



Preventing the misuse of commercial aviation:

Using passenger data to identify high-risk passengers and emerging threats



Preventing the misuse of commercial aviation: Using passenger data to identify high-risk passengers and emerging threats

Authors:

Deborah Manzi
Sara Valle

Università Cattolica del Sacro Cuore di Milano
Transcrime – Joint Research Centre on Innovation and Crime
Legal Office: Largo Gemelli 1 - 20123 Milan (Italy)
Phone: +39 02 7234 3715/3716
www.transcrime.it

ISBN: 978-88-99719-54-8

Suggested Citation: Manzi D. & Valle S. (2025), *Preventing the misuse of commercial aviation: Using passenger data to identify high-risk passengers and emerging threats*. Milan: Transcrime – Joint Research Centre on Innovation and Crime.

This publication presents the results of research activities carried out by Transcrime within the EU-funded project **TENACITY – Travelling Intelligence Against Crime and Terrorism** (Grant Agreement No. 101074048).

The information provided in this report offers only a high-level overview of the topic and does not include the detailed and comprehensive content found in the project's official deliverables. The findings presented are primarily based on a review of the literature, complemented by insights from end-user consultations. No sensitive or operationally restricted information obtained during the project is included.

This work represents the collective contributions of several authors at Transcrime, specifically by **Deborah Manzi** and **Sara Valle**. Deborah Manzi developed the content and prepared the initial structure. All authors contributed to finalising and editing the publication.

Graphic Design:

Ilaria Mastro

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior written permission of the authors.

Introduction: Travel intelligence and the use of PNR data

- The 9/11 attacks marked a turning point in how authorities use travel data for security. Before then, **Passenger Name Record (PNR)** data—collected by airlines mainly for booking—was not systematically used by law enforcement (De Hert & Papakonstantinou, 2010; Kanellopoulos, 2023). After the attacks, the U.S. passed the **Aviation and Transportation Security Act (2001)**, initiating the development of modern air travel intelligence systems to detect and prevent terrorism (US Government Publishing Office, 2001).
- In Europe, the **2004 Madrid bombings** pushed the EU to take a more active role in counter-terrorism and border control. This led to the adoption of key legislative tools like the **Advance Passenger Information (API) Directive** (The Council of the European Union, 2004) and the **Schengen Borders Code** (The European Parliament and the Council of the European Union, 2016b), which strengthened cross-border information exchange and cooperation with third countries.
- Over time, the EU has developed a more comprehensive approach to border security. New initiatives—such as the **Entry/Exit System (EES)**¹ and the **European Travel Information and Authorisation System (ETIAS)**²—aim to improve the monitoring of people crossing EU borders, although they are not yet fully operational.
- A cornerstone of the EU’s approach is the **PNR Directive (2016/681)**, which mandates that Member States set up **Passenger Information Units (PIUs)** to collect, store, and analyse PNR and API data. These units support investigations into terrorism and serious crime, and can share data with national authorities, Europol, and other countries—while ensuring compliance with data protection and privacy standards (The European Parliament and the Council of the European Union, 2016a; Aposkiti & Makri, 2025).

1. More information on the Entry Exist system can be accessed via: https://travel-europe.europa.eu/ees_en.

2. More information on ETIAS can be accessed via: https://travel-europe.europa.eu/etias_en.

The TENACITY Project in brief

Travel Intelligence Against Crime and Terrorism (TENACITY)³ is an

EU-funded project that addressed the growing need for more effective, coordinated, and intelligent use of travel data in the fight against terrorism and serious crime.

Law Enforcement Agencies (LEAs) across Europe rely on travel and border data—but face serious challenges (Aposkiti & Makri, 2025):

TENACITY tackled these challenges through three main pillars:



Smart Tools & Open Architecture:

TENACITY has developed cutting-edge, interoperable tools for analysing travel intelligence data. These tools use advanced digital technologies to integrate multiple sources and provide real-time, actionable insights.



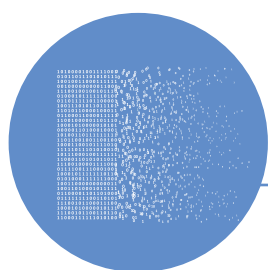
Training, Hackathons & the Living Lab:

To support LEAs in using these tools effectively, the project has built a **Living Lab**—a space for hands-on learning, experimentation, and collaboration. It hosted hackathons, workshops, and training sessions for practitioners and key stakeholders.

