Il volume è stato pubblicato con il contributo della

Fondazione
FONDAZIONE CRTRIESTE

L'opera costituisce l'esito della ricerca effettuata
dall'unità triestina nell'ambito del PRIN 2005 –
dedicato al tema "Protezione dei dati personali e processo penale" –
che ha visto coinvolte anche le Università di Ferrara, Firenze e Roma

impaginazione
Gabriella Clabot

ISBN 978-88-8303-256-1

EUT - Edizioni Università di Trieste
p.zzale Europa, 1 – 34127 Trieste
http://eut.units.it

Cooperazione informativa e giustizia penale nell'Unione europea

a cura di
Francesco Peroni
Mitja Gialuz

EUT EDIZIONI UNIVERSITÀ DI TRIESTE

Sommario

Abbreviazioni

AFIS: *Anti-Fraud Information System/Automated Fingerprint Identification System*
API: *Advance Passenger Information*
art.: Articolo
CAAS: Convenzione di applicazione dell'accordo di Schengen
CE: Comunità Europea
CEDU: Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
Conv. eur. ass. giud.: Convenzione europea di assistenza giudiziaria in materia penale
COREPER: *Comité des représentants permanents*
Cost.: Costituzione
c.p.p.: Codice di procedura penale
d.lgs.: Decreto legislativo
d.P.R.: Decreto del Presidente della Repubblica
ECR: *European Criminal Record*
ECRIS: *European Criminal Records Information System*
ELO: *Europol Liaison Officers*
EPOC: *European Pool against Organized Crime*
Eurodac: *European dactylographic system*
GAI: Giustizia e Affari Interni
GEPD: Garante europeo della protezione dei dati
MAE: Mandato d'Arresto Europeo
MER: Mandato Europeo di Ricerca delle prove
OLAF: *Office Européenne de Lutte Anti Fraude*
PNR: *Passenger Name Record*
SIRENE: *Supplementary Information Request at the National Entry*
SID: Sistema Informativo Doganale
SIS: Sistema di Informazione Schengen
TCE: Trattato che istituisce la Comunità europea
TECS: *The Europol Computer System*
TESTA: *Trans-European Services for Telematics between Administrations*
TUE: Trattato sull'Unione europea
UE: Unione Europea
UNE: Unità Nazionali Europol
VIS: *Visa Information System*

L'ultimo accesso ai siti citati nel volume risale al 30 aprile 2009.

Introduzione

Quasi dieci anni or sono veniva pubblicato il Programma di Tampere, vero e proprio atto fondativo dello spazio europeo di libertà, sicurezza e giustizia[1]. Nel dare attuazione agli obiettivi fissati in tale documento, l'Unione europea ha compiuto, in questi due lustri, significativi passi avanti nella costruzione di detto spazio, tramite l'approvazione di svariati strumenti normativi di grande impatto. Nella letteratura processualpenalistica italiana si è dedicata prevalente attenzione ai progressi realizzati nell'ambito della cooperazione giudiziaria e, in particolare, a quella che è probabilmente la più rilevante delle riforme, ossia la decisione quadro sul mandato d'arresto europeo. Non è stata, invece, oggetto di autonomo approfondimento una forma specifica di cooperazione, che pure ha assunto un ruolo essenziale nella società dell'informazione, ossia quella che si è definita cooperazione informativa.

Si tratta di una forma di cooperazione che è assurta a perno del rafforzamento della libertà, della sicurezza e della giustizia nel secondo documento programmatico elaborato dal Consiglio europeo nel 2004, vale a dire nel Programma dell'Aia. Negli anni successivi, proprio la materia della cooperazione informativa

1 In tal senso, E. Barbe, L'*espace judiciaire européen*, Parigi, La documentation française, 2007, p. 21.

è stata oggetto di numerosi interventi normativi. Da ultimo, la valenza strategica della cooperazione informativa emerge dai lavori preparatori del "Programma di Stoccolma", che dovrebbe essere adottato nella seconda metà del 2009 (sotto la Presidenza svedese) e dovrebbe indicare le priorità del legislatore europeo in materia di sicurezza e giustizia per i prossimi cinque anni[2].

Il volume nasce con il proposito di contribuire al superamento della segnalata lacuna. Esso è il frutto di uno studio realizzato nell'ambito di un progetto di ricerca di rilevante interesse nazionale – dedicato al più ampio tema della "Protezione di dati personali e processo penale" e condotto insieme alle unità degli Atenei di Ferrara, di Firenze e di Roma – dai processualpenalisti del Dipartimento di Scienze Giuridiche triestino.

Come si vedrà, nell'orbita concettuale della cooperazione informativa si sono individuati due profili: uno statico e uno dinamico. Si è approfondito in particolare il secondo, che investe specificamente lo scambio di informazioni tra le autorità di polizia e le autorità giudiziarie dei Paesi membri dell'Unione. In questa cornice, si sono coltivate molteplici le linee di ricerca, in corrispondenza ad altrettante chiavi di lettura dell'indagine.

Anzitutto, ci si è prefissi di fornire una ricostruzione sistematica delle diverse fattispecie di cooperazione informativa, individuando due diverse tipologie, che appaiono in certa misura riconducibili a due differenti approcci all'integrazione europea. Da un lato, si è individuata la cooperazione informativa "accentrata" di stampo comunitario, imperniata su banche dati europee centralizzate, ossia su sistemi informativi gestiti, sia pure con modalità variabili, da un organismo sovranazionale: si pensi al SIS, al SID, al TECS di Europol, all'EPOC-III di Eurojust. Dall'altro lato, si è dato conto del crescente ricorso alla cooperazione informativa "diretta" o a rete, che appare figlia di un approccio intergovernativo: essa è rappresentata dallo scambio di informazioni tra le autorità dei singoli Paesi membri. Tra le principali figure, si sono analizzati il sistema a rete introdotto dal Trattato

