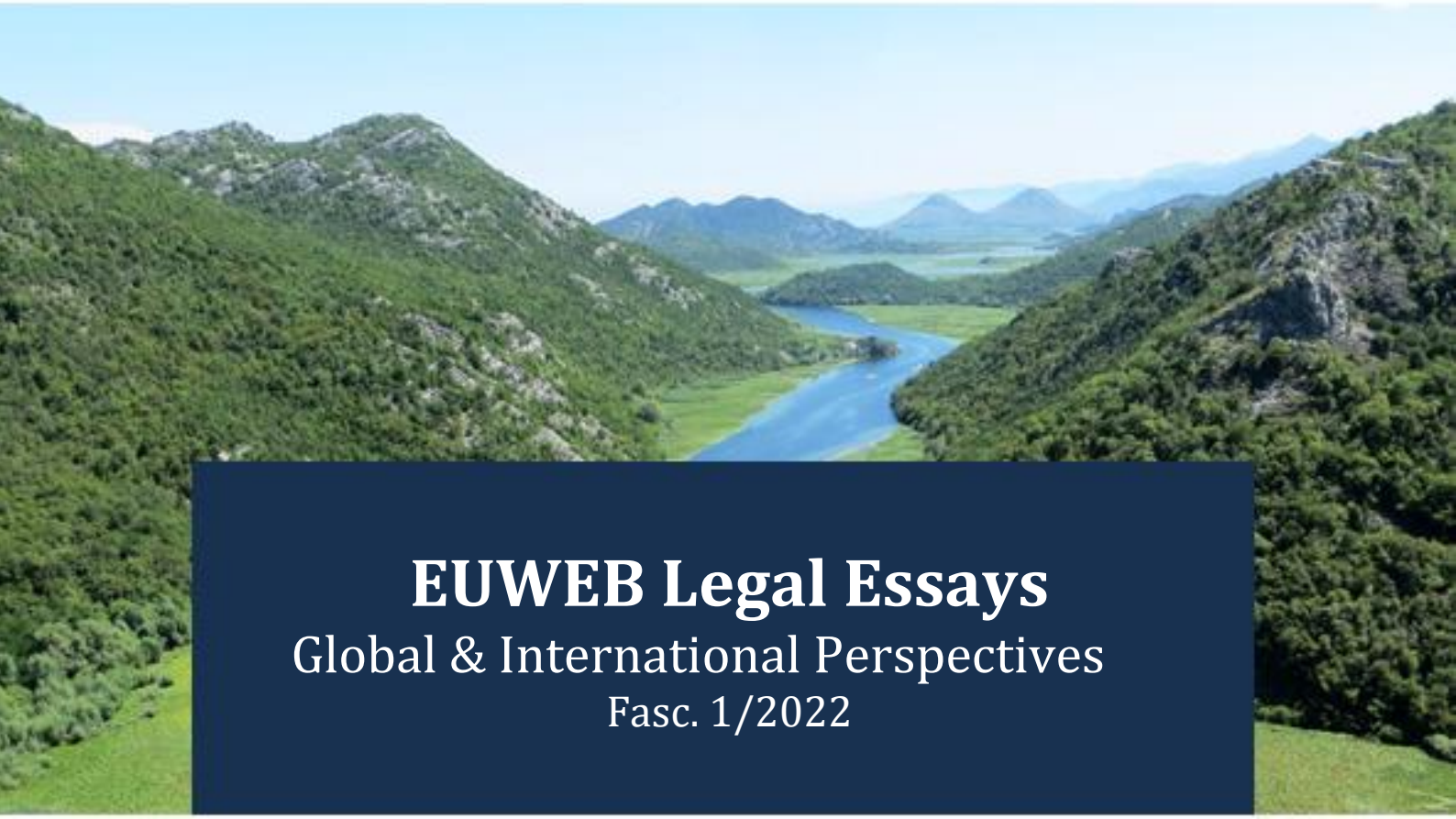
ISSN 2785-5228

EUWEB
EU-WESTERN BALKANS
Cooperation on Justice and Home Affairs



EUWEB Legal Essays

Global & International Perspectives

Fasc. 1/2022

EDITORIALE SCIENTIFICA

Rivista semestrale on line EUWEB Legal Essays. Global & International Perspectives
www.euweb.org
Editoriale Scientifica, Via San Biagio dei Librai, 39 – Napoli
Registrazione presso il Tribunale di Nocera Inferiore n° 5 del 23 marzo 2022
ISSN 2785-5228

Index
2022, n. 1

Databases and Protection of Human Rights

PRINCIPIO DI DISPONIBILITÀ, COOPERAZIONE ORIZZONTALE E SCAMBIO DEI DATI PNR

di Paolo Troisi[*]

1. Introduzione

A partire da "Maastricht", ma in maniera più rilevante ancora con i successivi Trattati, la cooperazione informativa in materia penale è progressivamente entrata a far parte degli obiettivi istituzionali dell'Unione europea (UE) nel settore della *law enforcement cooperation*. La base normativa è, oggi, rappresentata dall'articolo 87, paragrafo 2, lettera. a) del Trattato sul Funzionamento dell'Unione europea (TFUE), che consente di stabilire misure riguardanti "*la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni*"[1].

In realtà, fin dall'Accordo di Schengen e dalla relativa Convenzione applicativa l'implementazione dello scambio di informazioni tra le competenti autorità nazionali è stata intesa quale fattore compensativo della libera circolazione in ambito europeo. In uno spazio in cui sono abolite le frontiere si è reputato irrinunciabile semplificare ed agevolare l'*information sharing*, in vista di plurime finalità: attuare i controlli alle frontiere, applicare le norme in materia di asilo, combattere la migrazione illegale e, soprattutto, contrastare fenomeni criminosi a carattere transnazionale.

La svolta si è avuta, però, solo con il Programma dell'Aia (formulato dal Consiglio europeo di Bruxelles del 4 e 5 novembre 2004), attraverso l'elaborazione del c.d. *principio di disponibilità*, destinato ad aprire nuovi orizzonti in un ambito fino ad allora regolato dall'opposto principio del dominio esclusivo degli Stati sui dati acquisiti nel corso o in funzione delle investigazioni penali. Nella prospettiva delineata dal principio di disponibilità, le barriere costituite dai confini nazionali non devono più rappresentare

[*] Ricercatore confermato in Procedura penale; *Lecturer* in Procedura penale – Università "Tor Vergata" di Roma.

[1] Sul tema v., tra gli altri, S. BRAUM, V. COVOLO, *From Proven Fragmentation to Guaranteed Data Protection within the Virtual Criminal Law Enforcement Area: A Report on Personal Data Protection within the Framework of Police and Judicial Cooperation in Criminal Matters*, in K. LIGETI (ed.), *Toward a Prosecutor for the European Union, A Comparative Analysis*, Vol. 1, Oxford, 2013, p. 1011 ss.; F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonized Data Protection Principles for Information Exchange at EU-level*, Berlino-Heidelberg, 2012; G. DI PAOLO, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in T. RAFARACI (a cura di), *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona*, Milano, 2011, p. 198 ss.; C. FANUELE, *Lo scambio di informazioni a livello europeo*, in L. FILIPPI, P. GUALTIERI, P. MOSCARINI, A. SCALFATI (a cura di), *La circolazione investigativa nello spazio giuridico europeo: strumenti, soggetti, risultati*, Padova, 2010, p. 19 ss.; F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009. Sia consentito anche il rinvio a P. TROISI, *Il potenziamento della cooperazione transfrontaliera. Lo scambio di informazioni*, in L. KALB (a cura di), *«Spazio europeo di giustizia» e procedimento penale italiano*, Torino, 2012, p. 195 ss., e ID., *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, 2012.

