TRENDREPORT 10

January / 2026

ALGORITHMIC TRUTH-MAKING: FROM BORDER CHECKPOINTS TO ALWAYS-ON FILTERS

Özgecan Eskiduman

Österreichisches Institut
für Internationale Politik
Austrian Institute
for International Affairs

EXECUTIVE SUMMARY

States are shifting from analogue checkpoint-based border control to “algorithmic truth-making.” Automated verification systems increasingly determine which identity information counts as credible, and which signals are treated as risk before travel begins.

In 2025–2026, the EU becomes the most visible laboratory: the Entry-Exit System (EES), fully operational from April 2026, and the European Travel Information and Authorisation System (ETIAS), expected in the last quarter of 2026, are normalizing upstream biometric registration and pre-travel screening.

Comparable pre-travel permission regimes already structure mobility beyond Europe, notably through the US Electronic System for Travel Authorization (ESTA) and the UK’s Electronic Travel Authorisation (ETA), with enforcement increasingly embedded in carrier workflows.

The trend is sustained by security-driven politics, procurement lock-in, and commercial incentives, yet it remains exposed to legal challenges, cyber incidents, and systemic epistemic failures such as misidentification or manipulated data spreading across interoperable systems.

Three scenarios are likely: routine mobility scoring through continuous verification, a scandal-led reset that tightens oversight and redress, or vendor dominance in which technology firms become key intermediaries in digital border security.

KEYWORDS:
Border control, mobility governance, algorithmization, automation

ZUSAMMENFASSUNG

Staaten gehen von analogen Grenzkontrollen an Kontrollpunkten zu “algorithmischer Wahrheitsfindung” über. Automatisierte Verifizierungssysteme bestimmen zunehmend, welche Identitätsinformationen als glaubwürdig gelten und welche Signale vor Reiseantritt als Risiko eingestuft werden.

In den Jahren 2025–2026 wird die EU zum sichtbarsten Versuchslabor: Das Einreise-/Ausreisesystem (EES), das ab April 2026 voll funktionsfähig sein wird, und das Europäische Reiseinformations- und -genehmigungssystem (ETIAS), das im letzten Quartal 2026 erwartet wird, normalisieren die vorgelagerte biometrische Registrierung und die Überprüfung vor Reiseantritt.

Vergleichbare Genehmigungssysteme vor Reiseantritt strukturieren bereits Mobilität außerhalb Europas, insbesondere durch das US-amerikanische Electronic System for Travel Authorization (ESTA) und das britische Electronic Travel Authorisation (ETA), wobei die Durchsetzung zunehmend in Arbeitsabläufe von Beförderungsunternehmen integriert wird.

Dieser Trend wird durch sicherheitsorientierte Politik, Beschaffungsbindung und kommerzielle Anreize gestützt, bleibt jedoch rechtlichen Herausforderungen, Cybervorfällen und systemischen, epistemischen Fehlern wie Fehlidentifikationen oder manipulierten Daten, die sich über interoperable Systeme verbreiten, ausgesetzt.

Drei Szenarien sind wahrscheinlich: die routinemäßige Mobilitätsbewertung durch kontinuierliche Überprüfung, eine skandalbedingte Neugestaltung, die die Monitoring und Schadensersatz verschärft, oder eine Dominanz der Anbieter, bei der Technologieunternehmen zu wichtigen Vermittlern in der digitalen Grenzsicherheit

KEYWORDS:
Grenzkontrolle, Mobilitätssteuerung, Algorithmisierung, Automatisierung

AUTHOR

Dr. Özgecan Eskiduman

is an Ernst Mach Fellow at the oiip from September 2025 until May 2026. She holds a PhD in International Relations at Hacettepe University. Her doctoral research focuses on Israeli security narratives and ontological security in the context of the First and Second Palestinian Uprisings. She has worked as a research assistant on several nationally funded projects in Türkiye, including studies on counterterrorism, social polarisation, and migration. At the oiip, her research focuses on European security discourses, with a particular emphasis on migration and ontological security. Her broader academic interests include critical security studies, terrorism, identity politics, narrative analysis, Middle East politics, Israeli foreign policy, foreign policy analysis, and conflict studies.