---

2 Cfr. la *Relazione del Gruppo consultivo informale ad alto livello sul futuro della politica europea in materia di affari interni ("Gruppo del futuro")*, *Documento del Consiglio n. 11657/08*, 9 luglio 2008, <http://register.consilium.europa.eu/pdf/it/08/st11/st11657.it08.pdf>, p. 12 (§ 44), p. 16 (§ 52): siffatto documento dovrebbe introdurre il *convergence principle*, che mira «a ravvicinare gli Stati membri non solo mediante la [standardizzazione] quando è necessaria ma anche con mezzi operativi. Programmi di formazione comune, reti di scambio, meccanismi di solidarietà, utilizzazione in comune di alcuni strumenti, procedure semplificate di cooperazione e, ovviamente, scambi di informazioni sono mezzi essenziali per giungere a una coooperazione operativa vera ed effettiva tra gli Stati membri dell'Unione». Sulle prospettive relative al documento programmatico per il quinquiennio 2009-2014, si legga E. Guild – S. Carrera – A. Faure Atger, *Challenges and Prospects for the EU's Area of Freedom, Security and Justice: Recommendations to the European Commission for the Stockholm Programme*, CEPS Working Document No. 313/April 2009, pp. 1 sgg.

di Prüm e recepito dalla decisione 2008/615/GAI e il sistema europeo di informazione dei casellari giudiziari (ECRIS) previsto dalla decisione 2009/316/GAI.

Con riguardo alle banche dati centralizzate dell'Unione, si è inteso compiere un aggiornamento del quadro di riferimento: nel novembre del 1999, il *Select Committee on European Union* della *House of Lords* presentò un *Report* sulle banche dati europee[3]. La premessa dalla quale muoveva lo studio era che, a fronte dei notevoli benefici indotti dalle crescenti opportunità di raccolta delle informazioni, si profilavano nuovi interrogativi legati all'origine e alla qualità dei dati. Ci si chiedeva, in particolare, chi alimentasse questi archivi, chi vi avesse accesso, quali fossero i diritti di controllo dei cittadini, quali i legami tra i diversi *databases* e, quale, infine, il livello di sicurezza garantito. A questi stessi interrogativi si cerca qui di fornire una risposta, alla luce delle significative modifiche normative sopravvenute[4].

Il terzo obiettivo fondamentale è stato quello di verificare se, e in qual misura, lo sviluppo della cooperazione informativa si sia accompagnato all'effettiva tutela dell'*habeas data*. In termini generali, vi è ormai consenso sul fatto che tra implementazione delle politiche di sicurezza e rafforzamento dei diritti – o, in termini ancor più ampi, tra *efficiency* e *accountability* – non vi è incompatibilità concettuale. Altrettanto non sembra potersi affermare per quel che riguarda il rapporto tra «police information gathering and data protection»[5]: al proposito, resta diffusa – almeno a livello politico[6] – l'idea che si tratti di due punti di vista difficilmente conciliabili. Effettivamente, la fatica con la quale si è giunti all'adozione di una decisione quadro sulla protezione dei dati e – ciò che più conta – il contenuto stesso della decisione 2008/977/GAI sembrano confermare che questo è il substrato culturale che ha ispirato l'approccio concreto del Consiglio, a differenza di quello delle istituzioni comunitarie[7].

---

3 Il testo è disponibile all'indirizzo <http://www.publications.parliament.uk/pa/ld199899/ldselect/ldeucom/120/12001.htm>.

4 In un'ottica non dissimile si pone il saggio di F.F. Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, <http://www.libertysecurity.org/IMG/pdf__Databases__and__Systems__of__Information__Exchange__in__the__Area__of__Freedom__Security__and__Justice.pdf>, p. 3.

5 Così, N. Walker, "Freedom, Security and Justice", in *Ten reflections on the constitutional Treaty of the Europe*, a cura di B. De Witte, European University Institute, Fiesole, 2003, p. 169.

6 In ambito scientifico è invece acquisito che una migliore tutela del diritto alla protezione del dato non può che aumentare la propensione allo scambio delle informazioni: cfr. M. McGinley – R. Parkes, *Data Protection in the EU's Internal Security Cooperation. Fundamental Rights vs. Effective Cooperation?*, SWP Research Paper No. 5, Berlino, 2007, <http://www.swp-berlin.org/en/common/get__document.php?asset__id=4034> p. 13.

7 D'altra parte, si era acutamente osservato che «if and when the EU does introduce rules on data protection in the police sector, they are likely, in the current context of law enforcement "globalization," to meet a very low standard» (B. Hayes, "A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe", in *Ethnic Profiling by Police in Europe*, Justice

Proprio la constatata, diversa sensibilità delle varie istituzioni dell'Unione introduce un terzo filo, sotteso a molte delle riflessioni sviluppate nel volume: quello dei costi dell'assetto istituzionale del cosiddetto "terzo pilastro". Si allude, anzitutto, agli effetti che l'assetto istituzionale dell'Unione produce sul piano dei contenuti delle norme europee: dall'analisi dello sviluppo della cooperazione informativa emerge chiaramente il prezzo, in termini di salvaguardia dei diritti fondamentali, del mancato superamento, nella materia *de qua*, del metodo intergovernativo. Il secondo pregiudizio attiene invece alla frammentazione del processo d'integrazione in materia penale: la persistenza del voto all'unanimità ha condotto infatti al proliferare di cooperazioni "rafforzate", esterne alla cornice comunitaria. Di fronte all'incapacità del Consiglio di dare risposte in tempi ragionevoli alla notevole spinta all'implementazione della cooperazione informativa, diversi Stati membri – tra i quali, purtroppo, non l'Italia – si sono mossi fuori dalle istituzioni dell'Unione: oltre al caso degli ormai risalenti accordi di Schengen, si sono analizzate le vicende – più recenti e più prossime ai profili di attuazione del canone di disponibilità – relative al Trattato di Prüm e all'interconnessione dei casellari giudiziari[8]. Merita notare sin d'ora che, in questi ultimi casi, l'accelerazione realizzata da alcuni Stati membri è stata velocemente riassorbita dall'Unione europea, che, nell'arco di qualche anno, ha recepito le novità nell'*acquis communautaire*. Il che sembrerebbe dimostrare che i ritardi delle istituzioni dell'Unione erano imputabili – almeno con riguardo alla cooperazione informativa – proprio all'imperfetto meccanismo decisionale, più che all'insufficiente grado di integrazione degli ordinamenti nazionali.