ISSN 2785-5228
DOI

un ostacolo; questo significa che, in tutta l'Unione, "*un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni sia in condizione di ottenerle da un altro Stato membro"* e che *"il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni sia tenuto a trasmettergliele per i fini dichiarati*" (punto 2.1 del Programma).

Il salto di qualità è notevole: le singole autorità di *law enforcement* devono poter individuare il Paese che dispone di informazioni utili e di potervi accedere. Ciascuno Stato è tenuto, di conseguenza, a conservare ed a mettere a disposizione dei partner europei i dati raccolti per prevenire e reprimere reati commessi da soggetti che si muovono liberamente nel territorio dell'Unione[2].

Due sono i fattori che hanno determinato il mutamento di prospettiva: la recrudescenza – a seguito degli attacchi di New York e di Madrid del 2001 e del 2004 – del terrorismo internazionale, che ha reso indispensabile pianificare nuove strategie di contrasto, implicanti necessariamente, a fronte di un fenomeno planetario, il potenziamento della condivisione informativa; il progresso tecnologico, che ha incrementato le possibilità di raccogliere, archiviare e trasmettere dati.

Duplice è stato l'obiettivo perseguito: stimolare uno scambio "diretto" tra gli Stati membri; favorire lo sviluppo di una circolazione di informazioni promossa da organismi sovranazionali, attraverso la progressiva creazione di banche dati europee con finalità di sicurezza e giustizia.

Sotto il primo profilo – cooperazione "orizzontale" – la prospettiva era realizzare, a seconda della tipologia di informazioni, "*l'accesso reciproco o l'interoperabilità di basi di dati nazionali*". Sotto il secondo, il Programma dell'Aia ha posto l'accento su uno scambio "mediato" (o "verticale"), attraverso archivi centrali da rendere accessibili *on-line* agli organi di *law enforcement* nazionali; il che ha determinato il proliferare di *database* europei, tra loro interoperabili[3], fruibili per finalità di cooperazione e di contrasto: oltre ad *Europol*, eletto a "*punto nodale dello scambio di informazioni nell'Unione*"[4], a tali scopi sono, oggi, variamente utilizzabili il *Sistema informativo*

[2] In argomento, v. S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in F. PERONI, M. GIALUZ (a cura di), *op. cit*., p. 42.

[3] Il percorso verso l'interoperabilità dei sistemi informativi UE è stato intrapreso con i Regolamenti (UE) 2019/817 e 2019/818; Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, *che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio*, del 20 maggio 2019, in GUUE L 135, del 22 maggio 2019, pp. 27-84; Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, *che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816*, del 20 maggio 2019, in GUUE L 135, del 22 maggio 2019, pp. 85-135. Per un'analisi critica, v. E. BROUWER, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, in *European Public Law*, Vol. 26, n. 1, 2020, p. 71 ss.; C. BLASI CASAGRAN, *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, in *Human Rights Law Review*, Vol. 21, n. 2, 2021, p. 433 ss.

[4] Così lo definisce il Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, *che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI*, dell'11 maggio 2016, in GUUE L 135, del 24 maggio 2016, pp. 53-114.

Schengen (SIS)[5], l'*European dactylografic system* (EURODAC)[6], il *Sistema di informazione visti* (VIS)[7], nonché, attualmente in fase di sviluppo, il *Sistema di ingressi/uscite* (EES)[8], il *Sistema europeo di informazione e autorizzazione ai viaggi* (ETIAS)[9], il *Sistema sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi* (ECRIS-TCN)[10].

Il conseguimento di questi obiettivi ha avuto notevoli ricadute su due fronti.

Innanzitutto, sull'attività di raccolta e di archiviazione: lo scambio in tanto può svolgere un ruolo strategico, in quanto sia migliorata l'attività di selezione e memorizzazione dei dati rilevanti per la lotta alla criminalità. Uno degli aspetti su cui si è concentrato il legislatore europeo, nel dare seguito alle direttive del Programma dell'Aia, è stata proprio l'implementazione dell'attività di conservazione dei dati funzionali alla cooperazione informativa, ora richiedendo agli Stati l'istituzione di nuove banche dati (o l'armonizzazione degli schedari nazionali esistenti), ora prevedendo, come detto, la creazione o il potenziamento di sistemi informativi UE.

In secondo luogo, sul terreno della protezione dei dati: il passaggio da una dimensione prettamente nazionale ad uno scenario in cui le informazioni circolano, senza "steccati", nel territorio europeo amplifica l'esigenza di assicurare l'integrità e la correttezza dei dati trasmessi, nonché la tutela dei diritti individuali; il che ha reso necessario elaborare una strategia comune a livello sovranazionale. È proprio dal Programma dell'Aia che ha preso

---

[5] L'uso del SIS nel settore della cooperazione in materia penale è, oggi, normato dal Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, *sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione*, del 28 novembre 2018, in GUUE L 312, del 7 dicembre 2018, pp. 56-108.

[6] Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, *che istituisce l' «Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia*, del 26 giugno 2013, in GUUE L 180, del 29 giugno 2013, pp. 1-30.

[7] Regolamento (CE) n. 767/2008, così come riformato dal Regolamento (UE) 2021/1134 del Parlamento europeo e del Consiglio, *che modifica i regolamenti (CE) n. 767/2008, (CE) n. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (EU) 2019/1896 del Parlamento europeo e del Consiglio e che abroga le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, ai fini della riforma del sistema di informazione visti*, del 7 luglio 2021, in GUUE L 248, del 13 luglio 2021, pp. 11-87.

[8] Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, *che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011*, del 30 novembre 2017, in GUUE L 327, del 9 dicembre 2017, pp. 20-82.

[9] Regolamento (UE) 2018/1240, come aggiornato dal Regolamento (UE) 2021/1152 del Parlamento europeo e del Consiglio, *che modifica i regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861 e (UE) 2019/817 per quanto riguarda la definizione delle condizioni di accesso agli altri sistemi di informazione dell'UE ai fini del sistema europeo di informazione e autorizzazione ai viaggi*, del 7 luglio 2021, in GUUE L 249, del 14 luglio 2021, pp. 15-37.

[10] Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, *che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726*, del 17 aprile 2019, in GUUE L 135, del 22 maggio 2019, pp. 1-26.

avvio il lento percorso che ha condotto, prima, alla Decisione quadro 2008/977/GAI (mai compiutamente attuata dagli Stati membri), poi, alla Direttiva (UE) 2016/680[11], approvata contestualmente al Regolamento (UE) 2016/679. Nonostante i significativi passi avanti computi (soprattutto sul versante dell'equiparazione tra trattamento transfrontaliero e trattamento *purely domestic*), il quadro, comunque, resta, tutt'oggi, frammentario, in quanto anche la nuova disciplina non ha sostituito le specifiche disposizioni per la *data protection* dettate dai singoli strumenti della cooperazione informativa, sebbene si sia previsto il progressivo allineamento di questi ultimi ai principi sanciti dalla Direttiva (articolo 62, paragrafo 6)[12].

2. I cardini della cooperazione informativa orizzontale: il "sistema Prüm" e la Decisione quadro "svedese"

Concentrando, ora, l'attenzione, per quanto d'interesse in questa sede, sulla cooperazione orizzontale, ruolo pioneristico è stato svolto, come noto, dal Trattato di Prüm, sottoscritto il 27 maggio 2005 e, successivamente, inglobato nel quadro giuridico dell'Unione (Decisioni 2008/615/GAI e 2008/616/GAI)[13].

Il sistema Prüm ha introdotto forme innovative di trasferimento *cross border* per quattro categorie di dati: genetici, dattiloscopici, automobilistici e relativi ad eventi di rilievo a dimensione transfrontaliera[14].

