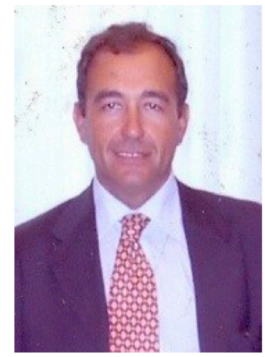
SISTEMI TECNOLOGICI E SICUREZZA DELLE FRONTIERE AEREE



DORIANO RICCIUTELLI
Istruttore ENAC della sicurezza

Nell'ottica di una modernizzazione tecnologicamente avanzata nella gestione del controllo dello spazio Schengen, percepiamo come questione di assoluta centralità, peraltro legata all'esigenza di rafforzamento delle frontiere esterne dell'Unione europea, l'imprescindibile conseguimento di una compiuta interoperabilità dei meccanismi di informazione oggi a disposizione degli organi di *law enforcement*.

Nel novero delle iniziative più recenti avviate in tale campo di interesse, spicca senz'altro il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS - *European Travel Information and Authorization System*), analogo all'*Electronic System for Travel Authorization* (ESTA) statunitense, che, assieme ad altre similari progettualità concepite su larga scala, risulterà presto davvero essenziale per potenziare la sicurezza in termini di efficacia e efficienza presso gli scali aerei.

Si tratta di un insieme normativo creato principalmente per focalizzare i rischi per la *security* e la mitigazione della migrazione irregolare, che disciplina la maniera in cui i cittadini di 61 paesi terzi, i quali attualmente sono esenti dall'obbligo del visto per una permanenza di 90 giorni nell'area Schengen, potranno fare ingresso nell'Unione. Più in particolare il sistema informatico in argomento consentirà, una volta entrato a pieno regime, lo svolgimento di verifiche preventive da parte delle competenti autorità che saranno in grado, ove necessario, di denegare l'autorizzazione ai viaggi con tutto il vantaggio di incentivare la sicurezza degli Stati membri, di facilitare l'accertamento di reati di terrorismo e di altri gravi crimini, di prevenire il fenomeno dell'immigrazione illegale e di proteggere la salute pubblica da epidemie, tema, quest'ultimo, assai sensibile in tempi giustappunto di pandemia.

Secondo una interpretazione autentica del compilatore per "rischio per la sicurezza" deve intendersi esattamente quello di minaccia per l'ordine pubblico, la sicurezza interna o le relazioni internazionali di uno dei paesi UE, per "rischio di immigrazione illegale" ci si riferisce alla prospettiva illecita che un cittadino di paese terzo non soddisfi le condizioni d'ingresso e di soggiorno di cui all'articolo 6 del regolamento (UE) 2016/399 e, da ultimo, per "alto rischio epidemico" si ritiene qualunque malattia infettiva ai sensi dei regolamenti sanitari internazionali dell'Organizzazione mondiale della sanità (OMS) o del Centro europeo per la prevenzione e il controllo delle malattie (ECDC), nonché altre patologie infettive o parassitarie contagiose, sempreché siano oggetto di disposizioni di protezione applicate ai cittadini degli Stati membri.

Ci accorgiamo che recentemente il legislatore europeo è intervenuto a emendare in maniera tangibile la normativa di riferimento, adottando il regolamento (UE) 2021/1134 del 7 luglio 2021 che modifica il regolamento (UE) 2018/1240[1] nonché altri regolamenti correlati, occupandosi di aspetti relativi all'interconnessione con il sistema di informazione visti e introducendo nuove norme sul funzionamento di ETIAS da parte delle autorità competenti ad assumere decisioni su una domanda di visto di soggiorno di lunga durata o d'un titolo di soggiorno. In questo panorama, va richiamato anche il regolamento (UE) 2021/1152 (emanato in pari data del precedente e in vigore dal 3/8/2021) apportante modificazioni al regolamento (UE) 2018/1240, nonché i regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1861 e

(1) Regolamenti (CE) n. 767/2008, (CE) n. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (UE) 2019/1896, al fine della riforma del sistema di informazione visti.

