunisian and especially sub-Saharan African migrants both in Tunisian territory and at the sea (FTDES, 2025).

In fact, many organizations and coalitions for migrant rights have emphasized through press releases and joint statements that Tunisia is not a haven for migrants rescued at sea (Amnesty International et al, 2024). This was a conclusive note after a high record of violent measures and human rights violations towards sub-Saharan migrants across the country, including deprivation of shelter through last minute evictions from properties, access denial to care and assistance amidst racist attacks and most importantly the continuous waves of arbitrary arrests in Tunisia and also at the borders followed by concentrated deportation approaches at southern borders with Libya and Algeria (OMCT, 2023).

This has exposed some contradictions that serve the EU's agenda of border externalization and pushbacks in the Mediterranean which has not only been fuelled by the "safe third country" designation, but also the continuous flow of financial and resource investments by the EU and the Italian ministry of Interior in the Tunisian government's suppression and violent deterrence of migrants. Consequently, the relevance of examining the tech-migration nexus in the region has become a pressing issue for the Tunisian civil society. It examines how investments in capacity are behind the tools applied for misuse and misconduct in data practices and technology applications, instead of rescue missions.

# FINDINGS & ANALYSIS

## 01. Tech-facilitated Border Externalization

This wave of tech-driven applications and data-hungry methods in border control and externalization has only surfaced now due to the openness of emerging technologies and information about them. However, this wave dates back at least a decade, beginning with multiple phases of ICMPD programmes, which were tested across North African countries from

2015 for the IBM and from 2018 for the BMP. These programmes run with the financial support from different actors as the Swiss, German, Danish and Austrian governments —depending on the project phase— accompanied by the supervision and technical support of the Italian government. The ICMPD's implementation of the BMP was part of being a key player in the EU border regime and its border control agenda (Naceur, 2021).

By the time these programs achieved certain goals in trainings and technical skills reinforcement of the Tunisian coast guard and other North African coast guards, ISMaris a locally developed software system for vessel detection, tracking and maritime surveillance focused on the Tunisian Gulf since 2020, has been supervised together by ICMPD and the Italian Ministry of Interior. This is part of the EU's structural adoption and use of surveillance tools for intercepting migrants at sea and facilitating arrests and deportations despite the harsh conditions and health problems that the people on these boats are experiencing. The Tunisian national coast guard still deploys the ISMaris system for interconnecting data gathered from GPS positions, VHF radar sensors which detect movement and boats presence, along with surveillance cameras on the associated vessels, all to provide relevant information for the EU (CMRCC, 2024).

Today, ISMAris could be playing a significant role in data exchange on suspicious grounds with other border control agencies and frameworks such as FRONTEX agency and EUROSUR information exchange EU program. Nonetheless, no direct connection has been proven yet besides the fund's association to the EU. This is based on the European Parliament's claim in 2020 that this technology is only a pathway to strategic and cross-regional communication and information exchange for maritime security and cooperation between Tunisia and Italy, as one of the goals behind implementing the BMP (European Parliment, 2020). Given the EU's financial contribution, the lack of governance of this technology from an independent entity makes it further difficult to assess the credibility of these claims and of ISMaris's applications as a technology.

However, activists and leaders of sea rescue boats and organizations are convinced that technologies such as the Tunisian ISMaris do not serve for regional security but rather for intercepting migrants before they reach Italian territory. The Tunisian national guard has reported that the total number of intercepted migrants between January and April 2024 alone has increased by approximately 22.07% from the previous year (Guard, 2024). These interceptions prevent SAR missions and organizations from intervening in a timely manner, despite the significant number of women, children and persons with severe medical conditions usually on board. This phenomenon demonstrates that, even if the EU claims that ISMaris' technological sovereignty is not linked to any non-Tunisian entity, it still advances the EU's broader international sovereignty agenda.

> **National vs international sovereignty is one of the many ways Italy and the EU are externalizing borders. Their purpose is to redefine shipwrecks on territory into migrants in 'transit'.**
>
> Mediterranean sea rescue activist

After the gradual investment in ISMaris, Italy renewed this new typology of tech-driven cooperations between Tunisia and Italy's ministries of interior by signing a memorandum of understanding in December 2023, confirming that the Tunisian Coast Guard is receiving six well-equipped patrol boats by June 2024, coinciding with the Tunisian government's inauguration of its proper SAR zone.