Riguardo ai dati genetici, due sono state le principali novità: l'obbligo degli Stati di conservare i profili DNA, istituendo un'apposita banca dati nazionale allo scopo di perseguire le violazioni penali; lo scambio regolato da un meccanismo *hit/no hit*, che consente al punto di contatto nazionale di accedere *online* agli indici delle banche dati degli altri Stati membri, per conoscere in tempo reale se un profilo genetico sia in esse archiviato, e di ottenere, in caso di riscontro positivo, attraverso gli ordinari canali della cooperazione giudiziaria o di polizia, la trasmissione delle informazioni sulla persona a cui quel profilo appartiene.

Analogo doppio binario – consultazione diretta dei dati di indice e trasferimento su richiesta delle informazioni personali[15] – è stato previsto anche per le impronte digitali. In questo caso, però, lo scambio può avvenire non solo per finalità repressive (implicanti una *notitia criminis* già acquisita), ma anche per scopi preventivi.

L'accesso integrale *on-line* agli schedari nazionali è stato, invece, previsto per i dati automobilistici: i punti di contatto sono legittimati a consultare – per finalità sia di prevenzione e repressione dei reati, che di mantenimento dell'ordine e della sicurezza

[11] Al riguardo cfr., tra gli altri, P. MILAZZO, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, 2017, p. 709 ss. e, volendo, P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, p. 313 ss.

[12] V., al riguardo, la Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Via da seguire per allineare l'acquis dell'ex terzo pilastro alle norme sulla protezione dei dati*, del 26 giugno 2020, COM(2020) 262 final.

[13] V., in dottrina, A. MARANDOLA, Information sharing *nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione*, in F. PERONI, M. GIALUZ (a cura di), *op. cit.*, p. 164 ss.

[14] In senso critico, v. S. KIERKEGAARD, *The Prüm decision. An uncontrolled fishing expedition in "Big Brother" Europe*, in *Computer, Law & Security Report*, Vol. 24, n. 3, 2008, p. 243 ss.

[15] Cfr. M. O'NEILL, *A Europe that Protects: Moving to the Next Stage of Cross-Border Law Enforcement Cooperation*, in *Policy Journal*, Vol. 84, n. 2, 2011, p. 125 ss.

pubblica – i registri nazionali dei veicoli, potendo ottenere, inserendo il numero di telaio o il numero di targa, tutte le informazioni relative al veicolo e al proprietario.

La forma tradizionale di accesso su richiesta – arricchita, tuttavia, in ossequio al principio di disponibilità, dall'obbligatorietà della risposta – è stata, all'opposto, contemplata per le informazioni necessarie a prevenire i reati e garantire l'ordine e la sicurezza pubblica nel corso di manifestazioni a carattere transfrontaliero.

La logica che ha animato il sistema Prüm è stata, dunque, recepire diversamente il principio di disponibilità alla luce della natura (più o meno sensibile) dei dati da trattare, attraverso un approccio definito "per singoli campi di dati" (c.d. *data field-by-data field approach*).

Ulteriore tappa attuativa del principio di disponibilità è stata percorsa con la Decisione quadro 2006/960/GAI (c.d. Decisione quadro "svedese"), che si è posta un differente obiettivo: promuovere il più ampio scambio di dati possibile, congegnando un sistema generale di condivisione di informazioni ed *intelligence* tra le autorità di contrasto degli Stati membri, a fini di profilassi e di indagine penale. A fronte, tuttavia, della circolazione di una maggiore tipologia di dati, la forma di scambio, certamente meno ambiziosa e lontana dall'obiettivo dell'interoperabilità, è stata quella dell'*accesso indiretto su richiesta*: è direttamente l'autorità di contrasto, qualora abbia motivo di ritenere che i dati cercati siano disponibili in altro Stato membro, ad inoltrare, per il tramite di qualsiasi canale della cooperazione internazionale, una richiesta motivata. Si prescrive, in ogni caso, che la trasmissione non debba essere soggetta a condizioni più rigorose di quelle applicabili a livello nazionale; che la risposta debba intervenire entro termini stringenti; che la condivisione possa essere rifiutata solo per motivi tassativi motivi[16].

3. Gli sviluppi

Sotto la spinta propulsiva del Programma dell'Aia, sono fiorite ulteriori iniziative volte a creare circuiti di interconnessione tra le banche dati nazionali a fini di *law enforcement*. Rilevante è, innanzitutto, il *Sistema di scambio reciproco ed informatizzato delle informazioni estratte dai casellari giudiziari* (ECRIS), che nasce come rete informatica decentrata: i dati dei casellari giudiziari sono conservati unicamente negli archivi nazionali; non è prevista alcuna forma accesso diretto *on-line* da parte di autorità estere; la circolazione avviene per il tramite dello Stato di cittadinanza, che funge da centro di raccolta e smistamento delle informazioni concernenti le sentenze pronunciate, in altri Stati membri, nei confronti dei propri cittadini; titolare dei dati rimane, comunque, lo Stato della condanna, il quale può vietare la ritrasmissione per fini diversi da un procedimento penale ed è tenuto a comunicare ogni modifica o soppressione dei dati allo Stato di cittadinanza, affinché aggiorni il proprio database[17]. Il sistema – che realizza una

[16] Su questi temi, volendo, P. TROISI, *La circolazione di informazioni*, cit., p. 15 ss.

[17] Decisione quadro 2009/315/GAI, come modificata dalla Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, *che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio*, del 17 aprile 2019, in GUUE L 151, del 7 giugno 2019, pp. 143-150. Sul tema, tra i tanti, D. CIMADOMO, *Il casellario giudiziario*, in L. KALB (a cura di), *«Spazio europeo di giustizia»*, cit., p. 835 ss.; M. GIALUZ, *Il casellario giudiziario europeo: una frontiera dell'integrazione in materia penale*, in F. PERONI, M. GIALUZ (a cura di), *op. cit*., p. 190 ss.; L. Kalb, *Il sistema informativo giudiziario: il casellario e l'anagrafe*, in G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB (a cura di), *Procedura penale. Teoria e pratica del processo*, Torino, 2015, p. 748 ss.

forma di scambio orizzontale – è destinato, peraltro, ad essere integrato, come sopra detto, da un archivio centralizzato a livello dell'Unione (ECRIS-TCN), che consentirà di individuare gli Stati membri in possesso di dati sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi.

Plurimi sono, inoltre, gli strumenti adottati nel quadro della lotta al terrorismo ed alla grave criminalità transnazionale. Si possono, al riguardo, ricordare: la Decisione 2005/671/GAI, concernente lo scambio di informazioni in materia di terrorismo; la Decisione 2007/845/GAI, relativa alla cooperazione tra gli uffici degli Stati membri per il recupero dei beni (ARO) nel settore del reperimento e dell'identificazione dei proventi di reato o di altri beni connessi.

Maggiori cenni merita la più recente Direttiva (UE) 2019/1153, che, in vista della prevenzione e del perseguimento del terrorismo, della criminalità organizzata e del riciclaggio, regola un meccanismo di scambio su richiesta delle *informazioni finanziarie* e delle *informazioni estratte dai registri centralizzati nazionali dei conti bancari* tra le Unità di informazione finanziaria dei diversi Stati membri (FIU), le altre autorità nazionali appositamente designate, nonché tra le FIU (o le altre autorità nazionali) ed *Europol*. Un circuito, questo, abbastanza capillare, che completa la strategia UE *Anti-Money Laundering*, implementa la disciplina dettata dalla Direttiva (UE) 2015/849 e conferma la tendenza, sempre più massiccia, al reimpiego, nelle attività di contrasto, di dati personali raccolti e archiviati per altre finalità.

Si tratta di tendenza che rinviene, nel diritto dell'Unione, una delle prime manifestazioni nella normativa sulla *data retention*18, la quale, pur senza prevedere alcun canale privilegiato di trasferimento transfrontaliero, ha fatto emergere l'importanza, nelle investigazioni penali, dei metadati del traffico comunicativo, imponendone, ai gestori dei relativi servizi, una conservazione generale e indiscriminata, seppur limitata nel tempo.