L'ultima prospettiva esplorata nel libro concerne il progressivo superamento dei confini, tra quelli che erano tradizionalmente ambiti ben distinti: la cooperazione di polizia, da un lato, e la cooperazione giudiziaria, dall'altro. E in effetti, la cooperazione informativa presenta particolare interesse proprio in quanto trasversale ai due versanti: essa riguarda, sia le informazioni di polizia, sia quelle giudiziarie. In questa angolazione, si è tentato di verificare, se e in qual misura,

---

Initiative, 2005, p. 39, <http://www.justiceinitiative.org/db/resource2?res__id=102731>.

8 Esprimono perplessità sui benefici che queste cooperazioni intergovernative possono portare all'intera Unione europea, T. Balzacq- D. Bigo-S. Carrera-E. Guild, "The Treaty of Prüm and EC Treaty: Two Competing Models for EU Internal Security", in *Security Versus Freedom? A Challenge for Europe's Future*, a cura di T. Balzacq e S. Carrera, Ashgate, Aldershot, 2006, pp. 132 sgg.; N. Quillet, *Le traité de Prüm relatif à l'approfondissement de la coopération transfrontalière*, in "Revue du Marché commun et de l'Union européenne", 2007, pp. 660 sgg. Il fenomeno del crescente ricorso a iniziative di cooperazione da parte di «avanguardie» di Stati membri è posto in luce da F. Pastore, "L'evoluzione dello Spazio di libertà, sicurezza e giustizia. Progressi, limiti e divisioni", in *Perché l'Europa?*, a cura di J.L. Rhi-Sausi e G. Vacca, Bologna, il Mulino, 2007, pp. 250 sgg.

il rafforzamento delle banche dati europee centralizzate, l'attuazione dei canoni di disponibilità e di accessibilità possano agevolare lo scambio di informazioni, anche ai fini di un loro utilizzo nell'ambito del procedimento penale italiano.

FRANCESCO PERONI
Professore ordinario di Procedura penale
Università di Trieste

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

La cooperazione informativa quale motore del sistema europeo di sicurezza

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

Sommario: 1. La costruzione di un sistema di sicurezza dell'Unione europea. – 2. Principio di disponibilità in senso lato e cooperazione informativa. – 3. Il profilo dinamico della cooperazione informativa: interoperabilità, disponibilità in senso stretto e accessibilità. – 4. Il profilo statico della cooperazione informativa: principio di conservazione. – 5. (Segue): la direttiva sulla *data retention*.

1. La costruzione di un sistema di sicurezza dell'Unione europea

Il decennio che volge al termine si era aperto sotto i migliori auspici per il processo di integrazione europea. La strategia di Lisbona, l'introduzione dell'euro, la Carta dei diritti fondamentali di Nizza, la prospettiva dell'allargamento e, soprattutto, l'apertura di una stagione costituente avevano segnato i primissimi anni del nuovo millennio. In un celebre discorso, tenuto all'Università von Humboldt di Berlino nel maggio del 2000, l'allora Ministro degli Esteri tedesco Josckha Fischer aveva tracciato la via per una rifondazione costituzionale dell'Europa[1] e la sfida era stata successivamente raccolta, prima con la dichiarazione di Laeken e poi con il lavoro della Convenzione sul futuro dell'Europa.

Purtroppo, è ben noto come siano andate le cose. Tanto il progetto di "trattato costituzionale", quanto il Trattato di Lisbona – che dovrebbe consentire di salvare la sostanza delle modifiche indicate dalla "Costituzione per l'Europa" – sono stati bocciati dai referendum tenuti in alcuni Stati membri e ciò ha determinato una crisi profonda del processo di integrazione. Sotto il profilo istituzionale, quindi, il bilancio degli anni duemila è tutt'altro che soddisfacente.

Nonostante queste battute d'arresto, l'«ermafrodita europeo» ha continuato a crescere e a operare[2]. E un certo dinamismo ha dimostrato nel perseguire quell'obiettivo fondamentale rappresentato dall'istituzione di uno spazio di libertà, sicurezza e giustizia (art. 61 TCE). Le istituzioni dell'Unione e gli Stati membri hanno fatto progressi, soprattutto nella direzione del rafforzamento della sicurezza.

Evidentemente, ciò si spiega anzitutto sulla base di ragioni contingenti, legate alla necessità di fornire una risposta sovranazionale alla recrudescenza del terrorismo internazionale e di altre gravi forme di criminalità. Dopo gli attentati terroristici dell'11 settembre 2001, di Madrid e di Londra, la realizzazione dello spazio di sicurezza, libertà e giustizia ha registrato una sensibile accelerazione e ha avuto come motore decisivo la lotta al terrorismo. Ciò ha condotto inesorabilmente a valorizzare la sicurezza a discapito dei valori della libertà e della giustizia[3]. E, d'altra parte, il carattere reattivo delle politiche in materia di sicurezza

---

1 Cfr. J. Fischer, "From Confederacy to Federation: Thoughts on the Finality of European Integration", in *What Kind of Constitution for What Kind of Polity? Responses to Joschka Fischer*, a cura di C. Joerges, Y. Mény, J.H.H. Weiler, Badia Fiesolana, European University Institute, 2000, <http://www.jeanmonnetprogram.org/papers/00/symp.html>, p. 27.

2 La qualificazione dell'Europa come «ermafrodita» si deve a G. Amato, in *Una democrazia senza Costituzione? L'Europa e gli europei dopo i referendum*, a cura di G. Laschi, Bologna, CLUEB, 2007, p. 24.

3 In termini critici, T. Balzacq - S. Carrera, "The Hague Programme: the Long Road to Freedom, Security and Justice", in *Security Versus Freedom? A Challenge for Europe's Future*, a cura di T. Balzacq e S. Carrera, Ashgate, Aldershot, 2006, p. 18; D. Bigo, "Liberty, whose Liberty? The Hague Programme and the Conception of Freedom", *ivi*, pp. 36 sgg.; S. Buzzelli, "Processo penale europeo", in *Enciclopedia del diritto. Annali*, II.1, Milano, Giuffrè, 2008, p. 707 (ivi ulteriori indicazioni bibliografiche in ordine a quella che l'Autrice definisce «deriva securitaria europea»).

interna non è una novità, ma una caratteristica costante che si ritrova alla base anche di precedenti iniziative. Basti pensare all'istituzione della rete TREVI, come risposta al fenomeno terroristico degli anni settanta oppure alla stessa creazione della cooperazione di polizia e giudiziaria nel trattato di Maastricht quale scelta volta a compensare l'erosione graduale della sovranità degli Stati membri sul loro territorio, derivante dalla soppressione dei controlli alle frontiere prodotta dagli accordi di Schengen e dalla progressiva globalizzazione dell'attività delle organizzazioni criminali[4]. Sicuramente l'abolizione dei confini ha trasformato una parte dell'Europa «into one criminal–geographic space» e la successiva introduzione – con il Trattato di Amsterdam – del concetto di uno spazio di libertà, sicurezza e giustizia ha portato a definire «the territory of the EU in its entirety as indivisible in matters of internal security, i.e., de facto as territory of one state»[5].