IMPRESSUM:

Österreichisches Institut für Internationale Politik – oiip,
Austrian Institute for International Affairs
A-1090 Vienna, Währinger Straße 3/12,
www.oiip.ac.at, info@oiip.ac.at

ALGORITHMIC TRUTH-MAKING: FROM BORDER CHECKPOINTS TO ALWAYS-ON FILTERS

Digital borders increasingly operate as data-driven "truth-making" infrastructures: they do not just monitor movement but decide which pieces of identity information count as credible, which signals are treated as risk, and which travelers become machine-verifiable long before any face-to-face control at a checkpoint. This report approaches digital borders through a security and pre-emptive governance lens, highlighting how border control is shifting from reactive checks at the line to anticipatory risk management that operates upstream, before departure, during booking, and through carrier compliance.

Algorithmic truth-making matters because it shifts the core question from "Who is admissible?" to "Which information is admissible?"

> *Border control is shifting from reactive checks at the line to anticipatory risk management that operates upstream, before departure, during booking, and through carrier compliance*

As mobility governance becomes more data-driven, credibility is increasingly shaped through automated verification and inference, often on the basis of incomplete or outdated records, false matches or politically contested data resources. In such settings, travelers, especially visa-required nationals, asylum seekers, and racialized groups, can be excluded not on the basis of how they are profiled, but through the way data about them is assembled, matched, and interpreted across the systems. In practice, this kind of exclusion can take the form of being refused an e-visa or ETIAS-style authorisation, being denied boarding by airlines, being channelled into repeated secondary screening, or, in more coercive contexts, being detained at checkpoints or removed from the territory. These processes often lack transparency and are difficult to challenge, especially when automated inferences shape outcomes without a clear explanation (Wachter and Mittelstadt, 2019). While digital borders affect a broad range of travelers, their most intrusive and risky effects are concentrated on people who move from precarious legal and social positions, such as asylum seekers, people with temporary or uncertain status, and racialized groups coming from contexts of war, repression, or deep economic crisis. For them, delay or exclusion can mean losing access to protection or legal routes.

The idea of digital borders is not brand-new. Since the 2000s, EU databases such as the Schengen Information System (SIS), the European Asylum Dactyloscopy Database (Eurodac) and the Visa Information System (VIS) have already transformed border control into a data-intensive enterprise, especially for third-country nationals (Broeders, 2007, pp.

71–73). What is new around 2025–2026 is the scale, integration, and everydayness of this model. Recent scholarship describes a move from single databases to networked infrastructures in which biometric identifiers, passenger name records, visa data, and "travel histories" are continuously linked and analyzed (Leese et al., 2022, pp. 6–8). Border control is no longer centered at a physical site. It increasingly operates through continuous data flows. Airlines pre-check passengers, travelers facing authorization portals and carrier check-in systems request and validate permissions, and risk scores shape who is waved through, delayed, or stopped.

> *Digital bordering relocates sovereign gatekeeping into data infrastructures and pre-travel decision points*

This challenges three accepted narratives in International Relations. First, that borders are primarily territorial lines, whereas digital bordering relocates sovereign gatekeeping into data infrastructures and pre-travel decision points. Second, that bordering is a state monopoly, whereas carriers, platforms, and private vendors now become operational extensions of security governance. Third, border control is often assumed to be reactive, yet pre-emptive governance increasingly treats mobility as a forecastable risk and manages it upstream.