SISTEMI TECNOLOGICI E SICUREZZA DELLE FRONTIERE AEREE

segue

(UE) 2019/817, che stabiliscono le regole sull'attuazione della interrelazione stretta tra l'ETIAS, da un lato, e altri sistemi di informazione dell'UE e i dati Europol, dall'altro, nonché le condizioni per la relativa consultazione dei dati conservati ai fini dell'individuazione automatica di eventuali riscontri positivi riferibili alle menzionate minacce.

Non può trascurarsi la circostanza che la novella comprenda altresì, tra le verifiche automatizzate, una nuova categoria di segnalazioni effettivamente utili riguardante i cittadini di paesi extraeuropei oggetto di una decisione di rimpatrio i quali possono sfuggire agli ordinari controlli di *routine*.

Giova per di più sottolineare che l'impianto così tecnicamente inteso mira a sostenere gli obiettivi del SIS (sistema d'informazione Schengen) relativi alle notizie su cittadini di paesi terzi ai fini del rifiuto d'ingresso e di soggiorno, di persone ricercate per l'arresto o a fini di consegna o d'estradizione, di soggetti scomparsi o ricercati all'interno di un procedimento giudiziario ovvero da sottoporre a controllo discreto o specifico.

Quanto alla procedura prevista dal sistema ETIAS, occorre rimarcare che i visitatori stranieri interessati dovranno richiedere l'autorizzazione ai viaggi prima di intraprenderli e, a seguito della compilazione *online* di un modulo di domanda, il sistema stesso provvederà alla effettuazione dei controlli attraverso i sistemi di informazione per la sicurezza dell'Unione. Ciò, beninteso, garantendo nel contempo la tutela dei dati, grazie al sancito principio di "non discriminazione" e, in siffatta prospettiva, anche all'impegno della Commissione di orientamento sui diritti fondamentali dell'ETIAS con funzione consultiva e di valutazione [(2)].

Al di là delle problematiche di sicurezza si conseguono - come un indiscusso valore aggiunto - taluni vantaggi complementari, in termini di *facilitation,* in ispecie per il settore aeroportuale, tenuto conto che la verifica *in advance* degli stranieri esenti dal visto agevolerà i controlli, eviterà la burocrazia e i ritardi per i viaggiatori quando si presentano presso le aerostazioni di partenza, garantirà un *risk assessment* coordinato e armonizzato dei passeggeri e, infine, ridurrà in modo sostanziale il numero di rifiuti di ingresso agli aeroporti di destinazione.

Sotto il profilo organizzativo-strutturale, il sistema sarà sviluppato dall'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT nello spazio di libertà, sicurezza e giustizia (eu -LISA) e, oltretutto, potrà contare sulla istituzione di un'unità centrale ETIAS in seno all'Agenzia europea Frontex e di un'autorità competente, come unità nazionale ETIAS, designata da ogni Stato membro.

Conviene qui specificare che l'architettura tecnica del sistema d'informazione di cui si discute è composta di un'interfaccia uniforme nazionale (NUI), basata su specifiche tecniche comuni in tutti i paesi dell'Unione, la quale realizza la connessione "in maniera sicura" del sistema centrale ETIAS alle infrastrutture nazionali di frontiera e ai punti di accesso centrale nei paesi UE. Al riguardo, l'utilizzazione di ETIAS (ad eccezione di determinate previsioni) inizierà a decorrere dalla data stabilita dalla Commissione (verosimilmente non oltre il 2022), in base alla conclusione degli iter legislativi necessari al completamento dell'intero *framework* giuridico, ad avvenuta ultimazione dei collaudi e alla finalizzazione di ogni misura contemplata nel regolamento.

Ebbene, passando al trattamento delle richieste autorizzatorie, qualora dall'esame di una domanda risulti che non si profilano indicazioni concrete né fondati motivi per concludere che la presenza di una persona nel territorio degli Stati membri possa presentare un pericolo, il sistema centrale ETIAS o l'unità nazionale ETIAS dello Stato membro competente rilascia un permesso ai viaggi. In caso, invece, di dubbi in merito all'esistenza di motivi sufficienti per un diniego (e.g. segnalazione al SIS), l'unità nazionale ETIAS dello Stato membro competente

(2) Combinato disposto degli articoli 10 e 14 del regolamento (UE) 1240/2018.