Sarebbe peraltro riduttivo concepire le politiche di rafforzamento della sicurezza interna in senso meramente reattivo. È stato notato che non si possono comprendere i progressi realizzati nel corso degli anni novanta, né tanto meno si può capire l'esteso e ambizioso Programma di Tampere «apart from an appreciation of the growing desire in many EU policy circles to find a new 'big idea' to mobilize support for the European Union at a point when the founding ideals of the Union – peace and prosperity – had lost some of their earlier freshness (if not their relevance) and public opinion was becoming increasingly ambivalent about the legitimacy of increasing integration»[6]. Insomma, la tutela della sicurezza individuale – in senso lato – potrebbe rappresentare proprio questa "big idea" idonea a giustificare il rilancio dell'integrazione europea[7].

All'interno di queste coordinate, a livello europeo si sta costruendo «an enormous transnational security regime», che ruota intorno alla cooperazione informativa: com'è stato notato, infatti, «the core of this new European Security Regime is to be a system of transnational information Exchange»[8].

---

4 V. G. de Kerchove, "Améliorations institutionnelles à apporter au titre VI du traité sur l'Union européenne afin d'accroître l'efficacité et la légitimité de l'action de l'Union européenne dans le domaine de la sécurité intérieure", in *Quelles riforme pour l'espace pénal européen?*, a cura di G. de Kerchove e A. Weyembergh, Bruxelles, Editions de l'Université de Bruxelles, 2003, p. 20.

5 Così, L. Hempel – M. Carius – C. Ilten, *Exchange of information and data between law enforcement authorities within the European Union*, <http://www.statewatch.org/news/2009/apr/Study__Exchange%20of%20information%20and%20data%20between%20law%20enforcement%20authorities%20within%20the%20EU__EN.pdf>, p. 13.

6 Cfr. sul punto N. Walker, "Freedom, Security and Justice", in *Ten reflections on the constitutional Treaty of the Europe*, a cura di B. De Witte, European University Institute, Fiesole, 2003, p. 162.

7 Secondo G. Morgan, *The Idea of a European Superstate. Public Justification and European Integration*, Princeton e Oxford, Princeton University Press, 2005, p. 143, proprio la salvaguardia della sicurezza potrebbe rappresentare «a more promising basis to justify the sovereignist project of European integration».

8 Queste le parole di L. Hempel – M. Carius – C. Ilten, *op. cit.*, p. 13.

Evidentemente, la progressiva valorizzazione della cooperazione informativa è stata determinata anzitutto dallo sviluppo tecnologico: lo "tsunami digitale" che ha caratterizzato le nostre società negli ultimi lustri ha portato a un incremento esponenziale delle tracce digitali, delle informazioni, che risultano facilmente immagazzinabili in archivi informatici e che possono circolare per finalità di contrasto alla criminalità a prescindere dai tradizionali limiti spaziali[9]. Per altro verso, il potenziamento della cooperazione informativa è stato sicuramente favorito dalla diffusione del paradigma dell'*intelligence led policing*, ossia di quel modello di *policing* fondato sull'analisi strategica di tutte le informazioni disponibili[10].

2. Principio di disponibilità in senso lato e cooperazione informativa

Sul piano del diritto dell'Unione, il problema dello scambio di informazioni tra le autorità di *law enforcement* era stato affrontato già nel corso degli anni novanta. Il primo passo nel senso dell'implementazione di questa essenziale forma di cooperazione era stato la firma della Convenzione di applicazione dell'accordo di Schengen del giugno 1990, che prevedeva, da un lato, l'istituzione del Sistema di informazione Schengen (SIS) e, dall'altro, la possibilità di uno scambio diretto e spontaneo di informazioni tra le autorità di polizia (artt. 39 e 46); era seguita, nel 1995, la creazione dell'Europol, quale organismo deputato istituzionalmente ad «agevolare lo scambio di informazioni fra Stati membri» (art. 3, n. 1). Successivamente, erano intervenute la Convenzione sull'assistenza giudiziaria in materia penale – il cui art. 7 riprende l'istituto dello scambio di informazioni – e la decisione istitutiva di Eurojust.

Nonostante queste iniziative, ancora agli inizi del nuovo millennio le frontiere nazionali costituivano barriere reali per la circolazione delle informazioni rilevanti ai fini dell'applicazione della legge[11]. A una vera e propria svolta si è giunti soltanto dopo gli attentati terroristici di New York, Madrid e Londra. Tanto che la consacrazione della centralità della cooperazione informativa nel sistema europeo di sicurezza si è avuta con il Programma dell'Aia[12]. Se per molti versi esso è stato giudicato timido e poco ambizioso – soprattutto se comparato al primo do-

---

9 Cfr., per ulteriori indicazioni bibliografiche, *Information Technology and the Criminal Justice System*, a cura di A. Pattavina, Thousand Oaks, Sage Publications, 2005, *passim*.

10 Sul nesso tra sviluppo dell'*intelligence-led policing* e interoperabilità delle banche dati, cfr. P. De Hert - S. Gutwirth, *Interoperability of police databases within the EU: an accountable political choice?*, <http://papers.ssrn.com/sol3/papers.cfm?abstract__id=971855>, p. 9.

11 **Al riguardo, si legga** G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access*, Antwerp-Apeldoorn, Maklu, 2005, pp. 16 sgg., ove vengono indicati i sette principali ostacoli alla circolazione delle *law enforcement informations*.

12 In *GUUE*, C 53, 3 marzo 2005, p. 1.

cumento di pianificazione generale adottato nel 1999 a Tampere[13] –, altrettanto non può dirsi per il tema specifico oggetto di indagine. Al riguardo, il Programma ha realizzato un salto di qualità con l'introduzione del principio di disponibilità delle informazioni: questo canone viene esplicitato nel documento in termini restrittivi, con riferimento specifico allo scambio tra le autorità nazionali delle informazioni di *law enforcement*.