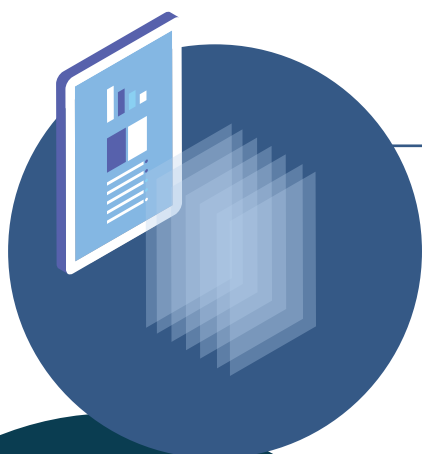


A Governance Framework for Travel Intelligence:

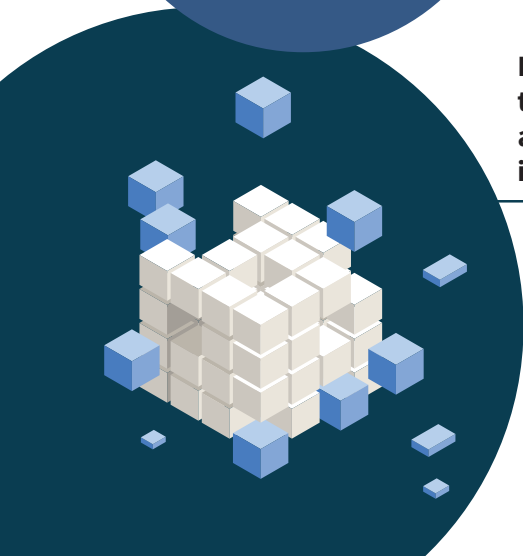
TENACITY promoted a strategic, long-term approach through a **Travel Intelligence Governance Framework**. This framework supports cooperation between LEAs and policymakers, guiding the ethical and effective use of digital tools to detect crime and terrorism patterns, as well as shaping smart regulation.



Fragmented data management across Member States



Inconsistent data quality and timeliness



Limited capacity to turn data into actionable intelligence

3. More information about the TENACITY project can be accessed via: <https://tenacity-project.eu/>

Understanding the threat:

How criminals exploit transportation systems

- To effectively disrupt criminal and terrorist activities, it is crucial to understand the ways in which transportation networks are misused for illicit purposes. Criminal organisations adapt quickly, exploiting vulnerabilities across maritime, air, and land routes to traffic drugs, weapons, contraband, or people.
- TENACITY has built its intelligence-led approach on the detailed analysis of these **modi operandi**, ensuring that law enforcement agencies can anticipate and respond to evolving tactics.

Illicit-goods smuggling: How criminals exploit transportation routes

Understanding how criminals move illicit goods and people is essential to improving travel intelligence and targeting law enforcement action. Criminal networks adapt their methods depending on risk levels, routes, and available infrastructure (UNODC, 2020).

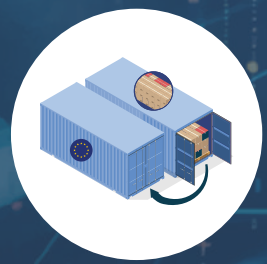
1. Maritime smuggling: Large-scale and hidden in plain sight

- Sea transport enables large shipments with relatively low scrutiny at ports.
- Common concealment techniques are explained in Figure 1 (EMCDDA, 2022; EMCDDA & Europol, 2019; Europol, 2021).
- Corruption of port workers often plays a key role in enabling these operations (Europol, 2021).

Figure 1.
Common concealment techniques



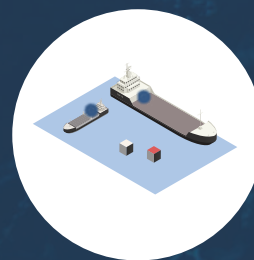
Rip-on/rip-off:
Illicit goods hidden in containers without the knowledge of legal cargo owners



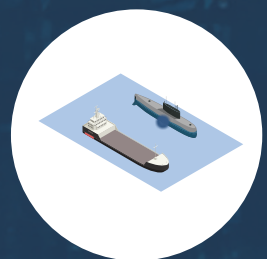
Switching containers: Illicit goods moved from one container to another before inspection



Illicit goods hidden within or among legitimate goods, or in the structure of the container itself



Use of commercial vessels, fishing boats, and pleasure yachts for covert drop-offs



Use of speed boats, inflatable crafts, and semi-submersibles for short-distance or high-risk drops

2. Air smuggling: Fast, global, and increasingly diverse

- Air routes are used for long-distance trafficking, especially when speed is critical (e.g., to quickly supply high-demand drug markets, deliver perishable drugs before degradation, or outpace competing criminal networks in establishing supply lines).
- Three types of criminal flights:
 - **White:** Seemingly legal, fully compliant.
 - **Grey:** Appear legal but deviate from rules mid-route (e.g., unreported landings).
 - **Black:** Completely clandestine, avoiding radar and radio contact (EMCDDA, 2022; EMCDDA & Europol, 2019; Europol, 2021).
- Methods are described in Figure 2 (EMCDDA, 2022; EMCDDA & Europol, 2019).