> *By grouping security, migration, and public health under the same risk logic, ETIAS reinforces a political framing in which cross-border mobility is first and foremost a potential threat to be managed*

VISIBLE SHIFTS IN BORDER PRACTICE

Several early signals underpin this trend. First, the EU has become the most visible laboratory of algorithmic truth-making at the border. The Entry/Exit System (EES) began operations on October 12, 2025, and replaces passport stamping with biometric registration and a centralized digital record of entry and exit, becoming fully operational at all external border crossing points from April 10, 2026 (European Commission 2025; 2025a). The European Travel Information and Authorisation System (ETIAS), expected to start operations in the last quarter of 2026, adds a pre-travel screening layer for visa-exempt visitors, explicitly designed to identify "security, irregular migration or high epidemic risks" before travel begins (European Commission, 2025b). By grouping security, migration, and public health under the same risk logic, ETIAS reinforces a political framing in which cross-border mobility is first and foremost a potential threat to be managed, rather than a right or routine practice. Together, these systems aim to normalize upstream verification as a routine condition of mobility, not an exceptional security measure, and they are likely to feed into domestic debates in Europe about who is "risky," who is "trusted," and how far pre-emptive control should reach.

Second, similar pre-travel permission regimes are already embedded beyond the EU, notably through the Electronic System for Travel Authorization (ESTA) in the United States and the Electronic Travel Authorisation (ETA) in the United Kingdom. Under the US Visa Waiver Program, travelers are required to obtain ESTA approval before boarding, turning acceptability into a pre-departure, data-based decision point (U.S. Department of State 2024; U.S. Customs and Border Protection 2025). The UK's ETA functions similarly as a digital permission to travel and is operationalized through carrier checks that effectively move enforcement into airline and ferry workflows (Kemp and Bossong, 2020). This broader pattern signals that "the border" is increasingly encountered during booking, check-in, and boarding, rather than only at a territorial line.

Third, these systems are spreading through external cooperation and migration governance partnerships. EU and member state funding and assistance increasingly support border management capacity, surveillance, and digital infrastructure in partner countries, extending European bordering practices beyond EU territory (Bellanova and Gonzalez Fuster, 2019). As partners build border capacity through technology transfers, training, and equipment, new upstream filtering points often appear along routes and in neighboring regions. These points shape who is sorted, flagged, or delayed long before any EU checkpoint.

Fourth, interoperability and risk analysis are becoming central to how digital borders operate in practice. EU policy has increasingly emphasized integrated border management and the use of large-scale information systems that enable data to be searched and compared across border, police, and migration authorities (Baceiredo Macho, 2025, pp. 1–2). This shift also reflects a broader move toward governing mobility through databases and routine data practices. Interoperability is not only a technical upgrade. It is designed to verify and cross-validate identities across systems through shared biometric matching and multiple identity detection (European Parliament and Council of the European Union, 2019). In practice, this means that matches, mismatches, and alerts can travel across connected infrastructures, and decisions may become harder to challenge because credibility is produced across a network rather than through a single assessment (Leese, 2022).

For asylum seekers and others moving from precarious legal and social positions, this networked architecture reinforces the EU's long-standing strategy of outsourcing and externalising control. Carriers, third countries and pre-border filters are expected to stop people before they reach EU territory and before they can submit an asylum claim. Digital interoperability does not abolish the 1951 Geneva Refugee Convention, but it helps maintain an "architecture of containment" in which refugee protection is handled through externalisation, procedural delay, and delegation (Davutoglu 2025). For asylum seekers, this builds on earlier responsibility-sharing rules such as the Dublin system, which already allocates the asylum procedure to the country of first entry and relies heavily on centralized registration (Council of the European Union, 2025). In practice, this data-driven "Fortress Europe" keeps the formal framework of protection in place while rendering itself less and less accessible.