Alla base si staglia un approccio di tipo proattivo, che da oltre oceano (e, in particolare, dagli Stati Uniti) si è gradualmente materializzato anche nell'Unione e che si estrinseca non più (e non solo) nella mera reazione agli eventi, ma nell'attivarsi a fini di profilassi come compito primario delle autorità deputate all'applicazione della legge. Il principale strumento impiegabile a tale scopo è la c.d. *intelligence* criminale, vale a dire l'analisi sistematica – che si avvale di meccanismi automatizzati e degli ingranaggi dell'intelligenza artificiale – di informazioni raccolte, spesso in maniera massiva (c.d. *Big data*), negli ambiti più disparati, non solo, quindi, nelle attività di contrasto, ma anche nel settore privato, con l'obiettivo di individuare legami tra soggetti "noti" e persone mai sospettate di reati, monitorarne i comportamenti, elaborare criteri valutativi e di profilassi, prevedere le condotte individuali, con l'obiettivo di prevenire in maniera *pro-active* futuri reati.

Espressione di siffatto approccio è, ad esempio, l'accordo del 2010 sul trattamento ed il trasferimento dei dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP)[19]. L'accordo, in effetti, obbliga i fornitori designati di servizi di messaggistica

[18] Si tratta della nota Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, del 15 marzo 2006, in GUUE L 105, del 13 aprile 2006, pp. 54-63, poi invalidata da Corte di Giustizia (Grande Sezione), sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e altri*, in quanto ritenuta non compatibile con gli artt. 7, 8 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea.

[19] L'accordo, siglato il 28 giugno 2010, è stato suggellato dalla Decisione del Consiglio 2010/412, *relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del*

finanziaria a trasferire al Dipartimento del Tesoro statunitense, sulla base di valutazioni specifiche della minaccia geografica e di richieste precise, i dati relativi alle transazioni finanziarie, conservati nel territorio UE, necessari a prevenire, indagare e perseguire il terrorismo ed in relativo finanziamento. I dati trasmessi contengono, tra l'altro, il nome, il numero di conto, l'indirizzo e il numero d'identificazione dell'ordinante e/o dei beneficiari delle transazioni finanziarie internazionali, ad esclusione di quelle avvenute nell'ambito dello Spazio unico dei pagamenti in euro (SEPA). Il Dipartimento del Tesoro può utilizzare i dati esclusivamente ai fini del TFTP e fornisce – spontaneamente o su richiesta – agli Stati membri dell'UE, ad *Europol* ed *Eurojust* le "*informazioni indiziarie*" riguardanti reati di terrorismo nell'Unione. Si dà vita, in tal modo, ad una sorta di scambio *circolare* di dati personali, che dall'Unione arrivano al Dipartimento del Tesoro degli Stati Uniti e che, da qui, possono, poi, essere ritrasmessi agli Stati membri, ad *Europol* ed *Eurojust*.

Evidenti sono i punti critici: l'accordo ben contempla la trasmissione alle autorità statunitensi di dati relativi ad individui che nulla hanno a che vedere col terrorismo o il suo finanziamento; tali dati sono trasferiti in blocco e non in risposta a una richiesta riguardante una o più persone. Chiaro è, dunque, l'obiettivo di un monitoraggio di massa di dati personati raccolti nel settore economico-finanziario[20].

4. Il sistema PNR

L'esempio più lampante della citata tendenza è, però, la Direttiva (UE) 2016/681, sull'uso dei dati del codice di prenotazione dei passeggeri dei voli in arrivo o in partenza dal territorio degli Stati membri a fini di prevenzione, accertamento, indagine e azione penale per reati di terrorismo ed altri gravi reati.

A seguito di un tormentato *iter* e sulla scia delle iniziative adottate, dopo l'11 settembre, negli Stati Uniti, in Canada, in Australia ed in altri Paesi, è stato introdotto, nell'ordinamento europeo, contestualmente all'approvazione del pacchetto UE di riforma della protezione dei dati, un meccanismo che consente l'archiviazione e l'analisi, per le attività di *intelligence* e le investigazioni penali, dei dati personali raccolti, a fini prettamente commerciali, da soggetti privati (le compagnie aeree)[21].

Messa da parte la possibilità per le autorità statali di accedere direttamente agli archivi informatici dei vettori, si è stabilito che siano questi ad inviare elettronicamente, da 24 a 48 ore prima della partenza e immediatamente dopo la chiusura del volo, i dati del codice di prenotazione (PNR) all'Unità nazionale d'informazione sui passeggeri

---

programma di controllo delle transazioni finanziarie dei terroristi, del 13 luglio 2010, in GUUE L 195, del 27 luglio 2010, pp. 3-4.

[20] Sul tema, v. V. MITSILEGAS, *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, in *Tilburg Law Review*, Vol. 20, n. 1, 2015, p. 35 ss.; M. TZANOU, *The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?*, in E. FAHEY (ed.), *Institutionalisation beyond the Nation State*, Cham, Springer, p. 55 ss.

[21] Per un'analisi del tema v., *ex multis*, F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?*, in *Dir. umani e dir. internaz.*, 2017, p. 213 ss.; D. LOWE, *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit For Purpose?*, in *International Criminal Law Review*, Vol. 17, n. 1, 2017, p. 78 ss.; F. ROSSI DAL POZZO, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui «codici di prenotazione» (PNR)*, in *Riv. dir. internaz. priv. e proc.*, Vol. 52, n. 4, 2016, pp. 1020-1059; G. TIBERI, *La direttiva UE sull'uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi*, in *Quaderni cost.*, n. 3, 2016, p. 590 ss.; e, volendo, P. TROISI, Passenger Name Records, privacy *e accertamento penale*, in *Proc. pen. giust.*, n. 1, 2019, p. 159 ss.

(UIP) istituita nello Stato membro nel cui territorio atterra o dal cui territorio parte il volo *extra* o *intra*-UE.

Quest'ultima provvede ad una prima analisi automatizzata, che si avvale di criteri di rischio prestabiliti e del confronto con le informazioni archiviate in altre banche dati. Lo scopo è controllare i viaggiatori prima dell'arrivo o della partenza del volo, per individuare persone che potrebbero essere implicate in atti di terrorismo o in altri gravi reati (c.d. *controllo in tempo reale*). Ad un eventuale "*riscontro positivo*", deve seguire un esame individuale non automatizzato (volto a verificare la necessità di appositi interventi), in seguito al quale l'Unità nazionale trasmette i dati e i risultati del relativo trattamento alle autorità di *law enforcement* competenti, nonché alle UIP di tutti gli altri Stati membri (per l'inoltro ai rispettivi organi giudiziari, di polizia e di *intelligence*).

A prescindere dall'esito delle analisi, tutti i dati ottenuti dalle compagnie aeree sono conservati, dall'Unità nazionale che li riceve, in apposita banca dati, per un periodo di cinque anni e, trascorsi sei mesi dal trasferimento, sono resi anonimi mediante mascheramento degli elementi che potrebbero servire per l'identificare il passeggero o altre persone.

La conservazione è funzionale, *in primis*, a consentire alla UIP di rispondere a richieste debitamente motivate rivolte, in relazione a casi specifici, dalle autorità statali di contrasto, dalle Unità di informazione (o, in casi di emergenza, direttamente dagli organi competenti) di altri Stati membri, da Europol o da Paesi terzi (c.d. *controllo reattivo*). La trasmissione dei dati integrali, dopo i primi sei mesi, è consentita solo se necessaria e previo *placet* di un'autorità giudiziaria o di altra autorità nazionale competente.

I dati archiviati sono, inoltre, analizzati per definire o aggiornare i criteri di rischio da adoperare per individuare persone implicate in gravi attività criminali (c.d. *controllo proattivo*).