3. Land transport: The backbone of intra-EU smuggling

- Once illicit goods enter the European Union, they frequently move across borders by road, exploiting the freedom of movement enabled by the Schengen Area. These goods are typically concealed in private vehicles or commercial trucks, often mixed with legitimate cargo to avoid suspicion. Criminal networks employ various tactics to evade detection, including the use of corrupt drivers, falsified licence plates, and rented vehicles (EMCDDA & Europol, 2019).

Figure 2.
Air smuggling methods



Passengers hiding drugs or other illicit goods in luggage or on their bodies (small-scale)



Cargo flights used to conceal illicit goods in parcels or commercial shipments



Private jets preferred for moving large quantities with lower inspection risk



Helicopters and drones (UAVs) used for short distances and hard-to-reach delivery points

Smuggling of migrants: The Logistics of irregular migration

Criminal groups also exploit transport infrastructure to facilitate irregular migration for profit. These methods vary by region, route, and price (Achilli, 2016; Tinti & Reitano, 2016).

1. Sea routes: Risky, crowded, and often deadly

Most irregular migrants in the EU arrive via Mediterranean Sea routes using various types of boats, chosen based on budget and journey length. These include **speedboats**, **sailing boats**, **motor yachts**, **small inflatable boats**, and sometimes **custom-built vessels**. Due to high costs and risks, **stolen boats** are often used to reduce expenses and complicate law enforcement efforts.

Smugglers often use a two-boat method: a larger ship carries migrants across open waters before transferring them to smaller boats for the final approach. The crew then abandons the migrants with minimal guidance.

The “mother ship” technique, common between Egypt and Italy, involves fishing boats operated by recruited fishermen transporting migrants in international waters before leaving them on smaller vessels to be intercepted by authorities (European Commission, 2015).



Speedboats



Sailing boats



Motor yachts



Small inflatable boats



Custom-built vessels



2. Land routes: Common for secondary movement

Overland transport is the second most common method used by irregular migrants, often serving both to reach departure points and for secondary movements after sea or air travel.

Cars, buses, lorries, and trains are typically used, depending on the route (Europol & Interpol, 2016).

Migrants are frequently hidden in dark, sealed cargo spaces—conditions that pose serious health and safety risks. Smugglers commonly use **rented vehicles** or **fake licence plates** to avoid detection (European Commission, 2015). In some cases, commercial trucks are unknowingly used, with smugglers breaking seals and placing migrants inside while drivers are unaware. Migrants may also travel on foot in large groups known as “**caravans of hope,**” seeking safety, solidarity, and visibility as they cross borders.



Cars



Buses



Lorries



Trains



By foot



3. Air routes: Less frequent, but growing (Europol, 2021)

Air smuggling into or within the EU is less frequent than land or sea routes but may grow as controls tighten elsewhere. It offers speed, relative safety, and low risk for smugglers, who often coordinate remotely from outside the EU. Major international airports are targeted for their global connectivity, and air travel is often one leg of a longer journey. Migrants may first fly to a neighbouring country before continuing to the EU by land or sea (UNODC, 2010).

Two main tactics are used. In one, migrants use EU airports as transit points, then intentionally miss onward flights to **claim asylum**—often after destroying documents. In another, migrants meet criminal facilitators in airport transit lounges, where they receive **forged documents** before attempting to exit the airport. Direct entry using fraudulent travel documents is also common, highlighting the key role of document fraud in air smuggling.



