SPECTO MEDIA

BORDER BUSINESS

The Data Market

EPISODE 1

November 2025

Last October, a new European database came into effect. From now on, all non-European citizens crossing the borders of an EU member state will have their biometric data electronically recorded in a single system. This new screening mechanism is part of a broader security reform that threatens individual freedoms and the right to privacy.

By testing new control technologies at its borders, the European Union is normalizing mass surveillance while upholding a racist and capitalist order.

"Legitimizing this kind of system or tool for foreign nationals will then pave the way for those kind of things to be used in different areas against European citizens. This is why people should care about what happens to foreign nationals in their country or those who are trying to come into it, because if a government can do it to them, it can also do it to you." **Chris Jones, Statewatch**

What is the Entry/Exit System (EES)?

Over the next six months, the Entry/Exit System (EES) will be gradually implemented in train stations, airports, seaports, and at the EU's external border crossings. When passing through these entry points, all non-EU nationals traveling to the EU for a short stay (up to 90 days) will now be required to provide their fingerprints and a biometric photograph. This information, along with the travelers' personal data, will then be recorded and stored in a centralized European database[1].

The EES is being added to the three databases already in place, which are designed to ensure the security of the European area[2]. By systematically recording the entries and exits of third-country nationals traveling within the EU, as well as identifying individuals who have previously been refused entry, the European Commission aims to strengthen the monitoring of foreign travelers and to detect, more quickly through an automated calculation system those who exceed their authorized length of stay.

To verify whether a person poses a threat to the integrity of the European Union, a data-matching software will consult European and international information systems. No fewer than 700 million people are expected to be affected by the large-scale analysis and storage of their data[3].

1. The collection of biometric information will take place upon the traveler's first entry into the European area. For subsequent crossings, scanning the passport will allow the necessary checks to be carried out (biometric identity verification, potential entry refusal for a short stay) as well as the recording of personal data (date and time of entry and exit, place of entry and exit, the traveler's passport number, etc.). This data will be stored for a period ranging from three to five years.

2. Eurodac, the Schengen Information System (SIS), and the Visa Information System (VIS). Two additional information systems will also be added to the existing databases in the coming months: the European Travel Information and Authorization System (ETIAS) and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

3. Schengen News, "EU Confirms Official Entry/Exit System Launch Date", 19 August 2024.

What is biometrics, and how has this technology become a tool for controlling bodies?

Biometrics is an identification system based on physical characteristics unique to each individual (fingerprints, facial images, iris scans, palm prints, etc.). This technology for managing bodies is part of a long history of exclusion and surveillance of populations deemed "undesirable." According to several historians, its logic dates back to the 17th-century slave system, where physical characteristics were already used to identify and track Black bodies during the slave trade.[4]

Biometric technologies, first experimented with in European colonial empires at the end of the 19th century, were later developed to monitor, classify, and control colonized populations. The accumulation of data on oppressed minorities was at the core of colonial power structures, ensuring the continuity of domination. These contexts gave rise to mass identification techniques, such as fingerprint recognition, establishing a racialized control over populations. The refinement of these identification techniques gradually helped extend this system of control to all citizens in Western societies.

Today, biometric data no longer serve merely to identify the holder of a passport: they determine access to the very rights that this document is supposed to guarantee. By combining and universalizing these control mechanisms, Western states have consolidated an unequal and racialized border regime, effectively reserving the right to free movement for populations from the wealthiest countries.

Driven by the desire to secure the internal free-movement area, European institutions have established, since the 2000s, several biometric databases that reinforce mobility hierarchies. The recent expansion of these large-scale information systems allows them to collect ever more data and broaden the number of actors authorized to access it. These mechanisms now form the foundation of an invisible border, built on a technological arsenal for surveillance and sorting of bodies.

4. Design -Politics. An inquiry into passeport, camp and borders", Mahmoud Keshavarz, 2016.
5. Arrêt sur image, "La reconaissance faciale ou l'oeil, du colonisateur", November 2021.

What is a “virtual wall[6]” ?

A “virtual wall” refers to a set of technological measures designed to reinforce physical barriers and complement the work of border guards. The cross-referencing of data, combined with the use of computer tools for processing and analysis, allows authorities to sort and control people even before they reach the borders. The use of these control technologies is part of the European “smart borders” strategy, launched in 2011 by the European Commission. This strategy envisions the implementation of a cutting-edge technological architecture aimed both at strengthening security within the European area and facilitating the “fluidity” of movement.

Biometric databases and their operating software are an integral part of the deployment of smart borders. Presented as a condition for maintaining the free movement of people within the European area, the use of these new technologies is intended to speed up decision-making and monitor migratory movements, through the accumulation of data considered necessary for risk assessment.

What is ETIAS, and how does the automated profiling system work?

This new system, which is equivalent to the American ESTA, is not a database. The European Travel Information and Authorization System (ETIAS) is an IT system responsible for assessing, using an algorithm, the potential risk level a traveler may pose. This automated technology, which applies to visa-exempt nationals, will issue a pre-entry authorization for the EU after an individualized profiling process. It complements the Entry/Exit System (EES).