In realtà, da un'interpretazione più attenta del Programma e da una lettura sistematica delle politiche dell'Unione, sembra potersi desumere l'esistenza di un canone di disponibilità in senso lato, in forza del quale le autorità di *law enforcement* degli Stati membri e dell'Unione debbono poter disporre del maggior numero possibile di informazioni rilevanti ai fini della prevenzione e della repressione dei reati.

Ebbene, lo strumento di attuazione di questo canone a livello europeo è rappresentato dalla cooperazione informativa. Ciò che dipende dall'architettura "costituzionale" dell'Unione: la quale impedisce di affidare l'implementazione della disponibilità in senso lato in tutto e per tutto agli organi e alle istituzioni dell'Unione. Nonostante i propositi di cui si è detto all'inizio, si deve prendere atto che la finalità di tutela della sicurezza interna non ha portato ancora a configurare l'Unione come un attore indipendente nell'ambito dell'attività di *law enforcement*. Dalla stessa intitolazione del titolo VI del Trattato sull'Unione europea – "*cooperazione* di polizia e giudiziaria" –, al catalogo delle competenze dell'Unione – che enfatizza soprattutto la facilitazione della cooperazione –, alla precisazione dell'art. 33 TUE – il quale specifica che rimane in capo agli Stati membri il compito di mantenere l'ordine pubblico e la sicurezza interna –, si evince come la "filosofia" che anima il "terzo pilastro" sia quella per cui gli Stati membri debbono usare l'Unione per incrementare l'efficienza dei loro sistemi nazionali di sicurezza: com'è stato rilevato, «the EU is thus seen as a qualitative addition to the repressive branch of the National systems of criminal justice»[14]. Si badi, peraltro, che queste considerazioni e lo stesso impiego della locuzione "cooperazione informativa" non escludono affatto che la stessa Unione abbia un ruolo diretto nella cooperazione. Come si avrà modo di vedere, vi è una cooperazione informativa "accentrata" di stampo comunitario, la quale è imperniata su banche dati europee

13 Cfr., in particolare, E. Paciotti, "Quadro generale della costruzione dello spazio di libertà, sicurezza e giustizia", in *Verso l'Europa dei diritti. Lo spazio europeo di libertà, sicurezza e giustizia*, a cura di G. Amato ed E. Paciotti, Bologna, il Mulino, 2005, p. 31. Proprio la genericità del documento aveva indotto qualche osservatore maligno a ribattezzare «the Hague Programme», come «the Vague Programme» (così, L. Salazar, "La costruzione di uno spazio penale comune europeo", in *Lezioni di diritto penale europeo*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2007, p. 455).

14 Così, M. Fletcher - R. Lööf - B. Gilmore, *EU Criminal Law and Justice*, Northampton, Edward Publishing Limited, 2008, p. 46.

centralizzate, che sono gestite da un organismo sovranazionale: si pensi al SIS, al SID, al TECS di Europol, all'EPOC-III di Eurojust[15].

3. Il profilo dinamico della cooperazione informativa: interoperabilità, disponibilità in senso stretto e accessibilità

Ragionando della cooperazione informativa, si possono mettere in luce due diversi profili: uno statico e uno dinamico. Merita prendere le mosse da quest'ultimo, per la semplice ragione che esso è l'unico a essere trattato espressamente dal Programma dell'Aia. Laddove riconosce l'irrilevanza dell'attraversamento delle frontiere dei dati utili ai fini dell'attività di *law enforcement* (§ 2.1), il Consiglio sancisce il canone della libera circolazione delle informazioni. E traccia le tre direttrici lungo le quali l'Unione deve muoversi per darvi attuazione.

La prima è rappresentata dall'investimento sulle tecnologie («lo scambio di informazioni dovrebbe sfruttare appieno le nuove tecnologie») e sullo sviluppo dei sistemi informativi centralizzati. In particolare, il Consiglio europeo ha auspicato l'attuazione del sistema di informazione sui visti (VIS), con l'incorporazione dei dati biometrici, la massimizzazione dell'efficacia dei sistemi di informazione dell'Unione (VIS, SIS II, Eurodac) e la loro eventuale interoperabilità (§ 1.7.2).

La seconda direttrice fondamentale coincide con il riconoscimento esplicito del principio di disponibilità (§ 2.1), che è destinato a governare la cooperazione tra le autorità nazionali di *law enforcement*: esso prescrive che «un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro, e che il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni è tenuto a trasmettergliele per i fini dichiarati, tenendo conto dei requisiti relativi alle indagini in corso nel suddetto Stato»[16]. Per la verità, alla luce di quanto si è notato, si dovrebbe parlare di tale canone come del principio di disponibilità in senso stretto[17]: esso appare riconducibile alla stessa matrice del principio del mutuo riconoscimento[18] e si è detto che rappresenta «one of the key challenges to state sovereignty, because the availability of information therefore no longer depends on the 'good will' of the law enforcement agency of the state

---

15 Cfr. *infra*, F. Decli - G. Marando, "Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia".

16 Così, *Programma dell'Aia*, cit., p. 7. Su tale canone, cfr. ampiamente, *infra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea".

17 A tale riguardo, è opportuno precisare che, nel libro, si utilizzerà l'espressione "principio di disponibilità" per indicare il canone di disponibilità in senso stretto.

18 Cfr. E. De Busser, *The architecture of data exchange*, in "International Review of Penal Law", 2007, p. 39.

reveiving the request and because the principle of availability touches indirectly upon the relation of National services amongst themselves»[19].

La terza prospettiva è quella connessa al principio di accessibilità, che, pur essendo solo abbozzato nel Programma, riguarda la possibilità per le autorità di *law enforcement* nazionali o europee di acquisire informazioni rilevanti contenute nei *databases* centralizzati: sia da quelli istituiti per finalità di sicurezza, sia da quelli che hanno finalità mista oppure finalità diverse da quelle di applicazione della legge[20].