STABILITY AND POTENTIAL TREND BREAKERS

Several reinforcing factors suggest that algorithmic truth-making at the border will not disappear quickly, which makes the trend relatively robust. Security and control logics remain central to contemporary border and mobility governance, which makes data-rich tools politically attractive (Leese et al. 2022, pp. 6–7). In policy debates, such systems are often presented as delivering more efficient and targeted control, reducing visible human error and showing that governments are "in control" of the border at relatively low political cost. Institutional and financial lock-in also matters. Once large-scale IT infrastructures and long-term public-private procurement arrangements are in place, reversing them becomes politically and economically difficult. Technology firms also have a clear interest in continued expansion. Border and identity technologies now form a significant market, including biometrics, AI-embedded risk tools, and cloud services, which creates strong incentives for further digitalization and system growth (Beduschi 2021, pp. 34–36). As states buy and integrate these systems, they also become more dependent on private vendors to exercise core border functions, further blurring the line between public authority and commercial infrastructure. It also makes responsibility less clear: if rights are violated or people are harmed, it is harder to determine state (or company) responsibility and pursue mechanisms to ensure accountability.

At the same time, there are notable fragilities and potential trend breakers. Legal challenges and rights-based pushback are one channel. Case law from the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR) has tightened legal constraints around large-scale surveillance and communications data retention by requiring necessity, proportionality, and robust safeguards. Similar principles could plausibly be extended to migration databases and automated decision support in border governance (ECtHR 2021; CJEU 2016). Technical failure and cyber risk form a second channel. Because large, interconnected systems concentrate vulnerability, a sufficiently severe or repeated outage or data breach could undermine political trust and trigger debates about temporary suspensions, stricter regulation or partial redesign, even if recent incidents suggest that the threshold for such a reaction is very high. A related epistemic risk concerns data quality. Where verification relies on biometric matching and cross-system checks, misbinding, low quality matches, inbuilt racial or other biases, or manipulated inputs can propagate across connected infrastructures and generate authoritative-looking but incorrect outcomes. Diplomatic backlash is a further channel. Long queues, (perceived) discrimination, or prominent cases of automated refusal can bring digital bordering into international contestation and strain relations between states.

SCENARIOS AND IMPLICATIONS AFTER 2026

These fragilities do not point to a single outcome. Instead, they shape a range of credible scenarios for how digital borders may evolve after 2026. In the first scenario—mobility score normalization—algorithmic sorting and truth-making consolidates into routine governance. EES stabilises after initial frictions, ETIAS launches broadly on schedule, and pre-travel authorization regimes expand across jurisdictions. Over time, this produces a de facto mobility score. Travelers are continuously verified through interoperable data infrastructures and automated checks, with each system adding signals to a traveler’s machine-readable credibility. Minor controversies persist, including queues, mismatches, and false positives, but they are handled as technical issues rather than political problems that require redesign. In this trajectory, digital borders become a taken-for-granted layer of European security politics: governments can show that they are “in control” of mobility without opening up deeper debates about whose movement is being constrained and at what cost.

In a second scenario, a scandal-led reset, a cluster of visible failures in 2026, such as a major breach, systemic misidentification, or discriminatory outcomes, turns algorithmic truth-making into a legitimacy crisis. Court cases, regulatory intervention, and public backlash shift the debate from efficiency to accountability and fundamental rights. Rather than abandoning digital borders, governments narrow and redesign them, tightening oversight. They strengthen human review, limit how data can be reused, require records that make decisions traceable, and expand practical options for appeal and correction. The result is not a return to analogue borders, but a more regulated form of verification that relies less on open-ended inference and offers clearer grounds for challenge over what information can be treated as decisive. This scenario is less likely in the short term, given current path-dependencies, but it highlights the conditions under which rights-based pushback could reshape the terms of European security politics.