Il sistema genera, pertanto, un vero e proprio circuito di scambio orizzontale di informazioni: per un verso, l'Unità nazionale, a seguito di riscontri positivi, trasmette alle autorità competenti i dati ricevuti dalle compagnie aeree (o dalle UIP di altri Stati); per altro verso, gli organi interni di contrasto possono richiedere i dati, nel corso di specifiche attività preventive o repressive, all'Unità nazionale o a quelle degli altri Paesi; in tale evenienza, la richiesta, di regola inoltrata tramite l'UIP nazionale, può essere formulata, in casi di emergenza, direttamente all'Unità d'informazione estera

Il trattamento e la trasmissione sono, in ogni caso, ammessi unicamente per la finalità di prevenire e reprimere reati di terrorismo o altri gravi reati specificamente elencati. È fatto divieto assoluto di trattamento di dati sensibili e di decisioni individuali automatizzate o fondate su ragioni discriminatorie.

Puntuali sono le regole in tema di protezione dei dati, soggetta, in via generale, alla disciplina della Direttiva (UE) 2016/680, per il trattamento effettuato a scopi di *law enforcement*, ed al Regolamento (UE) 2016/679, per quello da parte dei vettori, a cui spetta informare adeguatamente i passeggeri e adottare misure tecniche e organizzative a tutela della sicurezza e della riservatezza.

5. Gli aspetti critici

Lungo è stato il dibattito sulla necessità e proporzionalità di una misura di tal fatta, imperniata sulla generale schedatura ed analisi di dati personali, quand'anche non sensibili, relativi a chiunque decida di spostarsi con un aeromobile in ambito europeo o

al di fuori dell'Unione, a prescindere dall'esistenza di elementi indicativi di un qualsiasi nesso con azioni criminose.

La sorveglianza avviene in deroga ad uno dei cardini dell'autodeterminazione informativa, il *principio di finalità limitata*: dati ottenuti per scopi essenzialmente commerciali sono adoperati, senza il consenso dell'interessato, per obiettivi, anch'essi determinati e legittimi (il contrasto del terrorismo e della criminalità grave), ma assolutamente diversi e non consequenziali rispetto a quelli della raccolta iniziale. La deroga non è attenuata dall'obbligo, posto in capo ai vettori, di informare adeguatamente i passeggeri, in quanto il contesto in cui le notizie sono rese è profondamente difforme da quello in cui vengono, successivamente, riversate e costituisce, per di più, esercizio, almeno con riguardo ai viaggi *intra*-UE, della libertà di circolazione.

Manca, nel disegno tracciato dal legislatore europeo, la predeterminazione di meccanismi per definire i criteri di rischio da adoperare nell'analisi informatizzata in tempo reale dei dati PNR. Il tutto è rimesso alla discrezionalità della singola UIP, con il pericolo di una tutela non uniforme dei diritti individuali e soprattutto senza alcuna garanzia (o forma di controllo) sull'idoneità di tali criteri a condurre a risultati indicanti unicamente individui sui quali potrebbe gravare un sospetto ragionevole di partecipazione a reati di terrorismo o a reati gravi di natura transnazionale.

Analogo discorso vale per le banche dati con cui effettuare il raffronto, che dovrebbero essere affidabili, aggiornate e, soprattutto, limitate a quelle gestite in relazione alla lotta al terrorismo e ai detti gravi reati. L'impiego di *database* con funzioni più ampie o parzialmente diverse porrebbe, infatti, un concreto rischio di *function creep*, vale a dire di graduale allargamento dei confini di operatività del sistema; in tal caso, un eventuale *match* non fornirebbe, in maniera attendibile, sospetti di atti di terrorismo o di gravi reati, con chiara violazione del principio di finalità limitata. La disciplina europea, tuttavia, pare, anche al riguardo, deficitaria, in quanto si limita a fare riferimento a banche dati semplicemente "*pertinenti*" allo scopo e rimette, in ultima analisi, alle autorità statali la scelta degli archivi da compulsare.

Problematiche pone, altresì, la conservazione dei dati, da parte dell'UIP, ben oltre il trattamento in tempo reale ed a prescindere dal se abbia fornito (o meno) riscontri positivi. L'accesso, ad opera degli organi di *intelligence*, di polizia e giudiziari, alle informazioni così archiviate dovrebbe fondarsi su nuove circostanze che lo giustifichino ed avvenire in presenza di specifiche condizioni sostanziali e procedurali, quali: l'esistenza di elementi obiettivi che consentano di ritenere che i dati PNR di uno o più passeggeri possano fornire un contributo effettivo di lotta contro il terrorismo e i reati gravi di natura transnazionale; la preventiva autorizzazione, fuori dai casi d'urgenza, di un giudice o di un ente amministrativo indipendente[22]. Per i passeggeri che abbiano lasciato il territorio dell'Unione, inoltre, la permanenza dei dati si giustificherebbe unicamente in presenza di situazioni concrete che permettano di inferire che il singolo individuo presenti, ancora, profili di rischio.

[22] Si tratta di principi ampiamente affermati dalla Corte di Giustizia in materia di *data retention*. Cfr., di recente, Corte di Giustizia (Grande Sezione), sentenza del 2 marzo 2021, causa C-746/18, *H.K.*,; Corte di Giustizia (Grande Sezione), sentenza del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*; Corte di Giustizia (Grande Sezione), sentenza del 6 ottobre 2020, causa C-623/17, *Privacy International*. Nello stesso senso si era espressa la Sintesi del secondo parere del Garante europeo della protezione dei dati, *sulla proposta di una direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*, del 24 settembre 2015, in GUUE C 392, del 25 novembre 2015, punti 42-46, nell'osservare che, in caso di richiesta di accesso ai dati da parte di un'autorità competente, si dovrebbe sempre ottenere un'autorizzazione preventiva di un tribunale o di un organo amministrativo indipendente, e che i casi legittimanti l'accesso dovrebbero essere tassativamente definiti.

Nulla di ciò è, però, rinvenibile nella regolamentazione. Non sono tipizzati i casi in cui le autorità di contrasto possano domandare (ed ottenere) i dati: se ne consente l'accesso a seguito di mera "*richiesta debitamente motivata e basata su motivi sufficienti*", senza necessità di controllo giurisdizionale, se non qualora si tratti di trasmettere i dati integrali a seguito di mascheramento. Alcun collegamento è, peraltro, istituito tra conservazione e permanenza del soggetto nell'Unione: le notizie tratte dal PNR restano nella disponibilità della UIP anche dopo la ripartenza ed a prescindere dall'esistenza di pericoli qualificati.

Non sono, infine, previste comunicazioni a favore del passeggero i cui dati siano stati trattati in casi specifici, essendo l'informativa confinata alla sola evenienza in cui si siano verificate inosservanze suscettibili di arrecare rilevanti pregiudizi alla riservatezza. L'assenza di una "notifica individuale" – quand'anche relegata a momenti in cui non sia più suscettibile di compromettere le iniziative degli organi inquirenti – rende meramente "teorici" i diritti di accesso, rettifica e ricorso giurisdizionale, pur riconosciuti all'interessato.

La "vita privata" non è, peraltro, l'unico polo con cui la disciplina interagisce. Nell'arricchire l'armamentario al servizio delle autorità di *intelligence* e di *law enforcement*, è stata istituzionalizzata una specifica metodologia investigativa, fondata sull'esame dei dati PNR e suscettibile di sfociare nell'adozione di misure incidenti sulle libertà individuali. La peculiarità è che oggetto di *screening* sono informazioni ottenute e conservate, a scopi repressivi e di profilassi, a prescindere dall'emergere di elementi indizianti. L'obiettivo è individuare soggetti "non noti", persone, cioè, mai sospettate di essere coinvolte in gravi vicende criminose[23].