This overlapping of events was, according to sea rescue organizations, a systemic shadowing of the true purpose behind equipping Tunisia with sophisticated maritime vessels: pushbacks. These patrol boats include maritime surveillance network systems and integrated command systems that collect data from sensors such as a maritime radar for metal detection during navigation, and thermal imagery for identifying humans. In some cases, these technologies misidentify migrants, who are then wrongly labelled as smugglers or human traffickers.

They are also equipped with electro-optical sensors for underwater or low-light conditions, for intercepting communications, and for shadowing information exchanged between migrants (Abdul, 2024). The vessels provided for North African countries' maritime surveillance networks are not the only tech-facilitated strategy by Italy for border control. Leonardo-Finmeccanica is an Italian company leading the tech industry for military and maritime sectors, specializing in arms and defence technology in Italy and is amongst the leading companies in these sectors worldwide. The company is now assuming new responsibilities towards the Italian government by facilitating their surveillance and maritime arming technologies for cooperations with the Tunisian and Libyan coast guards (Middle East Monitor, 2024).

Leonardo's role is a piece of Italy's plan of recruiting North African countries for border control and is no longer limited to being a private company. Leonardo-Finmeccanica has been contracted as an implementing partner of the Mattei Plan, an Italy-Africa deal that doesn't disclose a lot of details on operations but aims at development cooperation between Italy and Africa (Middle East Monitor, 2024). Beyond serving a profitable agenda, Leonardo has been accused twice by human rights groups to be complicit in the political agenda of the Italian government regarding migration from African countries but refused to respond to the

allegations (Business and Human Rights Resource Centre, 2024). This is where the tech industry and the EU border regime meet and constitute further risks to human rights and lives.

## 02. Activist-targeting Spyware Attacks

One of the biggest threats to Italy and EU's plan for thwarting migration from Africa is the Italian and international networks of activists, lawyers and journalists who are exposing the facts and truths about the Italian government's 'puppeteering' strategy with North African countries, the systemic funding from the EU and the allocation of technological resources by third parties for pushbacks. The persistent efforts of advocacy and legal rights-driven resistance to violations and injustice has been closely monitored, especially by the Italian ministry of interior.

In February 2025, Meta, the tech giant behind WhatsApp, alerted one investigative journalist and two Italian activists that they had been targeted by a 'zero-click' cyberattack — an undetectable attack that requires no click action — which traced back to the Israeli tech company Paragon, specialized in cyber and forensic solutions. The spyware was installed in their WhatsApp accounts, along with dozens of others across Europe and was only dealt by Paragon with governmental contractors, which exposed a massive security breach for the actors targeted (Reporters Without Borders, 2025).

Both activists were founding leaders of non-governmental organizations supporting migrants in Italy, conducting rescuing missions and resisting Italy's pushbacks, while the journalist targeted was one of the most defying editors-in-chief who at that time was criticizing the right-wing governmental actions (though not strictly in relation to migration). This outrageous violation of privacy was a systemic and excessive abuse of power by the Italian government which, based on the profiles of the individuals targeted, is the only suspect from legal and contextual perspectives. The government initially denied the allegations before admitting the use of the surveillance tool on migrant activists, claiming it was a matter of national security (Kirchgaessner & Giuffrida, 2025b).

According to key activists and journalists recently targeted, the surveillance approach was expected from the Italian government, given its recent focus on deliberately shifting the narrative of migration from a cause of justice to a security issue for the EU. Nevertheless, the excessive use of digital military-grade technology was the true element of surprise for the targeted actors. It was an escalation of measures that the Italian government deemed justifiable in order to obstruct or end activists' efforts in advocacy, documenting human rights violations and rescuing migrants in the Mediterranean, a mission described by the Italian

government as a security issue when it admitted targeting civilians with invasive military technologies.