6. TEDx Talks, “Les murs, symboles de frontières”, Damien Simonneau, July 2025.

Decision-making will rely on an algorithm tasked with sorting authorization requests and creating an individual profile for each traveler. The system for recording individuals is based on cross-referencing information contained in European and international databases (EES, VIS, SIS, Europol, and Interpol), as well as matching against a watchlist[7]. o carry out its assessment, the ETIAS system will compare the personal data provided by travelers with "risk indicators"[8] predefined by the ETIAS central unit, under the responsibility of the Frontex agency[9]. According to Amnesty International, personal data freely available on the Internet could also be used by the algorithm[10].

Even though European regulations prohibit the algorithm from taking into account a person's ethnic origin, religion, or political opinions when assessing their risk level, some travelers could still be categorized in a discriminatory manner. The selection criteria defined in the ETIAS algorithm risk reinforcing biases and restricting the movement of individuals deemed to pose a potential threat, whether security-related, health-related, or migration-related. By relying on an automated sorting logic, the ETIAS decision-making system could amplify the discrimination already present in the global mobility regime.

"It is obvious that your address can serve as a proxy for your race, because if you come from a neighborhood that is predominantly Black or Asian, it can be inferred. The criteria can thus ascribe a racial category. One can imagine that young men of a certain age are more likely to be flagged as security risks".

Chris Jones, Statewatch

7. This watchlist will be updated by the Frontex agency as well as the police agency Europol. However, this surveillance mechanism raises concerns about potential abuses and the arbitrary nature of entry refusals that could result from a traveler being on the list. In reality, it serves as a way to bypass existing European regulations, since the listing is supposed to concern individuals who are "suspected of being involved in terrorist acts or serious offenses," but whose information is not sufficiently substantiated or justified to have their data entered into the Schengen Information System (SIS).
8. The risk assessment system is based on defining risk indicators such as age range, nationality, country and city of residence, travel destination, purpose of travel, level of education, and profession. See Statewatch, "Frontex and interoperable databases : knowledge as power ?", february 2023.
9. Regulations stipulate that the members of the ETIAS board define which risk indicators may violate the law. Despite the presence of a Fundamental Rights Advisory Committee within the board, it has no binding authority.
10. Amnesty International, "Primer : Defending the rights of refugees and migrants in the digital age", March 2024.

What are the risks to human rights?

According to the CNIL, automated decision-making systems have flaws and are "likely to result in inaccurate analyses and predictions, unjustified service denials, or other decisions that are detrimental to individuals, to perpetuate stereotypes, and to trap people in their choices."[11]

The risk of excluding certain populations is all the greater as the Committee on the Elimination of Racial Discrimination (CERD) has reminded, in a series of reports[12], that new technologies cannot be separated from contemporary social structures. From the design phase onward, racial biases are reproduced and embedded into the systems. The risk of racial profiling, inherent in automated decision-making systems based on databases, is thereby exacerbated.

Although human rights defenders have been raising concerns about algorithmic failures for several years, institutional discourse continues to present these technologies as objective and neutral governance tools. While European legislation prohibits entry refusals without human intervention, the high volume of applications and the pressure of automated decisions generated by ETIAS could heavily influence the final decision.

Moreover, neither the EES nor ETIAS has undergone impact assessments. It therefore remains uncertain whether the development of these technologies which pose risks to human rights and privacy protection actually enhances the EU's internal security. The ETIAS project had already been discussed in 2008, before being ultimately abandoned by the European Commission, which argued that its "potential contribution to enhancing the security of the Member States would neither justify the collection of personal data at such a scale nor the financial cost". However, the 2015 terrorist attacks and the so-called "migration crisis" reactivated the project, leading to the creation of an increasingly complex technological border architecture[14].

11. CNIL, "Profilage et décision entièrement automatisée", May 2018.
12. Committee on the Elimination of Racial Discrimination (CERD), Racial discrimination and emerging digital technologies: a human rights analysis Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, Xenophobia, and Related Intolerance, July 2020.
13. European Commission, "Smart borders - options and the way ahead", COM(2011) 680 final, 25 October 2011.
14. The reform concerning large-scale information systems is based on the concept of interoperability. It enables the networking of existing databases to cross-reference available information. This architecture tends to blur the boundaries between police, civil, and humanitarian uses, undermining the principle of proportionality, according to which any state interference in private life must be justified by a legitimate and strictly defined objective.

"The issue is that this is a kind of security theatre within the European Union. These policies don't really address the fundamental causes of problems but rather deal with certain symptoms that governments believe can be solved through the identification, tracking, and control of people." **Chris Jones, Statewatch**

The pursuit of economic interests by private companies, and their predominant role in the dissemination of surveillance technologies, also raise major questions regarding their responsibilities in data protection, privacy, and the safeguarding of fundamental rights.

What is the role of tech companies in strengthening border controls?

To fortify itself, the EU has continuously increased the budget allocated to border security. According to Euromed Rights, compared to the 2014–2020 budget period, the total contributions to the EU's border policy budget have risen by 94%[15].