Si profila, all'orizzonte, una potenziale interferenza con la presunzione di innocenza: ogni passeggero è trattato con un pre-giudizio di pericolosità[24], che induce a confrontare i suoi dati personali con quelli contenuti in altri *database* adoperati in ambito criminalistico ed a valutarli alla luce di predeterminati (ma sconosciuti) criteri predittivi. Per la sola ragione di spostarsi per via aerea in territorio europeo o al di fuori dell'Unione, gli individui diventano potenziali sospetti di iniziative illecite (passate o future).

Noti sono i risvolti di un'archiviazione di massa di tal fatta. L'utilizzo, nel contesto di investigazioni penali, di dati raccolti in maniera indiscriminata e riversati in schedari pubblici accresce la possibilità di incappare, per sbaglio, nelle maglie della giustizia, di essere ingiustamente accusati di reati, di subire rilevanti restrizioni di libertà fondamentali. L'evenienza potrebbe essere generata da errori contenuti nelle banche dati impiegate per il raffronto, mai del tutto eliminabili per quante cautele si vogliano apprestare, così come potrebbe derivare dal controllo *ex ante* sulla scorta dei criteri elaborati attraverso l'uso proattivo dei dati[25]. L'analisi fondata su modelli e profili prefissati (funzionali, almeno in tesi, a svelare sospetti criminali o terroristi ancora ignoti) presenta significativi margini di errore, ampiamente riconosciuti anche dalla Direttiva che, con riferimento ai criteri di rischio, auspica che siano "*definiti in maniera da ridurre al minimo il numero di persone innocenti erroneamente identificate dal sistema*" (considerando n. 7). È espressamente considerata ed accettata la possibilità di "*falsi riscontri positivi*" (articolo 12, paragrafo 5 della Direttiva).

Il sistema può, dunque, essere fallace. Certo, l'obbligo di un esame individuale dei risultati del trattamento ed il divieto di decisioni automatizzate sono diretti a

[23] Sul tema, con particolare riferimento al recepimento della direttiva nell'ordinamento italiano, sia consentito il rinvio a P. TROISI, *Dati PNR e trattamento pre-investigativo*, in A. SCALFATI (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 319 ss.
[24] Cfr. F. ROSSI DAL POZZO, *op. cit.*, p. 1054.
[25] Così G. TIBERI, *op. cit.*, p. 592.

ridimensionare il pericolo. Ma, sicuramente, non permettono di escludere che persone vengano sottoposte a misure in qualche modo incidenti su diritti primari per l'unico motivo di aver viaggiato a bordo di un aeromobile. Un siffatto esito è ben idoneo ad intaccare le fondamenta di una società democratica, evocando le poco rassicuranti effigi di uno Stato di polizia.

Sono, questi, in realtà, aspetti critici già in parte evidenziati dalla Corte di Giustizia UE nel valutare (negativamente) la compatibilità, con i diritti sanciti dagli articoli 7 e 8 della Carta, dell'accordo PNR tra l'Unione e il Canada[26]. Molti degli argomenti in quella sede adoperati sono certamente riferibili anche alla Direttiva[27]. Né le conclusioni (positive) raggiunte dalla Commissione in sede di riesame della normativa dopo i primi due anni di attuazione (fondate, tra l'altro, su tredici casi studio in cui il sistema avrebbe fornito contributi alle indagini e sulla limitata percentuale di riscontri positivi, segno di una ricerca mirata)[28] sembrano offrire prove consistenti della necessità e proporzionalità di un congegno che coinvolge, ogni anno, quasi un miliardo di viaggiatori[29].

Spetterà, dunque, alla Corte di Giustizia sciogliere i dubbi sulla legittimità (totale o parziale) della Direttiva da più parti sollevati[30], tentando, ancora una volta, di ristabilire le giuste gerarchie tra libertà e sicurezza.

---

[26] Si tratta di Corte di Giustizia (Grande Sezione), parere del 26 luglio 2017, n. 1/15. In dottrina, tra i tanti: C. KUNER, *International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15,* EU-Canada PNR, in *Common Market Law Review*, Vol. 55, n. 3, 2018, p. 857 ss.; A. VEDASCHI, *The European Court of Justice on the EU-Canada Passenger Name Record Agreement*, in *European Constitutional Law Review*, Vol. 14, n. 2, 2018, p. 410 ss.; ID., *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione europea*, in *Giur. cost.*, Vol. 62, n. 4, 2017, p. 1913 ss.; S. VILLANI, *Some Further Reflections on the Directive (EU) 2016/681 on PNR Data in the Light of the CJEU Opinion 1/15 of 26 July 2017*, in *Revista de Derecho Político*, n. 101, 2018, p. 899 ss.; M. ZALNIERIUTE, *Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *Modern Law Rewiev*, Vol. 81, n. 6, 2018, p. 1046 ss.; E. CARPANELLI, N. LAZZERINI, *PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU*, in *Air and Space Law*, Vol. 41, nn. 4-5, 2017, p. 377 ss.; C. Graziani, *PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali*, in *DPCE Online*, Vol. 33, n. 4, 2017, p. 959 ss.

[27] Si tratta di conclusione ben evidenziata dall'*European Data Protection Board* che, con lettera del 22 gennaio 2021 alla Commissione (Ref: OUT2021-0004), sulla scia di quanto già rilevato dall'*ex* W*orking Party* 29 (nella lettera dell'11 aprile 2018 alla Commissione, consultabile su www.ec.europa.eu/newsroom/article29/redirection/document/51023), ha posto l'accento, principalmente, sugli argomenti relativi alla conservazione indiscriminata e a lungo termine dei dati ed al rischio di falsi positivi prodotti dalle verifiche automatizzate.

[28] Cfr. la Relazione della Commissione europea al Parlamento europeo e al Consiglio, *sul riesame della direttiva (UE) 2016/681 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*, del 24 luglio 2020, COM(2020) 305 e SWD(2020) 128.

[29] Cfr. la citata Lettera dell'*European Data Protection Board* del 22 gennaio 2021 alla Commissione europea (Ref: OUT2021-0004). Già nel Parere del Garante europeo per la protezione dei dati, del 24 settembre 2015, cit., punti 12-14, si evidenziava che nessun esauriente vaglio sia stato compiuto sull'efficacia di misure meno invasive. In dottrina, per rilievi critici in ordine alla necessità e proporzionalità dell'ingerenza, v., tra gli altri, F. DI MATTEO, *La raccolta indiscriminata*, cit., p. 223 ss.; G. TIBERI, *op. cit.*, p. 593, e, volendo, V. D'ANTONIO, P. TROISI, *Il delicato equilibrio tra sicurezza pubblica e rispetto della vita privata nel trattamento dei dati PNR a fini di* law enforcement, in *Comp. e dir. civ.*, n. 3, p. 1031 ss.

[30] Si tratta delle domande di pronuncia pregiudiziale nei casi Corte di Giustizia, causa C-817/19, *Ligue des droits humains*; Corte di Giustizia, cause riunite C-148/20, C-149/20 e C-150/20, *Deutsche Lufthansa*; Corte di Giustizia, causa C-215/20 *Bundesrepublik Deutschland*.