Speed



Safety



**Low risk
for smugglers**



**Claim
asylum**



**Forged
documents**

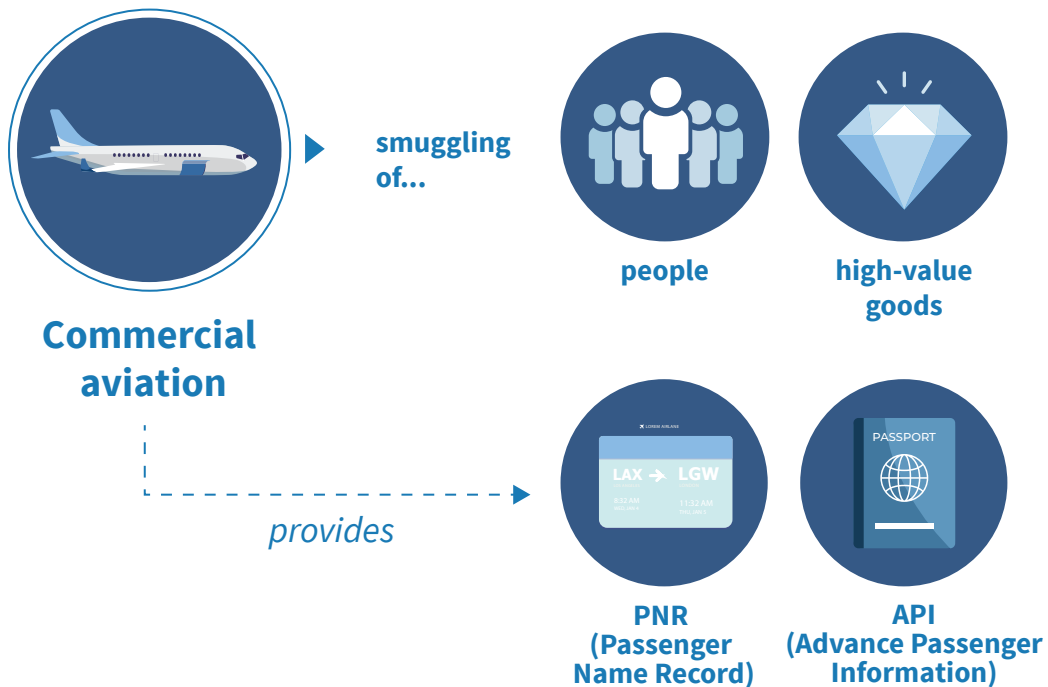


The role of passenger data in detecting aviation-related crime

While maritime and land smuggling remain dominant in terms of volume, the **use of commercial aviation** by criminal groups is becoming increasingly relevant—especially for **smuggling people or high-value goods**. Because commercial aviation involves structured booking processes, border checks, and digital records, it also provides **valuable data trails**—especially **PNR (Passenger Name Record)** and **API (Advance Passenger Information)** data—that can support early detection and intervention.

As part of TENACITY, a survey of law enforcement and PIU staff from 10 EU countries explored how passenger data supports the detection of crime involving air travel.⁴ Respondents

highlighted that commercial aviation is increasingly misused for **drug trafficking, migrant smuggling, organised crime movements, and human trafficking**, and that PNR and API data play a valuable role in identifying such activities. However, participants also noted challenges including **uneven data quality, lack of standardisation across airlines, and limited access for some law enforcement units**. Insights from this survey helped shape TENACITY’s **Risk Management Framework (RMF)**, ensuring that its risk indicators and tools reflect the real needs and priorities of practitioners working to detect and prevent crime in the aviation sector.



4. The survey was conducted online via the EU Survey platform and targeted practitioners directly involved in analysing PNR and API data for criminal investigations. It gathered 16 responses from law enforcement and Passenger Information Unit (PIU) personnel across 10 EU countries (Cyprus, Estonia,

Finland, Germany, Greece, Hungary, Italy, Latvia, Malta, and Spain) and the United Kingdom. Responses were anonymous and excluded any EU-restricted or sensitive information. Data were analysed using a combination of descriptive statistics and thematic content analysis to identify operational challenges, data gaps, and practitioner priorities.

Developing a Risk Management Framework (RMF)

Supporting the detection of criminal activity involving air travel

What is the RMF?

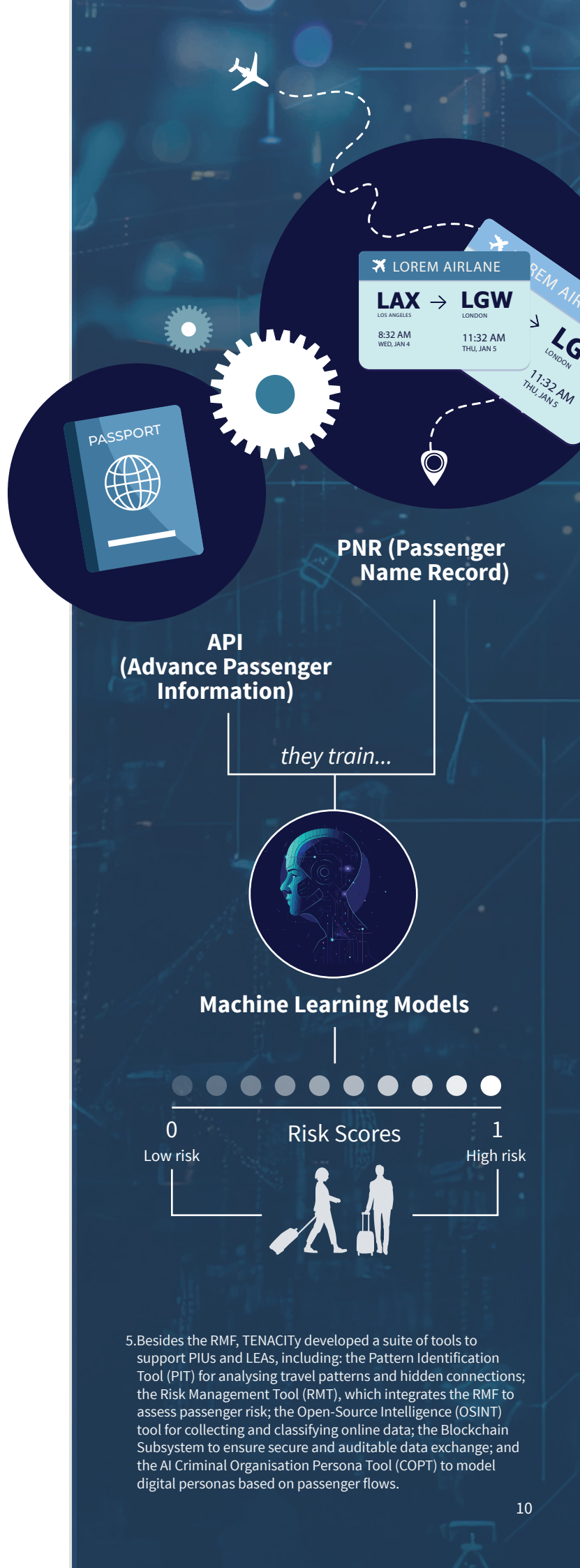
The Risk Management Framework (RMF) developed by **Transcrime** within the **TENACITY project** helps PIUs and law enforcement agencies detect potential misuse of commercial aviation for serious crime. It uses PNR and API to assign risk scores to passengers based on behavioural indicators, helping practitioners **prioritise checks and investigations** — without replacing expert judgment.⁵