SISTEMI TECNOLOGICI E SICUREZZA DELLE FRONTIERE AEREE

segue

ha la possibilità, anche dopo un colloquio, di rilasciare un'autorizzazione ai viaggi con un indicatore volto a raccomandare alle pertinenti autorità nazionali di procedere a una verifica cautelativa in seconda linea.

Sia in caso di rilascio che di rifiuto dell'autorizzazione ai viaggi, il richiedente viaggiatore riceve in tempo reale, tramite il servizio di posta elettronica, una comunicazione recante, rispettivamente, o la relativa favorevole attestazione di ottenimento o la comunicazione dell'avvenuto respingimento della domanda, incluse le informazioni sulle motivazioni e sul diritto di ricorribilità al provvedimento stesso.

Salvo le situazioni di transito aeroportuale o di un guasto, i vettori si devono collegare al sistema d'informazione ETIAS per verificare se i cittadini di paesi terzi siano in possesso o meno di un'autorizzazione valida.

L'accesso sicuro al portale per i vettori, di cui all'articolo 6, paragrafo 2, lettera k) del regolamento (UE) 1240/2018, accompagnato dalla possibilità di usare soluzioni tecniche mobili, permette convenientemente di procedere alla suindicata interrogazione prima che un passeggero salga a bordo.

Sulla scorta delle suddette premesse, è bene comunque ricordare che l'efficacia delle verifiche sistematiche dipende essenzialmente dalla interoperabilità dei sistemi di informazione dell'UE che sarà capace di rendere fruibili con immediatezza le informazioni necessarie ai diversi organi di polizia, in ossequio del principio di condivisione per i successivi seguiti operativi.

In merito, riveste una innegabile rilevanza il sistema automatico di ingressi e uscite (EES) IT per la registrazione dei viaggiatori provenienti da paesi extra-UE, che troverà applicazione sia nei confronti di coloro che necessitano di un visto di soggiorno di breve durata sia di chi proviene da paesi extra-UE esenti dall'obbligo del visto.

Non sfuggirà che, secondo l'impostazione regolamentare, l'EES sostituirà il regime corrente di apposizione manuale del timbro sul passaporto che, a titolo esemplificativo, molto rallenta il traffico aeroportuale, attesa soprattutto la dispendiosità in termini di tempo e delle risorse umane impiegate nei controlli dei varchi, non fornendo poi dati affidabili sull'attraversamento dei confini né permettendo di rintracciare i soggiornanti fuori termine.

Si aggiunga che per permettere al sistema centrale ETIAS di trattare i fascicoli delle domande è necessario realizzare il raccordo - come accennato - tra il sistema d'informazione ETIAS anche con il sistema (SIS), nonché con il sistema di informazione visti (VIS), con l'Eurodac (Banca dati dell'Unione per il confronto delle impronte digitali dei richiedenti asilo) e con il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN) indirizzato a verificare se un determinato cittadino di paese terzo o una persona con doppia cittadinanza UE/EXTRA UE abbia subito in precedenza una condanna per reati gravi (si veda il Regolamento (UE) 2019/816).

In proposito, il portale di ricerca europeo (ESP), istituito dal regolamento (UE) 2019/817 e dal regolamento (UE) 2019/818, provvederà ad "interrogare" contestualmente i dati conservati nell'ETIAS e quelli presenti negli altri citati sistemi di informazione dell'UE e, perfino, nelle banche dati dell'Interpol attraverso un accesso "rapido, continuato, efficace, sistematico e controllato".

Come noto, altre informazioni anticipate sui passeggeri, costituite segnatamente dai dati biografici personali raccolti dai vettori aerei durante le operazioni di check-in e trasmessi in anticipo tramite i sistemi PNR e API alle autorità di controllo del paese di destinazione, hanno concorso enormemente a ottimizzare i controlli eseguiti negli aeroporti e ad individuare minacce in precedenza sconosciute, procurando alle autorità di contrasto indizi di *intelligence* su reati e modelli di viaggio sospetti.