Based on digital forensics conducted by the research group *"CitizenLab"*, one of the targeted individuals confirms that the spyware attack was initiated at least as early as September 2024 and was neutralized around December 2024, shortly before Meta's alert (Marczak et al., 2025). They also stated that the fact that a military-grade spyware technology was used against them illegally and unethically is proof of how endless the Italian government's limits and costs can be. This includes the grave escalation of measures taken in considering human rights activists and fact-seeking journalists a national security issue.

When it comes to putting an end to migration flows from the Mediterranean Sea and to being one step ahead with the use of surveillance, Paragon's Graphite was considered a significant move against data protection and privacy of civil society actors, not only on their WhatsApp accounts but on the entire devices containing them. It was also a timely attack, given the attention on building a case with potential witnesses against Italy for allegations of being an accomplice to and aware of horrid crimes against Sub-Saharan migrants transiting in Libya, another key transit country to the EU in the North African region.

Amidst the legal actions undertaken by the cyberattack victims, and despite the contract termination between Paragon Solutions and the Italian government by the end of February 2025 (Kirchgaessner & Giuffrida, 2025a), further investigations have brought light to more journalists being affected by the "Graphite" spyware around June 2025, after which more individuals came forward once the digital forensics were shared (Marczak & Scott-Railton, 2025).

These recent discoveries are not only implicating but can also potentially lead to more cyberattack victims in Italy, Tunisia and Libya who may be representing obstacles to the Italian government's agenda. The spyware's link to the current government demonstrates how digital attacks against civil society have become a new form of warfare — one without arms — and a deliberate tool for reshaping narratives. Through these tactics, the Italian government seeks to evade responsibility for its actions toward migrants, whether on Italian territory, at sea, or in North African countries.

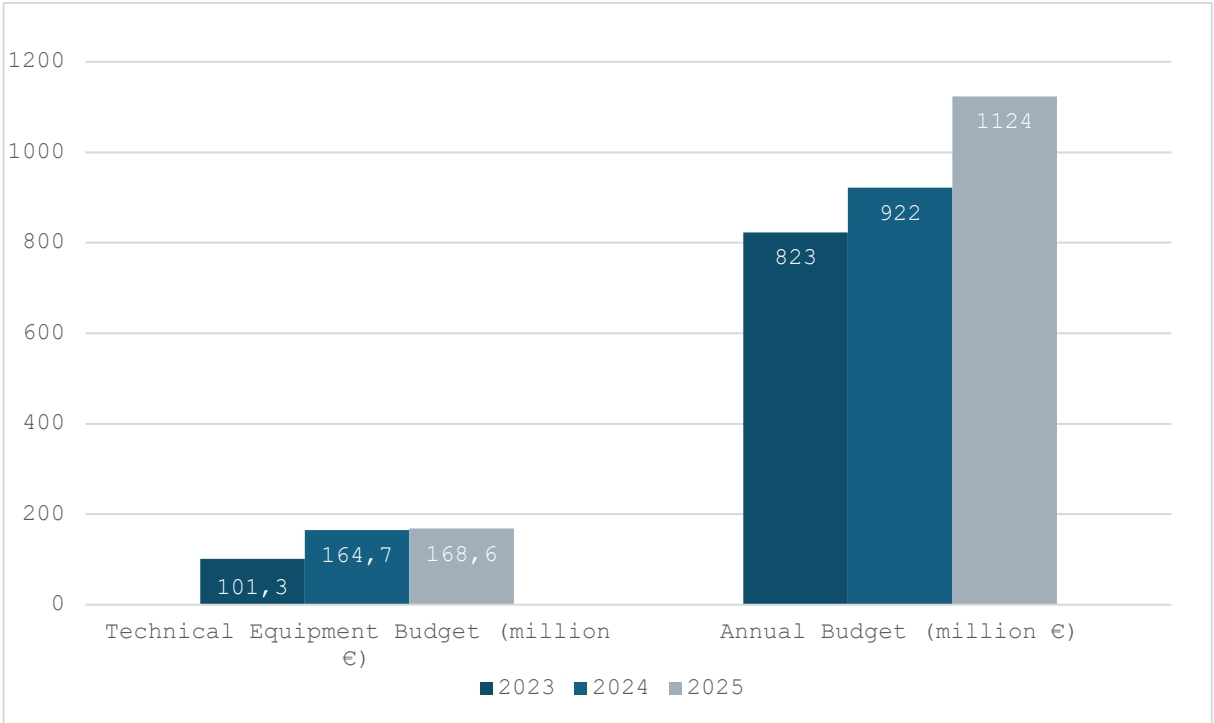
This jeopardizes the safety of migrants transiting in Tunisia as well as that of civil society actors supporting them, given Italy's long-standing supply of technical equipment to Tunisia, which deepens concerns over digital and human security.