In a third scenario, platformed and digital borders become politically more prominent than physical borders because control is increasingly exercised through verification infrastructures rather than territorial checkpoints. Technology firms and vendors gain influence as they design, maintain, and update the systems that produce credible identity and acceptable risk in practice. In effect, they become key intermediaries of digital border security, while states grow dependent on proprietary architectures, contracts, and technical expertise that are difficult to audit or challenge. Bordering, then, looks less like a sovereign act carried out only by public authorities and more like a shared arrangement in which private actors shape classification rules, error rates, and practical outcomes for travelers, often upstream and with limited public visibility. Although this scenario is more medium-term, elements of it are already visible and would further entrench a model of European security politics in which key decisions about mobility and risk are delegated to opaque, partly privatized infrastructures.

In conclusion, digital borders are moving from pilot projects to routine infrastructure. As control shifts upstream into data systems and carrier processes, mobility decisions increasingly depend on how identities are verified and how errors can be corrected. The key policy question is not whether borders will be digital, but what safeguards, transparency, and avenues for redress will be built into this new normal. For European security politics, this suggests that debates on border security are less about walls or patrols and increasingly about how digital systems handle mobility: what levels of error and bias are accepted, how much people are allowed to see and understand about how these systems work, and how far authority is handed over to technical systems and private actors. The political choice is whether these infrastructures end up reinforcing a more stratified Fortress Europe or are pulled closer to existing legal commitments on protection and mobility. Across the three scenarios, the core issue is who has the power to decide which data and classifications count as true when governing movement, and how those decisions shape the journeys of different groups of travelers.

BIBLIOGRAPHY

- Baceiredo Macho, I. (2025). Shaping EU borders: An analysis of the technological and institutional developments in border management in the European Union. Peace & Security – Paix et Sécurité Internationales, 13, 1–30.
- Beduschi, A. (2021). Artificial intelligence and migration management: The EU's new frontier of digital borders. Georgetown Journal of International Affairs, 22(1), 31–38.
- Bellanova, R., & González Fuster, G. (2019). Politics of metadata: Datafication of information and digital borders. European Journal of Migration and Law, 21(2), 149–170.
- Broeders, D. (2007). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. International Sociology, 22(1), 71–92.
- Broeders, D., & Dijstelbloem, H. (2015). Border surveillance, mobility management and the shaping of non-publics in Europe. European Journal of Social Theory, 18(1), 21–38.
- Broeders, D., & Dijstelbloem, H. (2016). The datafication of mobility and migration management: The mediating state and its consequences. In I. van der Ploeg & J. Pridmore (Eds.), Digitizing identities: Doing identity in a networked world (pp. 242–260). Routledge.
- Council of the European Union. (2025, February 25). A new asylum and migration management regulation.
  https://www.consilium.europa.eu/en/policies/asylum-migration-management/
- Court of Justice of the European Union. (2016, December 21). Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others (Joined Cases C-203/15 and C-698/15).
- European Commission. (2025). Entry/Exit System (EES).
- European Commission. (2025, October 13). How the new digital borders system works.
  https://commission.europa.eu/news-and-media/news/how-new-digital-borders-system-works-2025-10-13_en
  European Commission. (2025). European Travel Information and Authorisation System (ETIAS).
- European Court of Human Rights. (2017). Big Brother Watch and Others v. the United Kingdom (Application no. 58170/13).
- European Court of Human Rights. (2021, May 25). Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14, 24960/15).
- European Parliament and Council of the European Union. (2019). Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa (OJ L 135, 22.5.2019, p. 27).
- Kemp, S., & Bossong, R. (2020). The politics of data-driven migration governance: The case of the UK. Journal of Ethnic and Migration Studies, 46(11), 2277–2294.

- Leese, M. (2022). Fixing state vision: Interoperability, biometrics, and identity management in the EU. Geopolitics, 27(1), 113–133. https://doi.org/10.1080/14650045.2020.1830764
- Leese, M., Noori, S., & Scheel, S. (2022). Data matters: The politics and practices of digital border and migration management. Geopolitics, 27(1), 5–25.
- Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494–620.

www.oiip.ac.at

Österreichisches Institut
für Internationale Politik
Austrian Institute
for International Affairs