How it works

1. Combining passenger data and machine learning

The RMF uses **machine learning models** to estimate how likely a passenger may be involved in criminal activity.

- Models are trained on **millions of synthetic PNR and API records** that replicate realistic booking and travel behaviour.
- By learning patterns from this synthetic data, the models can **identify risk indicators that are relevant for real passengers**, while preserving privacy.
- Each passenger receives an **individual risk score** between 0 (low risk) and 1 (high risk).



5. Besides the RMF, TENACITY developed a suite of tools to support PIUs and LEAs, including: the Pattern Identification Tool (PIT) for analysing travel patterns and hidden connections; the Risk Management Tool (RMT), which integrates the RMF to assess passenger risk; the Open-Source Intelligence (OSINT) tool for collecting and classifying online data; the Blockchain Subsystem to ensure secure and auditable data exchange; and the AI Criminal Organisation Persona Tool (COPT) to model digital personas based on passenger flows.

2. Transparent and explainable results

To make predictions **understandable and accountable**, the RMF integrates **Explainable Artificial Intelligence (XAI) tools** (Box 1).

These tools show:

- Which data fields most influence the model's decisions.
- Why a specific passenger is classified as “at risk” (Aven, 2011; Hutchins, 2018; Joint Task Force Transformation Initiative, 2012).

Data foundations

The RMF was trained and tested using a **fully synthetic dataset** created within TENACITY by Fadlian et al. (2025). This dataset reproduces realistic passenger behaviour under plausible travel scenarios, while protecting privacy.

To enable modelling:

- Six **behavioural risk indicators** were created (e.g., booking behaviour, route patterns, demographics).
- Each indicator was scored from 1 (very low risk) to 5 (very high risk).
- Passengers with scores above 3 were labelled “**at risk**” — about **1% of the sample**.

This provided a realistic foundation for training the models to distinguish ordinary from potentially suspicious travel behaviour.



Box 1 - What is Explainable AI (XAI)?

The use of machine learning in criminology and security studies has been growing, with applications ranging from **recidivism prediction and risk assessment in the justice system** (Berk, 2013; Brennan & Oliver, 2013) to the **analysis of organized crime and terrorism** (Campedelli, 2022). These studies illustrate the potential of machine learning to support decision-making in complex and high-stakes environments.