Ebbene, negli anni successivi all'adozione del Programma, il legislatore europeo si è mosso seguendo queste indicazioni e ha mostrato un certo dinamismo[21]. A differenza di quanto accaduto in altri ambiti della cooperazione in materia penale, il Consiglio ha approvato una messe significativa di strumenti normativi diretti a concretizzare il canone della libera circolazione delle informazioni. Sul finire del 2006 è stata approvata, dopo un lungo *iter*, la decisione quadro sul principio di disponibilità delle informazioni in "terzo pilastro" (2006/960/GAI); ed è giunto in porto il regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II). L'anno successivo, ha visto la luce la parallela decisione sul SIS II (2007/533/GAI). Ma un'accelerazione davvero significativa si è registrata nel corso del 2008. In un solo anno sono stati approvati: il regolamento (CE) n. 767/2008, concernente il sistema di informazione visti e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata e la decisione 2008/633/GAI, relativa all'accesso per la consultazione al VIS da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi la luce la decisione; la decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera e la contestuale decisione 2008/616/GAI, volta a stabilire le disposizioni amministrative e tecniche necessarie all'attuazione della decisione 2008/615/GAI, in particolare per quanto riguarda lo scambio automatizzato di dati sul DNA, dati dattiloscopici e dati di immatricolazione dei veicoli; la decisione quadro 2008/876/GAI sulla considerazione delle decisioni di condanna in occasione di un nuovo procedimento penale; infine, la tanto attesa decisione quadro 2008/977/GAI sulla

---

19 Così, D. Bigo, "EU Police Cooperation: National Sovereignity Framed by European Security", in *Security versus Justice?, Police and Judicial Cooperation in the European Union*, a cura di E. Guild e F. Geyer, Ashgate, Aldershot, 2008, p. 106.

20 Cfr. *infra*, M. Gialuz, "Principio di accessibilità e banche dati di 'primo pilastro'".

21 Diversa la valutazione di L. Salazar, "Presente e futuro nello spazio di libertà, sicurezza e giustizia: dal piano d'azione dell'Aia alla 'visione' della Commissione europea", in *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2008, p. 625, secondo il quale «scarsi passi avanti sono stati fatti sul terreno della '*libera circolazione delle informazioni di polizia*'».

protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. Infine, nel febbraio del 2009, dopo un lavoro preliminare durato più di tre anni, è stata adottata la decisione quadro 2009/315/GAI, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario e, a distanza di neanche due mesi, è stata approvata la decisione 2009/316/GAI che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS).

4. Il profilo statico della cooperazione informativa: principio di conservazione

Al fine di dare attuazione al principio di disponibilità in senso lato, accanto al profilo legato alla circolazione di informazioni già esistenti a livello nazionale o europeo (disponibilità in senso stretto e accessibilità), l'Unione europea è intervenuta anche sul profilo statico della cooperazione informativa, garantendo quello che potrebbe definirsi come canone di conservazione delle informazioni rilevanti per finalità di prevenzione e repressione della criminalità. Da questo punto di vista, l'attività normativa dell'Unione si è tradotta – a seconda dei casi – nell'introduzione di specifici obblighi di conservazione per gli Stati membri oppure si è configurata come diretta a garantire l'uniformità delle scelte già operate dagli Stati membri.

Tra le iniziative più significative va segnalata senz'altro la già citata decisione 2008/615/GAI. Nel recepire i contenuti del trattato di Prüm[22], essa non implementa soltanto il canone di disponibilità con riguardo ai dati genetici e biometrici, ma prescrive a monte che «gli Stati membri si impegnano a creare e a gestire schedari nazionali di analisi del DNA per le indagini penali» (art. 1)[23]. Altrettanto rilevante è la recentissima decisione quadro 2009/315/GAI, relativa all'organizzazione e al contenuto delle informazioni estratte dal casellario giudiziario, che prevede l'obbligo per lo Stato di cittadinanza del condannato di conservare integralmente le informazioni trasmesse dallo Stato di condanna (art. 5). Su tali fonti si tornerà ampiamente nel prosieguo[24], mentre merita fare un rapido cenno ad altri due filoni di intervento dell'Unione, che non verranno ulteriormente approfonditi nel volume.

---

22 Cfr. R. Bellanova, "The 'Prüm Process': The Way Forward for EU Police Cooperation and Data Exchange?", in *Security versus Justice?*, cit., p. 203; S. Kierkegaard, *The Prüm decision. An uncontrolled fishing expedition in 'Big Brother' Europe*, in "Computer Law & Security Report", 2008, p. 243.

23 In *GUUE*, L 210, 6 agosto 2008, p. 3.

24 Cfr. *infra*, S. Ciampi, *op. cit.*, § 8; A. Marandola, "*Information sharing* nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione"; nonché, M. Gialuz, "Il casellario giudiziario europeo: una frontiera dell'integrazione in materia penale", § 7.

Il primo riguarda la conservazione e la fruibilità dei dati relativi ai passeggeri dei voli aerei. Su questo versante, il primo strumento normativo adottato dall'Unione è stato la direttiva 2004/82/CE del Consiglio[25], con la quale si prevedeva che gli Stati membri dovessero prescrivere ai vettori aerei di comunicare le informazioni anticipate sui passeggeri (*Advance Passenger Information*, API), al fine di combattere efficacemente l'immigrazione clandestina e migliorare i controlli alle frontiere: si tratta, in particolare, dei dati relativi al numero e al tipo di documento di viaggio utilizzato, alla cittadinanza, al nome completo, alla data di nascita, al valico di frontiera di ingresso nel territorio degli Stati membri, al numero del trasporto, all'ora di partenza e di arrivo del mezzo di trasporto, al numero complessivo di passeggeri trasportati con tale mezzo, al primo punto di imbarco (art. 3, par. 2).