## 03. Drone Surveillance: FRONTEX & The Tech Industry

While the Italian government's surveillance methods are more target-specific, there are still attempts of new methods in data collection, especially from migrants, that are supported by the Italian government and serve a coalition of other agencies in border control, pushbacks and mass deportations. The development, acquisition and deployment of many of these modern technologies was in initiatives led by FRONTEX. The agency's key role in this scheme is alerting Tunisian, Libyan and Egyptian coast guards as well as the neighbouring EU Mediterranean countries, when it comes to either interceptions or arrivals for deportation.

Italy's support, alongside that of Greece and Malta, extends to testing highly advanced unmanned aerial surveillance systems, commonly known as drones, particularly the medium-altitude long-endurance (MALE) models for maritime surveillance. This was confirmed in a FRONTEX statement announcing the renewal of a manufacturing contract with the German company ADAS, which joins the existing lead with the Israeli firm IAI (European Parliament, 2025b). The continuous technological contracting highlights FRONTEX's operational dependence on drones that identify migrants as security threats.

Figure 1: FRONTEX Technical and Annual Budgets (2023-2025)




*Sources:* Frontex Report on Budgetary and Financial Management in 2024 (European Parliament, 2025a) Budget 2025, Frontex Public Register of Documents (FRONTEX, 2024)

*Note. The ongoing 2025-year data refers to allocation and not expenditure.*

The agency's "Technical Equipment" budgetary line is one out of dozens of its financial segments. Although it mainly covers aerial surveillance systems and light technologies, it accounts for a significant share of the total yearly budget from 2023 to 2025. The figure above illustrates the steady yearly increase in funding for these unmanned systems, which continue to violate digital rights and identifiable data of migrants and asylum seekers at risk in the Mediterranean. Furthermore, for the first time in decades, the agency's annual budget allocation exceeds €1 billion, and it is already renewing contracts. From 2023 to 2024 alone, the contracted drones acquired by the agency recorded an almost 51% increase in flight hours over the Mediterranean from 3307 to 4993 flight hours of the German ADAS's Heron-1 drones (Monroy, 2025).

The concerns raised by many human rights defenders in the Mediterranean focused not only on the drones themselves, but also the associated risks and reasons behind the persistent use of AI to run those drones. It was an investment and complex testing phase of the use of AI systems such as the ones behind the drones deployed in the region. This testing phase is being extensively researched and examined as part of the EU-funded Horizon 2020 project that is further changing the narrative of migrants to security threats, but that the EU claims is enhancing research & development for external security services (Chiusi, 2024). This adds more risks to the injustice that migrants are already facing and could entail the integration of AI not only in facial recognition in the drones deployed by FRONTEX, but possibly also other acute decision-making processes, all of which require rigorous information exchange between the EU and other stakeholders.

## 04. Data Exchange & Migrants' Criminalization

The data exchange phenomenon for border control was once limited to databases compiled from EU border crossings' law enforcement and member states, such as the EURODAC and EU-LISA systems, which are deliberately used to monitor migration as a security issue. In 2025, new evidence emerged revealing a decade of exchanged brief reports and migrants' personal and biometric data between FRONTEX and EUROPOL, particularly concerning individuals who had been intercepted and were deemed suspicious (Fotiadis et al., 2025). The agency has been reprimanded by the EDPS for not complying with the EU regulations on data protection as an EU institution (European Data Protection Supervisor, 2025).