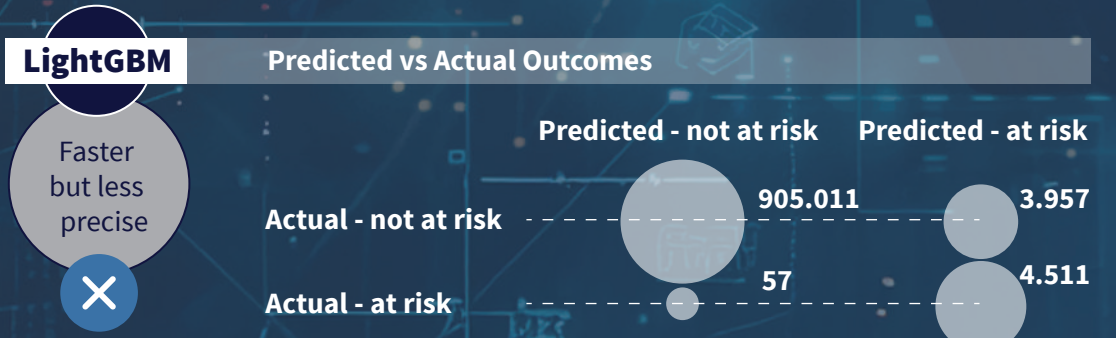
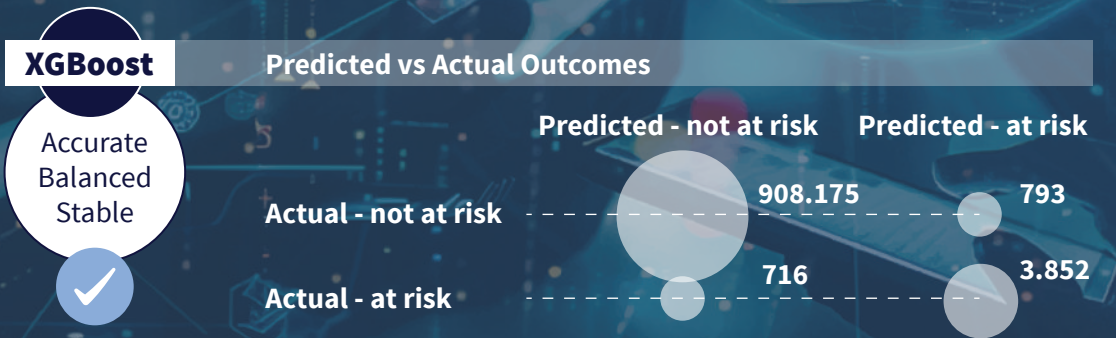
However, machine learning models are often “black boxes” — they predict outcomes without showing why. XAI methods such as **SHAP (Shapley Additive Explanations)** make these predictions transparent by highlighting which passenger features (e.g., route, payment method, age) increase or decrease the risk score.

This improves trust, accountability, and operational usability (Angelov et al., 2021; Gunning et al., 2019; Holzinger et al., 2017; Rudin, 2019).

Machine learning in action

Two advanced models were tested:

- **XGBoost** — accurate, balanced, and stable (Chen & Guestrin, 2016).
 - **LightGBM** — faster but less precise on unseen data (Luxburg et al., 2018).
- XGBoost achieved the best balance between detecting at-risk passengers and avoiding false positives and was therefore adopted for the RMF.



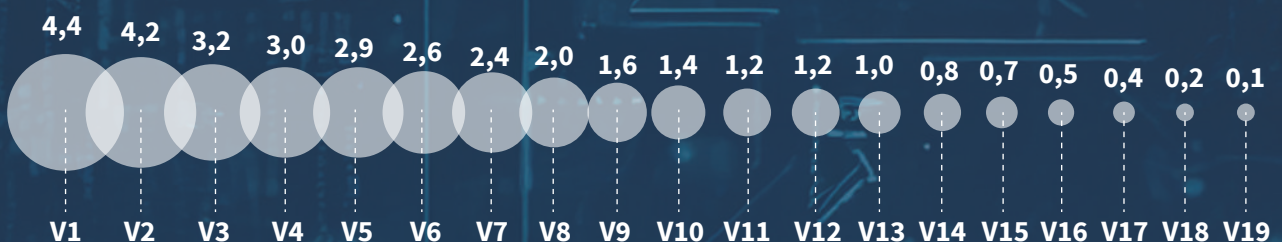
Making results transparent with SHAP

To make XGBoost predictions interpretable, the SHAP (Shapley Additive exPlanations) method was applied (Lundberg & Lee, 2017; Molnar, 2023). SHAP shows how each passenger characteristic affects the risk score, at both global and local levels.

Global interpretation:

Identifies which PNR/API fields have the strongest overall influence on risk predictions (bigger bubbles = higher influence).

SHAP analysis of feature importance and impact of each passenger characteristic

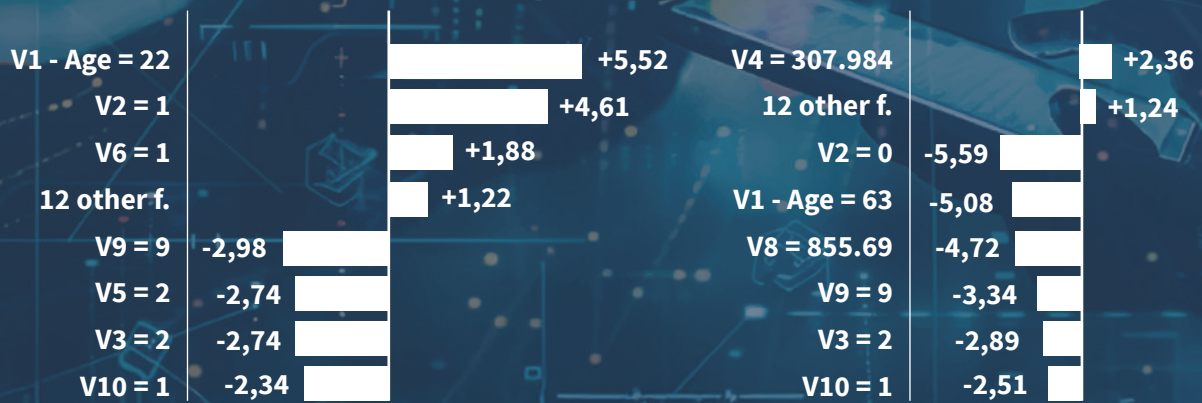


Local interpretation:

- Explains why a specific passenger is classified as high or low risk.
- **Example:** age is a common PNR data field. Criminological research consistently shows that delinquency and criminal involvement tend to peak in late adolescence and young adulthood,

then decline with age (Blonigen, 2010; Farrington, 1986; Hirschi & Gottfredson, 1983; Sweeten et al., 2013). Assuming that misuse of commercial aviation follows a similar pattern, SHAP values help reveal how age influences risk classification in the model.

Individual SHAP value explanations for high-risk and low-risk passengers



Younger age + certain itinerary patterns
 → High-risk score $p = 0.97$

Older age + safer travel behaviours
 → Low-risk score $p \approx 0$

SHAP allows practitioners to see which features drive each prediction, making the RMF both accurate and transparent. By combining global and local insights, the SHAP analysis

shows not just who is at risk, but why, providing actionable intelligence for preventive and targeted interventions while keeping predictions interpretable and accountable.

Operational relevance

The RMF is designed to support frontline law enforcement and PIUs by:

- Prioritising cases using standardised, data-driven scores.
- Seeing which data fields drive each risk assessment.
- Integrating machine learning models to support the identification of high-risk individuals.
- Maintaining transparency in how passengers are screened.

The RMF does not automate decisions — it supports intelligence-led, expert-guided analysis.

Keeping the RMF up to date

The framework is designed to evolve over time. Regular updates will ensure it reflects:

- New criminal tactics and routes identified by law enforcement.
- Emerging data sources and indicators.
- Refinements to model weights and scoring logic.

This dynamic approach keeps the RMF aligned with real-world operational needs and the changing landscape of aviation-related crime.

Conclusion

As criminal networks increasingly exploit the speed, reach, and anonymity of commercial air travel, the ability to detect high-risk passengers has become a critical need for EU law enforcement and PIUs. The TENACITY project responds to this challenge by developing a structured, evidence-based Risk Management Framework (RMF) that enables practitioners to assess the likelihood that a passenger may be involved in the misuse of commercial aviation for criminal purposes.

By integrating survey findings, expert rationale, behavioural risk factors, and machine learning methods into a weighted scoring system, the RMF offers a transparent and adaptable tool for operational use. It allows end-users to move from reactive investigations to more proactive threat detection—using PNR and API data to identify risk patterns early, allocate resources more effectively, and build cross-border intelligence.

Crucially, the RMF is designed to evolve through continuous feedback and validation, ensuring it remains relevant to the changing tactics of organised and serious crime. This approach not only enhances situational awareness but also contributes to a more secure and intelligence-led use of Europe's aviation infrastructure.