Non ci si è però fermati a tanto. Nel 2007, riprendendo un duplice invito del Consiglio europeo – il primo contenuto nella Dichiarazione sulla lotta al terrorismo adottata il 25 marzo 2004[26] e il secondo nel Programma dell'Aia (§ 2.2) –, la Commissione ha presentato una proposta di decisione quadro sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR) nelle attività di contrasto (COM (2007) 654 def.)[27]. Al fondo, vi è la consapevolezza, maturata in tutte le autorità di contrasto dopo l'11 settembre, del valore aggiunto rappresentato dalla raccolta e dall'analisi dei cosiddetti dati PNR nella lotta al terrorismo e alla criminalità organizzata. A tali fini, i dati API sono certamente utili ad identificare terroristi e criminali già noti, mediante l'impiego dei sistemi di segnalazione; i dati PNR, invece, non solo sono disponibili prima di quelli API, ma – contenendo informazioni relative a spostamenti dei passeggeri, ai numeri di telefono, all'agente di viaggio, nonché il numero di carta di credito, le variazioni del programma di viaggio, il posto a sedere preferito e altri particolari – rappresentano «uno strumento molto importante per effettuare valutazioni di rischio sui passeggeri, per ottenere informazioni e stabilire associazioni tra soggetti noti e non noti»[28]. La proposta ha come obiettivo esplicito quello di armonizzare le disposizioni degli Stati membri relative all'obbligo dei vettori aerei, che effettuano voli a destinazione

25 In *GUUE*, L 261, 6 agosto 2004, p. 24.

26 Cfr. *Documento del Consiglio n. 7906/04*, 29 marzo 2004, <http://register.consilium.europa.eu/pdf/it/04/st07/st07906.it04.pdf>, p. 9.

27 La proposta originaria è disponibile all'indirizzo <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:IT:PDF>.

28 Così, la *Relazione alla proposta di decisione quadro sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:IT:PDF>, p. 3. Per una definizione dei *passenger name record data*, cfr. D.R. Rasmussen, *Is International travel per se suspicion of terrorism? The dispute between the United States and European Union over passenger name record data transfers*, in "Wisconsin International Law Journal", 2008, p. 553.

del territorio di almeno uno Stato membro, o in provenienza dallo stesso, di trasmettere i dati PNR alle autorità competenti (art. 1).

Essa prevede l'istituzione a livello nazionale di un'unità di informazione sui passeggeri con il compito specifico di raccogliere i dati PNR presso le compagnie aeree e di trattarli per finalità specifiche, quali: l'identificazione di coloro che sono o potrebbero essere implicati in un reato di terrorismo o di criminalità organizzata, nonché i loro complici; la creazione e l'aggiornamento degli indicatori di rischio per la valutazione di questi soggetti; la fornitura di *intelligence* sui tipi di spostamenti e altre tendenze connessi ai reati di terrorismo e alla criminalità organizzata; l'utilizzo in procedimenti e indagini penali su reati di terrorismo e sulla criminalità organizzata (art. 3, par. 5). Inoltre, la proposta prescrive alle compagnie aeree di comunicare i dati PNR alle unità nazionali d'informazione (art. 5), utilizzando, in linea di principio, un sistema «*push*»[29]. Nella fase successiva, l'autorità di informazione filtra i dati e li trasmette esclusivamente alle autorità competenti, che «comprendono soltanto le autorità responsabili della prevenzione e della lotta contro i reati di terrorismo e la criminalità organizzata» (art. 4, par. 2).

Sulla proposta ha espresso un parere fortemente critico il Garante europeo per la protezione dei dati, il quale l'ha reputata non conforme ai diritti fondamentali, e, in particolare, all'art. 8 della Carta dei diritti fondamentali dell'Unione europea[30]. Tra i diversi rilievi mossi dal Garante merita richiamarne due.

Il primo concerne la stessa legittimità della proposta e va al cuore delle finalità del trattamento previsto dalla stessa: i dati PNR servono per compiere valutazioni di rischio dei passeggeri e a individuare soggetti che *potrebbero* essere implicati in un reato di terrorismo o di criminalità organizzata. Il Garante concentra l'attenzione sulle modalità di tale valutazione e si chiede se possa configurarsi come profilazione: pur consapevole delle incertezze definitorie relative a tale nozione[31], la preoccupazione è legata alla circostanza che «le decisioni relative

---

29 Si danno due diversi sistemi: il metodo "*pull*", secondo il quale le autorità competenti dello Stato che richiede i dati possono accedere al sistema di prenotazione del vettore aereo ed estrarre una copia dei dati richiesti; il metodo "*push*", invece, per cui i vettori aerei trasmettono i soli dati richiesti all'autorità richiedente. Si ritiene che questo secondo sistema offra «un livello più elevato di protezione dei dati» e per questo «dovrebbe essere obbligatorio per tutti i vettori aerei dell'Unione» (considerando n. 16).

30 Cfr. *Parere del garante europeo della protezione dei dati relativo al progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto*, in *GUUE*, C 110, 1° maggio 2008, p. 14.

31 In un recente studio sviluppato dal Consiglio d'Europa, la profilazione viene definita come un metodo informatico che, attraverso l'attività di *data mining* in un archivio di dati, consente o mira a consentire di classificare, con una certa probabilità, e, quindi, con un certo margine di errore, una persona in una determinata categoria, al fine di prendere decisioni individuali nei riguardi di tale persona (così, J.M. Dinant - C. Lazaro - Y. Poullet - N. Lefever - A. Rouvroy, *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion*

alle persone saranno prese sulla base di modelli e criteri stabiliti utilizzando i dati relativi all'insieme dei passeggeri»; insomma, «le decisioni riguardanti una singola persona potrebbero essere prese utilizzando come riferimento (almeno parzialmente) modelli derivati dai dati di altre persone»[32]. Peraltro, l'autorità rileva come i risultati relativi alle tecniche intese a valutare il rischio presentato dalle persone mediante strumenti di «data mining» e modelli comportamentali non siano ancora sufficientemente chiari e che occorra pertanto stabilirne chiaramente l'utilità nel quadro della lotta contro il terrorismo, prima di utilizzarle su una scala così vasta. Basarsi su diverse banche dati senza avere una visione globale dei risultati concreti e delle lacune, non solo è «contrario ad una politica legislativa razionale, che esige che non si adottino nuovi strumenti prima di aver pienamente attuato quelli esistenti e dimostrato la loro insufficienza», ma potrebbe «portare ad una società basata sulla sorveglianza totale»[33].

Il secondo profilo di particolare interesse concerne l'incertezza giuridica riguardo al regime di protezione dei dati applicabile ai diversi attori implicati nel progetto, in particolare alle compagnie aeree e ad altri attori riconducibili al "primo pilastro": in teoria potrebbero trovare applicazione le norme della proposta, quelle della decisione quadro 2008/977/GAI sulla protezione dei dati o la legislazione nazionale che attua la direttiva 95/46/CE. Si badi che il problema è ben più ampio: il Garante registra infatti la tendenza crescente del legislatore europeo di imporre in forma sistematica la cooperazione per finalità di contrasto ad attori del settore privato e sottolinea come questa cooperazione finisca per sollevare proprio «la questione del quadro di protezione dei dati (primo o terzo pilastro) che si applica alle condizioni di tale cooperazione: non è chiaro se le norme debbano basarsi sulla qualità del responsabile del trattamento (settore privato) o sulla finalità perseguita (attività di contrasto)»[34].