6. Conclusioni

Sullo sfondo delle linee evolutive che hanno caratterizzato il settore della cooperazione informativa campeggia l'intensificarsi, nel *post* 11 settembre, di un bisogno di sicurezza che, dal territorio nordamericano, si è rapidamente propagato nel "vecchio" continente, nella comune percezione di dover combattere, sinergicamente, una *global war*. In nome della difesa della collettività è progressivamente aumentata la propensione ad accettare limitazioni delle sfere di libertà, al punto da giustificare *counter-terrorism measures* che, se nel sistema statunitense si sono poste al di fuori del sistema penale ed hanno raggiunto livelli di aperta violazione di diritti umani (si pensi, in via meramente esemplificativa, agli omicidi mirati, alle *extraordinary renditions*, ai trattamenti detentivi degradanti)[31], non hanno tardato a fare ingresso, sia pure con intensità diversa, nella legislazione europea ed in quella dei singoli Stati membri. La necessità di fronteggiare la crescente minaccia terroristica e di combattere il fenomeno dei c.d. *foreign fighters* ha reso ancor più pressante, in linea con le indicazioni del Programma di Stoccolma[32], le *strategic guidelines* di Ypres[33], l'Agenda europea sulla sicurezza[34], l'esigenza di migliorare, intensificare e accelerare la circolazione di informazioni tra le autorità nazionali di contrasto, le agenzie dell'UE ed i Paesi terzi[35].

Il potenziamento dello scambio transfrontaliero e la tensione verso l'apprestamento di strumenti di sorveglianza di massa[36], quale indubbiamente è il monitoraggio automatizzato, su scala globale, dei dati forniti dai passeggeri all'atto della prenotazione di un volo, sono, nient'altro, che la reazione all'accresciuto senso di insicurezza.

Ad essere mutato sembra essere, in realtà, proprio il paradigma dei rapporti tra sicurezza e libertà: la "sicurezza pubblica", da fonte di possibili di compressioni, in via eccezionale, delle libertà individuali, ha assunto, essa stessa, fisionomia di diritto fondamentale, destinato tendenzialmente a prevalere, in un giudizio di bilanciamento, sui valori concorrenti[37].

---

[31] Su questi temi, per un'ampia panoramica, cfr., per tutti, T. GROPPI, *Democrazia e terrorismo. Diritti fondamentali e sicurezza dopo l'11 settembre*, Napoli, 2006, e, più di recente, K. ROACH (ed.), *Comparative Counter-Terrorism Law*, Cambridge, 2015.

[32] Documento del Consiglio n. 5731/10 relativo alle azioni da intraprendere nel quinquennio 2010-2014, del 3 marzo 2010.

[33] Si tratta del documento del Consiglio europeo n. 79/14, del 27 giugno 2014, contenente le conclusioni del Consiglio di Ypres, che hanno provveduto a delineare i nuovi orientamenti strategici destinati a guidare l'azione dell'Unione durante il quinquennio 2015-2020.

[34] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Agenda europea sulla sicurezza*, del 28 aprile 2015, COM(2015) 185 final.

[35] In tal senso si esprime la Risoluzione del Parlamento europeo, *sulle misure antiterrorismo*, dell'11 febbraio 2015, 2015/2530 (RSP), in GUUE C 310, del 25 agosto 2016, pp. 6-11, punto 22.

[36] Sul tema della "sorveglianza di massa" cfr., *ex multis*, D. COLE, F. FABBRINI, S. SCHULHOFER (eds.), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford, 2017; M. TZANOU, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, 2017; A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "*data retention*" al test di legittimità*, in *Dir. pubbl. comp. eur.*, n. 3, 2014, p. 1224 ss. Rilevante è, sul tema, Corte europea dei diritti dell'uomo (Grande Camera), sentenza del 21 maggio 2021, ricorsi nn. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito*, che ha ritenuto compatibile con l'art. 8 CEDU, sia pure a specifiche condizioni e con precise garanzie, intercettazioni di massa, acquisizioni e trasferimenti massivi di dati comunicativi a fini di *intelligence*.

[37] V., tra gli altri, sia pure con diversi accenti, C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova, Cedam, 2012, p. 73 ss; T.E. FROSINI, C. BASSU, *La libertà personale nell'emergenza costituzionale*, in A. DI GIOVINE (a cura di), *Democrazie protette e protezione della democrazia*, Torino, 2005, p. 77 ss.; P. TORRETTA, *"Diritto alla sicurezza" e altri diritti e libertà*

Le iniziative in cantiere sul versante dell'*information sharing* tra Stati membri ne danno ampia conferma. Tra le priorità della strategia dell'UE sulla sicurezza rientra, a pieno titolo, il rafforzamento della cooperazione informativa orizzontale, attraverso, principalmente, l'ammodernamento delle decisioni di Prüm ed un uso più efficace delle informazioni sui passeggeri[38].

Sotto il primo profilo, gli studi commissionati dalle Istituzioni europee hanno tracciato le direttrici per la realizzazione di un *Next Generation Prüm* sulla scia dei progressi tecnologici e dell'affermarsi di nuove metodiche di indagine fondate sull'impiego di dati genetici e biometrici[39]. Oltre all'aggiornamento delle norme sulla protezione dei dati, in coerenza con la Direttiva 2016/680/UE, le principali proposte mirano a migliorare efficacia ed efficienza del sistema[40], attraverso misure volte, tra l'altro, ad automatizzare la trasmissione dei dati personali in caso di *match* (soprattutto per quanto concerne le impronte digitali); ad incrementare le categorie di dati trattate, aggiungendo anche le immagini del viso (con conseguente sviluppo dei relativi archivi a livello nazionale), in modo da alimentare l'impiego del riconoscimento facciale per identificare gli autori di reati; a creare un *central router* che smisti le richieste degli Stati; ad individuare soluzioni per renderlo interoperabile con gli altri sistemi informativi UE; ad includervi anche i Paesi dei Balcani occidentali, per ricondurre nel quadro giuridico dell'Unione il percorso già avviato con la *Police Cooperation Convention for Southeast Europe* del 13 settembre 2018[41].

All'ordine del giorno, sotto il secondo profilo, è la revisione della Direttiva API[42] per eliminare le incongruenze che presenta con la normativa sul PNR[43]: la prima prevede che ogni Stato membro possa richiedere la trasmissione delle *Advance Passenger Information* al fine di migliorare i controlli alle frontiere e combattere l'immigrazione illegale, pur rimettendo alla discrezionalità di ciascun Paese la scelta di impiegarli anche per scopi, non meglio definiti, di *law enforcement* (senza, tuttavia, regolarne lo scambio); la seconda considera, invece, gli API componenti dei PNR, ove raccolti e registrati dal vettore. L'intento è omogeneizzare i due regimi, assoggettando le informazioni raccolte dai vettori in fase di *check-in* al medesimo trattamento previsto per quelle fornite in sede di prenotazione. Quanto a queste ultime, l'orientamento è, da un lato, rivedere l'attuale

---

della persona: un complesso bilanciamento costituzionale, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, 2003, p. 454 ss.

[38] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *sulla strategia dell'UE per l'Unione della sicurezza*, del 24 luglio 2000, COM(2020) 605 final, p. 26.

[39] Si tratta dello *Study on the feasibility of improving information exchange under the Prüm decisions*, redatto nel maggio 2020 da Deloitte Consulting su incarico della Commissione europea, e del *Police Information Exchange. The future developments regarding Prüm and the API Directive*", redatto nel settembre 2020 dal Policy Department for Citizens' Rights and Constitutional Affairs su richiesta della Commissione per le libertà civili, la giustizia e gli affari interni.

[40] Un invito in tal senso era stato già espresso dal Consiglio con il documento n. 11227/18, *on the implementation of the "Prüm Decisions" ten years after their adoption*, del 17 luglio 2018.

[41] In argomento, L. SCAFFARDI, Next Generation Prüm *e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it*, 24 marzo 2021.

[42] Si tratta della Direttiva 2004/82/CE del Consiglio, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate, del 29 aprile 2004, in GUUE L 261, del 6 agosto 2004, pp. 24-27, che fa rientrare tra i dati API tutte le informazioni che identificano il passeggero, il passaporto ed il volo;

[43] Cfr. lo *Study on Advance Passenger Information (API)*, redatto su incarico della Commissione europea nel febbraio 2020.

approccio restrittivo al trasferimento verso Paesi terzi[44]; dall'altro, estenderne l'utilizzo a forme di trasposto diverse da quello aereo[45].