For the development of the Entry/Exit System (EES), a consortium of companies, including industry giants IBM, Atos, and Leonardo, was awarded a contract worth €142 million. The sBMS (shared Biometric Matching System), a crucial component of the EES that allows biometric data to be cross-referenced across different databases, was awarded to Idemia and Sopra Steria under a €300 million contract.

European political ambitions, aimed at collecting as much data as possible to identify and then control citizens of so-called third countries, rely increasingly on specialized companies with close ties to power. In addition to intense lobbying by private companies, there is a regular movement of technocrats between industrial groups and European institutions. Thus, the company Atos welcomed Agnès Diallo into its ranks, a former executive who was later appointed as the director of the European agency eu-LISA[16], as well as Thierry Breton, a former European Commissioner who had led the group before taking office in Brussels. This creates a clear conflict of interest between companies benefiting from public contracts for the development of these systems and the institutions that hold power.

15. Euromedrights, "Europe's Techno Borders", July 2023.
16. Eu-LISA is a European government agency responsible for managing large-scale information systems within the Area of Freedom, Security, and Justice. It is the institution in charge of awarding part of the public contracts related to the management and development of these databases.

The European Union's security policies are built with a small conglomerate of private companies that have become indispensable across the entire development chain (data storage, system maintenance, cybersecurity, etc.). Surveillance technologies, developed in particular with European public funding for research and development, can later be marketed and sold to both states and European institutions.

The lack of clear rules governing the spread of new technologies risks exacerbating violations of fundamental rights, especially since the companies responsible for their development have already been implicated in the misuse of technological tools for authoritarian purposes.

This is a long-standing tradition, notably for IBM, which collaborated with the Nazi regime by implementing a data collection system on Jewish people that facilitated the execution of the Holocaust[17]. The company has also been accused of complicity in the ongoing genocide in Gaza[18], and is suspected of having sold facial recognition software to the Kazakh government, used to monitor and repress regime opponents[19]. Atos is no exception: its subsidiary Amesys has also been implicated in selling surveillance software to authoritarian regimes, notably in Libya[20].

What are the long-term consequences of such systems?

Since the September 11, 2001 attacks, fear-based discourses portraying immigration as a threat to the internal security of the EU have intensified, further justifying and legitimizing the use of mass surveillance technologies. By intertwining counter-terrorism and crime-fighting concerns with migration issues, the EU and its Member States contribute to the construction of a stigmatizing discourse and the criminalization of people on the move.

17. The Guardian, "IBM 'dealt directly with Holocaust organisers'", March 2002.
18. Al Jazeera, "UN report lists companies complicit in Israel's 'genocide': Who are they?", July 2025.
19. ARTE, "Reconnaissance faciale : des entreprises de la tech au cœur de la surveillance", October 2025.
20. EDRi, "Amesys – Complicity in torture: surveillance tech export control needed", May 2012.

With the EES and ETIAS, the European Union is establishing a generalized suspicion toward all travelers[21]. It is no longer just about verifying identities, but about monitoring and assessing the very legitimacy of individuals to move within the European area through an algorithmic selection process. The introduction of these new technologies adds another layer to a free-movement space where travelers deemed "low-risk" can move freely and safely, while racialized or marginalized individuals may be denied entry to the European Union based on presumed risk assessments.

With the removal of internal border barriers, the outsourcing of external borders, and the strengthening of individualized surveillance and control have become two sides of the same coin. The creation of a two-tiered mobility space reflects a racist approach to border management[22]. These obstacles exacerbate border violence, notably by forcing people deemed "undesirable" to circumvent official systems and take secondary or informal routes, putting their safety at risk[23].

"In a context marked by the rise of right-wing governments, xenophobia, and anti-immigrant sentiment, these technologies can very easily be abused by governments with bad intentions to identify and track individuals, particularly through biometrics and live facial recognition. A look at European history over the past century shows that massive registers containing information on people deemed 'undesirable' have often been used by the extreme right for profoundly despicable purposes."

Chris Jones, Statewatch

21. Statewatch, "Automated suspicion. The EU's new travel surveillance initiatives", July 2020
22. Building walls, "Fear and securitization in the European Union", Centre Delàs d'Estudis per la Pau, November 2018.
23. "Digital Racial Borders", E. Tendayi Achiume, 2021.

Through the convergence of economic interests and European security concerns, mass surveillance is legitimized to extend the racialized control of mobility. Computer systems reproduce and amplify the social inequalities and discriminations present in our societies, while making them difficult to challenge, thereby reinforcing the arbitrary nature of movement restrictions.

Unlike a wall, which retains primarily a symbolic dimension, the control technologies deployed at borders operate discreetly and obscure the fate of people on the move. Despite their deeply concerning ethical implications, these surveillance mechanisms shape an opaque reality without sparking any debate on the future of our societies. In short, these systems are creating a new architecture of power, where the border is no longer merely a geographic line but an algorithmic apparatus capable of filtering, classifying, and hierarchizing human lives.

Press Contact

- **Author -** Maëlle Parfait
- **Founder of Specto Média -** Eléonore Plé // contactspecto@gmail.com