Pertanto, anche alla stregua dei risultati scaturiti dal rapporto della Commissione sui progressi della Strategia della sicurezza del 23 giugno 2021, si può affermare che l'auspicata revisione della Direttiva UE 2016/681 appunto

SISTEMI TECNOLOGICI E SICUREZZA DELLE FRONTIERE AEREE

sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, ricompresa nella relazione della Commissione (COM (2020) 305 del 24/7/2020), potrebbe favorire un utilizzo ancor più incisivo del patrimonio informativo comune, garantendo parallelamente il rispetto della relativa legislazione (Direttiva 2016/680/UE) e agevolando il flusso di passeggeri.

Su un diverso versante, notiamo che i prossimi sviluppi in materia di intelligenza artificiale IA (Libro bianco (COM(2020)65 final del 19 febbraio 2020) apporteranno un cospicuo contributo sulla capacità di reagire alle eventuali minacce contro il trasporto aereo. Di certo, infatti, avrà un significativo impatto sugli standard di sorveglianza degli spazi pubblici aeroportuali il ruolo delle tecnologie di identificazione facciale in grado di intercettare terroristi e criminali in movimento per mezzo del confronto dell'immagine del loro volto con una banca dati di riferimento.

Inoltre, l'identificazione di determinate categorie di oggetti (ad esempio dei bagagli abbandonati all'interno dei terminal) o di comportamenti sospetti mediante sistemi di *behaviour detection* (secondo le raccomandazioni di cui all'annex 17 della Convenzione di Chicago, 4.1.3-13.2.3 b) può essere estremamente utile per individuare in anticipo forme di aggressioni nei confronti dell'aviazione civile.

In questa cornice di ipotesi innovative, la Comunicazione della Commissione relativa al terzo rapporto sui progressi in ordine alla implementazione della Strategia della sicurezza in UE dell'8 dicembre 2021 (COM(2021) 799 final) richiama proprio un parere congiunto dello "*European Data Protection Board*" e dello "*European Data Protection Supervisor*" sulla proposta della Commissione stessa inerente all'Artificial Intelligence Act (COM 2021 (206) del 21 aprile 2021). Per contro, circa la fattibilità dei progetti affini a detti strumenti di contrasto è doverosa una sottolineatura inequivocabilmente critica emersa nella Risoluzione del Parlamento europeo del 6 ottobre 2021 (2021P9_TA (2021)0405) sull'intelligenza artificiale e il suo utilizzo da parte delle autorità giudiziarie e di polizia in sede penale.

L'Alta Istituzione ha ritenuto difatti che "la raccolta di dati biometrici per finalità di identificazione a distanza, ad esempio attraverso il riconoscimento facciale in luoghi pubblici nonché i cancelli per il controllo automatizzato negli aeroporti, possano presentare rischi specifici per i diritti fondamentali, le cui implicazioni potrebbero variare notevolmente a seconda delle finalità, del contesto e dell'ambito di impiego".

Il Parlamento europeo ravvisa, *inter alia*, la controversa validità scientifica della tecnologia di riconoscimento, come le fotocamere che rilevano i movimenti degli occhi e le variazioni delle dimensioni della pupilla, nella sfera delle attività di contrasto, ritenendo che l'uso dell'identificazione biometrica dovrebbe sempre essere considerato ad "alto rischio" e, dunque, soggetto a ulteriori requisiti, come previsto dalle raccomandazioni del gruppo di esperti della Commissione sull'IA dell'8 aprile 2019.

A ben vedere sul punto, nella anzidetta risoluzione si fissano opportunamente le condizioni secondo le quali, come minimo, le tecniche di riconoscimento facciale debbano essere conformi ai requisiti di minimizzazione, affidabilità e precisione dei dati, del relativo limite di conservazione e sicurezza ed essere lecite, eque e trasparenti, nonché "perseguire una finalità specifica, esplicita e legittima, chiaramente definita nel diritto degli Stati membri o dell'Unione".

Orbene, in vista di una prossima definizione del complesso quadro giuridico sin qui delineato atto a stabilire, attraverso soluzioni inedite e all'avanguardia, elevati livelli di prestazione dei sistemi tecnologici inter operativi, delle apparecchiature di analisi comportamentale e di intelligenza artificiale, si può conclusivamente sostenere che a breve assisteremo a un consistente miglioramento globale della qualità di protezione e resilienza delle infrastrutture critiche aeroportuali contro atti di interferenza illecita e della difesa interna degli Stati dell'Unione.