From 2016 to 2023, Frontex has been transferring reports containing data on migrants intercepted at border crossings, involving at least 13,000 individuals whose personal information was unlawfully transferred to EUROPOL databases, including those classified as criminal records (Stavinoha et al., 2025). This poses great risks to the identities of these

individuals and may implicate them in criminal activities identified by EUROPOL all without any legal grounds, even extending to their family members and next of kin.

> **Biometric data is collected for identifying 'suspects'. For the past few years, Frontex has said there are no guidelines or specific criteria to identify suspects.**
>
> Investigative journalist on FRONTEX

Tunisia's repeated compliance with the EU's expectations of contributing to putting an end to migration flows falls within the loophole of the 2023 EU-Tunisia deal (European Commission, 2023). The memorandum of understanding emphasizes cooperation between the two parties in the areas of mobility and migration. Nonetheless, Tunisia is also affected by the unlawful transfer of migrants data –Tunisian and Sub-Saharan alike– as EUROPOL's limited transparency regarding the use of data provided by FRONTEX indicates it may have been used for purposes of criminalization beyond allegations of smuggling and human trafficking. It is possibly being processed for suspicions of terrorism and other organized crimes that lack evidence and are subject to intentional or unintentional racial profiling of all African nationals.

# RECOMMENDATIONS

## Tunisia & the EU's Cooperation

- The Tunisian Ministry of Interior must revise current and future memorandums of understanding beyond the financial planning and exchange. This revision refers to the nature of the equipment and skills being shared by Italy and the EU as well as details on which party will be taking responsibility for any consequences when applying those skills with the technical equipment provided, especially beyond territorial waters.

  This measure is crucial for establishing red lines in any agreement between parties, ensuring the safe deployment of technologies, accountability for any abuses of power resulting from equipping Tunisia, and protecting human rights.

- The Tunisian Coast Guard must develop and publicly share safety guidelines and protocols to the SAR zone established in 2024, whereby intercepted migrants boats must first be examined for any passengers with critical medical conditions before relying solely on the technology for identification and immediate pushback.

- The Tunisian government, along with cooperating parties such as the EU and the Italian government, must commit to full transparency regarding any migration-related agreements or deals that may involve the use of outsourced technologies by the EU or the exchange of information collected through these technologies with other entities or institutions, particularly those affiliated with the EU.

- For accountability reasons, the Tunisian Ministry of Interior should cooperate with independent entities when conducting open investigations on any misuse and abuse of technical capacities and digital equipment (Tunisian or foreign) that may lead to a shipwreck during interceptions or to safety risks of people onboard.

  Similar to the European Data Protection Supervisor which oversees the regulation of data collection, processing and use in the EU, the Tunisian government must invite independent data and technology regulation bodies. These may include the National Authority for Protection of Personal Data to review the data behind the systems in use, or a coalition of independent experts to conduct thorough technical reviews, security audits and risk assessments from a rights-based perspective. Independent and specialized UN agencies such as the ITU could also be invited to contribute.

## EU Institutions, FRONTEX & EUROPOL

- EU institutions responsible for digital safeguards such as the GDPR and the EU AI Act must invoke laws and/or amendments to the existing frameworks, to fully regard and protect digital and human rights of migrants, refugees and asylum seekers. These frameworks must include personal and biometric data protection as well as the non-legal compliance of using AI during interviews at arrivals.

- EU institutions, member states and agencies such as FRONTEX and EUROPOL that may have taken part in unlawful exchange of personal and biometric data of migrants, especially when in vulnerable situations, must refer to any documents that could criminalize migrants based on racial profiling.

- In the contracting phase, the EU commission, as the responsible entity for public procurement of EU institutions' operations, must conduct and publicly share a full technical and legal review of the solutions offered by tech industry providers. These tech solutions and equipment must not be put in place without legal grounds and must not be used for unlawful mass surveillance, privacy invasion, sensitive data sharing and border externalization missions.

  The procurement phase of the EU commission must also include a thorough human rights impact assessment (HRIA) —a systemic process for evaluating and identifying negative impacts on human rights in a business, an operation or a project. The HRIA must take place with access to equipment for internal testing and share the outcomes of the assessment for independent review. This can help detect any discrimination resulting from facial recognition by the manufactured drones, as well as identify any data practices and safety gaps that expose migrants and asylum seekers' lives to danger.