Reference 1/2

- Achilli, L. (2016). Irregular migration to EU and human smuggling in the Mediterranean: The nexus between organized crime and irregular migration, Mobility and refugee crisis in the Mediterranean [IEMED POLICY Brief]. <https://cadmus.eui.eu/handle/1814/43667>
- Angelov, P. P., Soares, E. A., Jiang, R., Arnold, N. I., & Atkinson, P. M. (2021). Explainable artificial intelligence: An analytical review. *WIREs Data Mining and Knowledge Discovery*, 11(5), e1424. <https://doi.org/10.1002/widm.1424>
- Aposkiti, C., & Makri, F. (2025). Navigating the challenges of passenger name record data and the way forward. *Open Research Europe*, 4, 168. <https://doi.org/10.12688/openreseurope.18037.2>
- Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability Engineering & System Safety*, 96(7), 719–726. <https://doi.org/10.1016/j.res.2010.12.020>
- Berk, R. (2013). Algorithmic criminology. *Security Informatics*, 2(1), 5. <https://doi.org/10.1186/2190-8532-2-5>
- Blonigen, D. M. (2010). Explaining the relationship between age and crime: Contributions from the developmental literature on personality. *Clinical Psychology Review*, 30(1), 89–100.
- Brennan, T., & Oliver, W. L. (2013). The Emergence of Machine Learning Techniques in Criminology: Implications of Complexity in our Data and in Research Questions. *Criminology & Public Policy*, 12(3), 551–562. <https://doi.org/10.1111/1745-9133.12055>
- Campedelli, G. M. (2022). Explainable machine learning for predicting homicide clearance in the United States. *Journal of Criminal Justice*, 79, 101898. <https://doi.org/10.1016/j.jcrimjus.2022.101898>
- Chen, T., & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System (No. arXiv:1603.02754). arXiv. <https://doi.org/10.48550/arXiv.1603.02754>
- De Hert, P., & Papakonstantinou, V. (2010). The EU PNR framework decision proposal: Towards completion of the PNR processing scene in Europe. *Computer Law & Security Review*, 26(4), 368–376. <https://doi.org/10.1016/j.clsr.2010.05.008>
- EMCDDA. (2022). EU drug market, Cocaine. Publications Office. <https://data.europa.eu/doi/10.2810/944155>
- EMCDDA & Europol. (2019). EU drug markets report 2019. Publications Office. <https://data.europa.eu/doi/10.2810/796253>
- European Commission. (2015). A study on smuggling of migrants. Characteristics, responses and cooperation with third countries. https://www.icmpd.org/file/download/54169/file/A%2520study%2520on%2520smuggling%2520of%2520migrants_full%2520study.pdf
- Europol. (2021). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021: A corrupting influence : the infiltration and undermining of Europe's economy and society by organised crime. Publications Office. <https://data.europa.eu/doi/10.2813/346806>
- Europol & Interpol. (2016). Migrants Smuggling Networks. Joint Europol-Interpol Report. https://www.europol.europa.eu/cms/sites/default/files/documents/ep-ip_report_executive_summary.pdf
- Fadlian, M. F., Ireson, N., & Lanfranchi, V. (2025). Generating Realistic Passenger Name Records with Privacy Compliance for Security Analysis. Proceedings of the International ISCRAM Conference. <https://doi.org/10.59297/mbf3dq94>
- Farrington, D. P. (1986). Age and crime. *Crime and Justice*, 7, 189–250.
- Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S., & Yang, G.-Z. (2019). XAI—Explainable artificial intelligence. *Science Robotics*, 4(37), eaay7120. <https://doi.org/10.1126/scirobotics.aay7120>
- Hirschi, T., & Gottfredson, M. (1993). Age and the explanation of crime. *American Journal of Sociology*, 89(3), 552–584.

Reference 2/2

- Holzinger, A., Biemann, C., Pattichis, C. S., & Kell, D. B. (2017). What do we need to build explainable AI systems for the medical domain? arXiv. <https://doi.org/10.48550/ARXIV.1712.09923>
- Hutchins, G. (2018). ISO 31000: 2018 enterprise risk management. Greg Hutchins.
- Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (No. NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Kanellopoulos, A.-N. (2023). Travel intelligence as a tool for counterintelligence and border security. *Security and Defence Quarterly*. <https://doi.org/10.35467/sdq/174523>
- Lundberg, S., & Lee, S.-I. (2017). A Unified Approach to Interpreting Model Predictions. arXiv. <https://doi.org/10.48550/ARXIV.1705.07874>
- Luxburg, U. von, Guyon, I., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S. V. N., Garnett, R., & Neural Information Processing Systems Foundation (Eds.). (2018). Advances in neural information processing systems 30: 31st Annual Conference on Neural Information Processing Systems (NIPS 2017): Long Beach, California, USA, 4-9 December 2017. Curran Associates, Inc.
- Molnar, C. (2023). Interpreting machine learning models with SHAP: A guide with Python examples and theory on shapley values (First Edition). Christoph Molnar c/o MUCBOOK, Heidi Seibold.
- Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206–215. <https://doi.org/10.1038/s42256-019-0048-x>
- Shapley, L. S. (1953). A value for n-person games. *Princeton University Press*, 2(28), 307–317.
- Sweeten, G., Piquero, A. R., & Steinberg, L. (2013). Age and the explanation of crime, revisited. *Journal of Youth and Adolescence*, 42(6), 921–938.
- The Council of the European Union. (2004). COUNCIL DIRECTIVE 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0082>
- The European Parliament and the Council of the European Union. (2016a). DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681>
- The European Parliament and the Council of the European Union. (2016b). Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0399>
- The European Parliament and the Council of the European Union. (2025). Regulation (EU) 2025/12 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC.
- Tinti, P., & Reitano, T. (2016). *Migrant, refugee, smuggler, saviour*. Hurst & Company.
- UNODC. (2010). *Migrant smuggling by air* [Issue Paper]. https://www.unodc.org/documents/human-trafficking/Migrant-Smuggling/Issue-Papers/Issue_Paper_-_Migrant_Smuggling_by_Air.pdf
- UNODC. (2020). *Global Study on Firearms Trafficking 2020*. United Nations on Drugs and Crime. <https://www.unodc.org/unodc/en/firearms-protocol/firearms-study.html>
- US Government Publishing Office. (2001). *Aviation and transportation security act: To improve aviation security and for other purposes*. S.1447 - 107th US Congress. <https://www.congress.gov/bill/107th-congress/senate-bill/1447>