L'ottica è, insomma, prettamente securitaria: le ricadute sulle libertà fondamentali sbiadiscono di fronte all'obiettivo del controllo proattivo delle più gravi forme di criminalità transnazionale.

Due sono, in particolare, i poli su cui è mancata adeguata riflessione: il rispetto della vita privata e la tutela dei diritti difensivi.

Quanto al primo, va rimarcato che l'apprestamento di un reticolo di norme – per quanto ampio e solido – a presidio della protezione dei dati non esaurisce il bisogno di tutela sotteso al concetto di *privacy*46, il cui nucleo duro poggia sul diritto del singolo di escludere la propria sfera intima da arbitrarie ingerenze da parte della pubblica autorità[47]. È, questo, un valore non solo individuale, ma anche sociale, che qualunque ideologia deve garantire se vuole lasciare all'individuo un margine di libertà nel quale agire ed operare[48]. La mera consapevolezza di non poter confidare nell'assenza di intrusioni pubbliche nella vita privata è, infatti, in grado di produrre un rilevante effetto dissuasivo all'esercizio delle altre libertà (c.d. *chilling effect*)[49].

Difficile è disconoscere, al riguardo, che tale diritto sia violato da meccanismi che, quand'anche rispondenti a finalità di interesse generale (sicurezza pubblica e lotta al terrorismo) e accompagnati da specifica disciplina sulla *data protection*, consentano ad organi di contrasto di accedere ad informazioni idonee ad aprire una significativa finestra sulla privatezza di soggetti non indiziati di reati, in assenza di *regole chiare* e *precise* che ne delimitino portata e campo applicativo; di *elementi oggettivi* che permettano di ritenere l'interferenza in grado di fornire un contributo *effettivo* a prevenire ben precise minacce; di autorizzazioni *preventive* (o, in caso di urgenza, *successive*) rilasciate da un *giudice* o da un'*autorità amministrativa indipendente*.

Quanto ai secondi, agevole è constatare che, nonostante le prerogative della persona coinvolta nell'accertamento penale occupino, oramai, un posto centrale nella "politica processuale" europea, nell'ambito dello sviluppo della cooperazione informativa si è registrato, sul tema, un sostanziale "non pervenuto". Ben vero è che gli strumenti basati sul principio di disponibilità non hanno l'ambizione di porsi come canali alternativi per l'acquisizione transnazionale della prova (tra i quali, oggi, domina l'ordine europeo di indagine penale); non può, tuttavia, escludersi che i dati, una volta penetrati nel procedimento penale, possano assumere rilievo probatorio. La possibilità è, ad esempio, espressamente contemplata dalla Decisione quadro "svedese", in base alla quale, con il consenso dello Stato trasmittente, le informazioni ricevute possono essere utilizzate come

---

[44] Cfr. la Comunicazione della Commissione al Parlamento europeo e al Consiglio EMPTY, *Prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza*, del 9 dicembre 2020, COM(2020) 797 final, p. 29.

[45] Documento del Consiglio n. 14746/19, *on widening the scope of the use of passenger name record (PNR) data to forms of transport other than air traffic*, del 2 dicembre 2019.

[46] Cfr. P. DE HERT, S. GUTWIRTH, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in E. CLAES, A. DUFF, S. GUTWIRTH (eds.), *Privacy and the Criminal Law*, Cambridge, 2006, p. 77, secondo cui "*the sheer wordings of the data protection principles (…) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice, [with data protection law creating] a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal*".

[47] Nella versione di *right to be let alone*, fondamentale è il contributo di S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Har. L. Rev.*, Vol. 4, n. 5, 1890, p. 193 ss.

[48] Cfr. P. PATRONO, *Privacy e vita* privata, voce in *Enc. dir.*, Vol. XXXV, Milano, 1986, p. 560.

[49] Sul c.d. *chilling effect*, cfr. le considerazioni di A.F. WESTIN, *Privacy and Freedom*, New York, 1967, p. 349 ss., secondo cui lo scopo della *privacy* è proprio "*to allow for unguarded, experimental 'release' behavior of individuals, and this outlet is just what our dossier-computer system is threatening*".

"*prove dinanzi ad un'autorità giudiziaria*" (articolo 1, paragrafo 4, della Decisione quadro). Gli stessi dati PNR, trasferiti dalla UIP all'autorità giudiziaria, è inevitabile che acquistino valenza probatoria ove riversati in ambito procedimentale. Né preclusioni sembrano ricavabili dal principio di finalità limitata: arduo sarebbe, ad esempio, negare che i dati PNR entrati nei fascicoli processuali siano valutabili per la prova di reati ulteriori e diversi da quelli che ne legittimano l'iniziale trattamento.

A fronte di questa prospettiva, evidente è il *vulnus* per le garanzie difensive sotto una duplice prospettiva: la difficoltà di verificare e, dunque, criticare l'affidabilità delle informazioni che hanno ingresso nel procedimento attraverso i circuiti della cooperazione informativa; la carenza di poteri di accesso da parte della difesa alle banche dati nazionali ed europee nelle investigazioni difensive.

Inevitabile è la conclusione: senza valorizzare la vita privata ed il diritto di difesa, la legislazione dell'Unione sulla cooperazione informativa è destinata, inevitabilmente, a divenire l'occasione per un livellamento verso il basso delle garanzie individuali.

ABSTRACT

Migliorare la condivisione delle informazioni tra le autorità degli Stati membri secondo il principio di disponibilità è un obiettivo centrale della strategia di sicurezza dell'UE. Nella lotta contro il terrorismo e la grave criminalità transnazionale, le tendenze attuali puntano nella direzione di un crescente utilizzo dei dati personali raccolti nel settore privato e trattati per scopi proattivi. A questo proposito, emblematico di questa tendenza è la disciplina dettata dalla Direttiva PNR, che crea un sistema di sorveglianza di massa basato sulla raccolta, l'archiviazione, l'analisi e lo scambio indiscriminati di dati personali dei passeggeri senza alcun motivo che basato su circostanze oggettive faccia dedurre che le persone interessate possano essere coinvolte in un reato. Molte sono però le criticità che riguardano il diritto alla privacy*, la presunzione di innocenza e le tutele difensive. La prospettiva, confermata anche dai progetti in cantiere (*Next Generation Prüm *e utilizzo dei dati API), è essenzialmente securitaria. Ciò che manca è un'adeguata riflessione circa gli effetti sulle libertà fondamentali.*

KEYWORDS

Condivisione delle Informazioni, Cooperazione tra le forze dell'ordine, Direttiva PNR, Diritto alla Privacy, Pubblica Sicurezza, Sorveglianza di Massa.

PRINCIPLE OF AVAILABILITY, HORIZONTAL COOPERATION AND PNR DATA EXCHANGE

ABSTRACT

Enhancing the information sharing between the law enforcement authorities of the Member States according to the principle of availability is a central objective of the EU Security Strategy. In the fight against terrorism and serious transnational crime, current trends point in the direction of an increasing use of personal data collected in the private sector and processed for proactive purposes. In this regard, emblematic of this trend is the regulation dictated by the PNR Directive, which creates a system of mass surveillance

based on the indiscriminate collection, storage, analysis and exchange of personal data of passengers without any reason based on objective circumstances to infer that the individuals concerned may be involved in a crime. There are, however, many critical issues, involving the right to privacy, the presumption of innocence, and defensive safeguards. The perspective, also confirmed by projects in the pipeline (Next Generation Prüm and use of API data), is essentially securitarian. What is lacking is an adequate reflection on the effects on fundamental freedoms.

KEYWORDS
Information Sharing, Law Enforcement Cooperation, Mass Surveillance, PNR Directive, Public Security, Right to Privacy.