## Civil Society Organizations & Actors

- Tunisian CSOs and regional Mediterranean rescue organizations must resist the technological invasion of their missions in advocating for migrants' rights and saving their lives by establishing cooperations with other actors in the digital rights community to build a stronger defence in the technology-migration nexus. This can be accomplished through multi-actor coalitions, collaborating with independent bodies responsible for reviews (e.g. technical, HRIA), exchanging technical/political knowledge and providing sufficient technical information from the industry and other sources, to mitigate the militarization of border control.

- Activists and journalists across the Mediterranean who are involved in criticizing the EU border control regime and Italian border externalization policies, and in building legal cases to seek justice for the violations committed, must maintain digital security checks for cyber-attacks in collaboration with trusted entities and digital rights organizations.

  New data protection measures should be established at both individual and organizational levels, particularly for databases containing information about the victims they represent. Finally, digital safety nets – such as back-up databases and private servers – should be set up in advance to mitigate any risks of criminalization and arbitrary arrests.

- Tunisian activists and organizations engaged with migrants in transit through the country must significantly contribute to their digital literacy, all while taking time sensitivity into account.

  Instructions and guidelines on how to protect their biometric and personal data and lawfully resist coerced data collection processes must be established and regularly conducted, so as to mitigate the risks of having their information transmitted across EU institutions and to prevent criminalization under suspicions of data correlation, based on racial profiling and discrimination.

# CONCLUSION

The Tunisia-Italy corridor for exchange and international cooperation has been built on different layers of strategies, all serving the EU plan for border externalization with the compliance of North African countries. Many of these layers consist of tech-facilitated methods for maritime surveillance, targeting boats for interception instead of rescue and reinforcing the Tunisian coast guard in using foreign technologies to assume territorial responsibility.

The international community of migrant rights activists, defenders, lawyers and journalists have been resisting this scheme in every possible way because human rights laws, supported by technical evidence, has more the power to shed light on the true narrative, that exposes how migration operations by EU institutions and the Italian government are now militarized and tech-weaponized with no safeguards or protection whatsoever. This led to targeting this community of civil societies with more surveillance and unethical collection and exchange of private and personal information, thus threatening the safety and freedom of people on the move.

The stakeholders involved in the excessive and invasive use of emerging technologies and equipment claim that their actions serve regional security. However, security should never come at the cost of human lives nor through unlawful and discriminatory measures. Tunisia, Italy, the EU and FRONTEX, along with other relevant institutions and alliances in North Africa, should be fostering unbiased safety protocols in their operations, ensuring that technology is not weaponized and that accountability is upheld for actions that affect the lives of migrants and asylum seekers.

# REFERENCES


Abdelmoula, M. R. (2024, 24 August). Maritime Search and Rescue: Tunisian Responsibility for European Problems. Legal Agenda. https://english.legal-agenda.com/maritime-search-and-rescue-tunisian-responsibility-for-european-problems/

Abdul, K. (2024, 1 October). *Italy supplies patrol boats to Tunisia* https://www.military.africa/2024/10/italy-supplies-patrol-boats-to-tunisia/

Alarmphone. (2024). *The Illegal and Violent Practices of the Tunisian National Guard in the Central Mediterranean*. https://alarmphone.org/wp-content/uploads/2024/06/Interrupted-sea-EN.pdf

Amnesty International et al. (2024, 4 October). *Joint Statement: Tunisia is Not a Place of Safety for People Rescued at Sea* https://www.amnesty.org/en/latest/news/2024/10/joint-statement-tunisia-is-not-a-place-of-safety-for-people-rescued-at-sea/

Business and Human Rights Resource Centre. (2024, 4 June). *Leonardo*. Business and Human Rights Resource Centre,. https://www.business-humanrights.org/en/companies/leonardo/#associated_allegations

Carrer, L., & Coluccini, R. (2022). *Technologies for border surveillance and control in Italy*. European Digital Rights (EDRi). https://edri.org/our-work/technologies-for-border-surveillance-and-control-in-italy/

Catelli, C. (2024). *Beyond walls and fences: EU funding used for a complex and digitalised border surveillance system*. PICUM the Platform for International Cooperation on Undocumented Migrants & ECRE European Council on Refugees and Exiles. https://picum.org/wp-content/uploads/2024/07/Beyond-walls-and-fences_EU-funding-used-for-a-complex-and-digitalised-border-surveillance-system_EN.pdf

Chiusi, F. (2024, 22 October). Automating EU Borders, Broken Checks and Balances. Algorithm Watch. https://algorithmwatch.org/en/automating-eu-borders/

CMRCC. (2024, 21 January). From Libya to Tunisia: How The EU is extending the push-back regime by proxy in the central Mediterranean. Civil MRCC. https://civilmrcc.eu/from-libya-to-tunisia-how-the-eu-is-extending-the-push-back-regime-by-proxy-in-the-central-mediterranean/

EU AI Act, (2024). https://artificialintelligenceact.eu/ai-act-explorer/

EU Council. (2024, 1 August). *Pact on Migration and Asylum* https://home-affairs.ec.europa.eu/policies/migration-and-asylum/pact-migration-and-asylum_en

European Commission. (2023). *Memorandum of Understanding on a strategic and global partnership between the European Union and Tunisia*. European Commission, Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3887

European Data Protection Supervisor. (2025, 8 January). *EDPS reprimands Frontex for non-compliance with Regulation (EU) 2019/1896* https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/edps-reprimands-frontex-non-compliance-regulation-eu-20191896_en

European Parliment. (2020). Parliamentary question - E-003820/2020(ASW). In: European Parliment.

European Parliment. (2025a). *Frontex Report on Budgetary and Financial Management in 2024* https://www.europarl.europa.eu/cmsdata/294489/Frontex%20BFMR%202024.pdf

European Parliment. (2025b). Parliamentary question - E-000420/2025(ASW). In: European Parliment.

EUTF. (2018). *Border Management Programme for the Maghreb region (BMP-Maghreb)*. European Union,. https://trust-fund-for-africa.europa.eu/our-programmes/border-management-programme-maghreb-region-bmp-maghreb_en

EUTF. (2024). *Emergency Trust Fund for Africa*. European Union. https://trust-fund-for-africa.europa.eu/index_en

Fotiadis, A., Hierro, L., & Stavinoha, L. (2025, 7 July). Frontex unlawfully shared thousands of people's personal data with European police. *Le Monde*. https://www.lemonde.fr/en/les-decodeurs/article/2025/07/07/frontex-illegally-shared-thousands-of-people-s-personal-data-with-european-police_6743113_8.html

FRONTEX. (2024). *Budget 2025*. https://prd.frontex.europa.eu/document/budget-2025/

FTDES. (2025, 30 April). *Tunisia's designation as a safe third country of origin: The European Commission rewards Tunisian authorities for their cooperation on migration and whitewashes their abuses* https://migreurop.org/article3410.html

Gandhi, S. (2024). Frontex as a hub for surveillance and data sharing: Challenges for data protection and privacy rights. *Computer Law & Security Review*, *53*, 105963. https://doi.org/https://doi.org/10.1016/j.clsr.2024.105963

Garavoglia, M. (2024). *Le rôle des financements européens sur la migration dans les pratiques violentes des autorités sécuritaires tunisiennes*. Tunisian Forum for Social & Economic Rights (FTDES). https://ftdes.net/le-role-des-financements-europeens-sur-la-migration-dans-les-pratiques-violentes-des-autorites-securitaires-tunisiennes/

Guard;, T. N. (2024, 12 May). إحصائية جديدة ورسمية عن ظاهرة الهجرة غير النظامية. *Al Horria*. https://alhorria.com/2024/05/12/%d8%a5%d8%ad%d8%b5%d8%a7%d8%a6%d9%8a%d8%a9-%d8%ac%d8%af%d9%8a%d8%af%d8%a9-%d9%88%d8%b1%d8%b3%d9%85%d9%8a%d8%a9-%d8%b9%d9%86-%d8%b8%d8%a7%d9%87%d8%b1%d8%a9-%d8%a7%d9%84%d9%87%d8%ac%d8%b1%d8%a9-%d8%ba/

Kirchgaessner, S., & Giuffrida, A. (2025a, 12 June). European journalists targeted with Paragon Solutions spyware, say researchers. *The Guardian*. https://www.theguardian.com/media/2025/jun/12/european-journalists-targeted-with-paragon-solutions-spyware-say-researchers

Kirchgaessner, S., & Giuffrida, A. (2025b, 27 March). Italian government approved use of spyware on members of refugee NGO, MPs told. *The Guardian*. https://www.theguardian.com/world/2025/mar/27/italian-government-approved-use-of-spyware-on-members-of-refugee-ngo-mps-told

Marczak, B., & Scott-Railton, J. (2025). *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*. CitizenLab. https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

Marczak, B., Scott-Railton, J., Robertson, K., Perry, A., Brown, R., Razzak, B. A., Anstis, S., & Deibert, R. (2025). *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*. CitizenLab. https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/

Middle East Monitor. (2024, 31 January). Italy-Africa deal is 'border control disguised as aid', say rights groups. Middle East Monitor. https://www.middleeastmonitor.com/20240131-italy-africa-deal-is-border-control-disguised-as-aid-say-rights-groups/

Molnar, P. (2023, 20 December). EU's AI Act Falls Short on Protecting Rights at Borders. Just Security. https://www.justsecurity.org/90763/eus-ai-act-falls-short-on-protecting-rights-at-borders/

Monroy, M. (2025, 15 April). Frontex significantly expands drone operations. neues deutschland. https://www.nd-aktuell.de/artikel/1190562.migrationsabwehr-frontex-weitet-drohneneinsaetze-deutlich-aus.html

Naceur, S. P. (2021). *Decrypting ICMPD*. Tunisian Forum for Social & Economic Rights (FTDES). https://ftdes.net/rapports/DecryptingICMPD.pdf

Napolitano, A. (2023). *Artificial Intelligence: The New Frontier of the EU's Border Externalisation Strategy*. Euromed Rights. https://euromedrights.org/wp-content/uploads/2023/07/Euromed_AI-Migration-Report_EN-1.pdf

Napolitano, A., & Barker, H. (2025, 13 January). Europe's Digital Border Wars: How the EU's Facilitation Package is Another Step in Europol's Unjustified Power Expansion. Border Criminologies. https://blogs.law.ox.ac.uk/border-criminologies-blog/blog-post/2025/01/europes-digital-border-wars-how-eus-facilitation

OMCT. (2023). *Torture Roads: Mapping of violations suffered by people on the move in Tunisia*. W. O. A. T. O. M. C. l. T.-. OMCT). https://omct-tunisie.org/wp-content/uploads/2024/05/Migration-et-torture-Pages-EN-OMCT.pdf

Reporters Without Borders. (2025, 3 March). Italian government must explain spyware surveillance of journalist Francesco Cancellato. Reporters Without Borders. https://rsf.org/en/italian-government-must-explain-spyware-surveillance-journalist-francesco-cancellato

Rijtano, R. (2023, 10 July). Drones in Niger and radar in the Mediterranean: EU spends billions on high-tech borders. LaviaLibera. https://lavialibera.it/en-schede-1482-eu_spends_billions_on_high_tech_borders_against_migrants

Soverino, R. (2024, 7 February). Biometric Data, Data Protection Authorities, and Migrants: A Complex Nexus. OpinioJuris. https://opiniojuris.org/2024/02/07/biometric-data-data-protection-authorities-and-migrants-a-complex-nexus/

StateWatch, & Euromed Rights. (2023). *Europe's Techno Borders*. https://www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/

Stavinoha, L., Fotiadis, A., & Hierro, L. (2025, 7 July). Frontex unlawfully shared thousands of people's personal data with Europol. *Solomon*. https://wearesolomon.com/mag/format/investigation/frontex-unlawfully-shared-thousands-of-peoples-personal-data-with-europol/

Vavoula, N. (2024, 16 October). The transformation of EURODAC from an asylum tool into an immigration database. EU Migration Law Blog. https://eumigrationlawblog.eu/the-transformation-of-eurodac-from-an-asylum-tool-into-an-immigration-database/