---

destinés au travail futur du Comité consultatif (T-PD), <http://www.coe.int/t/f/affaires__juridiques/coop%E9ration__juridique/protection__des__donn%E9es/documents/rapports%20et%20%E9tudes%20des%20experts/1CRID__Profilage__2008__fr.pdf>, p. 5). Su tale concetto, cfr. anche L. A. Bygrave, *Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, <http://www.austlii.edu.au/au/journals/PLPR/2000/40.html>; nonché, per una ricognizione analitica delle diverse tipologie di profilazione, M. Hildebrandt, "Defining Profiling: A New Type of Knowledge?", in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, a cura di M. Hildebrandt e S. Gutwirth, Springer, 2008, pp. 18 sgg.

32 Cfr. *Parere del garante europeo della protezione dei dati relativo al progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione*, cit., p. 4.

33 Ancora, *Parere del garante europeo della protezione dei dati relativo al progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione*, cit., p. 14. In termini analoghi, *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, <http://www.libertysecurity.org/IMG/pdf__FRA__opinion__PNR__en.pdf>, p. 13. Sull'esperienza americana, cfr. T. M. Ravich, *Is Airline Passenger Profiling Necessary?*, in "University of Miami Law Review", 2007, pp. 1 sgg.

34 Testualmente, *Parere del garante europeo della protezione dei dati relativo al progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione*, cit., p. 14. Peraltro, lo stesso Garante

Nonostante questi rilievi, il lavoro di elaborazione della decisione sta procedendo[35]. Peraltro, è risaputo che, parallelamente al percorso di adozione della decisione quadro, si è sviluppata una vicenda, ancor più travagliata, con riguardo agli accordi che l'Unione europea ha concluso con Paesi terzi ai fini della trasmissione dei dati stessi[36]. Com'è noto, un primo accordo, concluso con gli Stati Uniti nel maggio 2004, è stato sostituito – a seguito della sentenza con cui la Corte di giustizia aveva annullato la decisione del Consiglio 2204/496/CE e la decisione della Commissione 2004/496/CE[37] – da un nuovo accordo nel luglio 2007[38]. Accordi analoghi sono stati conclusi con il Canada nel 2006 e con l'Australia nel 2008[39].

5. (Segue): la direttiva sulla *data retention*

Oltre a quello relativo alle informazioni sui viaggiatori aerei, vi è un altro ambito nel quale le istituzioni europee sono intervenute al fine di dare attuazione a quello che si è definito canone di conservazione delle informazioni utili all'attività di

---

aveva già sottolineato il rischio che lo sviluppo di attività trattamentali di soggetti privati per finalità (sia pure indirettamente) legate all'applicazione della legge possa determinare un vuoto giuridico per la difficoltà di inquadramento nel primo o nel terzo pilastro (cfr. *Parere del garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati*, in *GUUE*, C 255, 27 ottobre 2007, pp. 2, 7).

35 L'ultima versione è contenuta nel *Documento del Consiglio n. 5618/09*, 23 gennaio 2009, <http://register.consilium.europa.eu/pdf/it/09/st05/st05618.it09.pdf>.

36 Sul punto, cfr. D.R. Rasmussen, *op. cit.*, pp. 573 sgg.

37 Si allude a Corte giust., 30 maggio 2006, cause riunite C-317/04 e C-318/04, *Parlamento europeo contro Consiglio e Commissione*, in "Diritto dell'informazione e dell'informatica", 2006, pp. 761, con nota di D. Maffei, *«Legislazione dell'emergenza» e tutela dei dati personali dei passeggeri: il conflitto Europa-Usa*. Su tale vicenda, per tutti, A. Adam, *L'échange de données à caractère personnel entre l'Union européenne et les Etats-Unis*, in "Revue trimestrielle de droit européen", 2006, n. 3, pp. 420 sgg. Cfr. anche E. Guild – E. Brouwer, *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, <http://shop.ceps.eu/BookDetail.php?item__id=1363>.V. Michel, *La dimension externe de la protection des donées à caractère personnel: acquiescement, perplexité et frustration*, in "Revue trimestrielle de droit européen", 2006, pp. 549 sgg.

38 In *GUUE*, L 204, 4 agosto 2007, p. 18. La firma dell'accordo è stata autorizzata con la decisione 2007/551/PESC/GAI (in *GUUE*, L 204, 4 agosto 2007, p. 16). Su tale complessa vicenda, si leggano, anche per ulteriori indicazioni bibliografiche, E. Guild, "Inquiry into the EU–US Passenger Name Record Agreement", CEPS Policy Brief No. 125, <http://shop.ceps.eu/BookDetail.php?item__id=1481>; M. McGinley – R. Parkes, *Data Protection in the EU's Internal Security Cooperation. Fundamental Rights vs. Effective Cooperation?*, SWP Research Paper No. 5, Berlino, 2007, <http://www.swp-berlin.org/en/common/get__document.php?asset__id=4034> pp. 19 sgg.

39 Rispettivamente, in *GUUE*, L 82, 21 marzo 2006, p. 15, e in *GUUE*, L 213, 8 agosto 2008, p. 49. Al riguardo, cfr. P. Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, in CEPS Special Report/September 2008, <http://shop.ceps.eu/BookDetail.php?item__id=1704>.

law enforcement: si tratta della materia relativa ai dati generati dalle comunicazioni elettroniche.

Come noto, l'utilizzo di servizi o reti di comunicazione elettronica – sia ai fini delle conversazioni telefoniche, sia per l'accesso a Internet – genera diverse tipologie di dati: da un canto, i dati relativi al traffico, che includono ad esempio informazioni relative al numero del chiamante e del chiamato, alla data, all'ora e alla durata della chiamata; dall'altro, i dati relativi all'ubicazione delle apparecchiature di comunicazione mobile. Questi dati, combinati con quelli che consentono l'identificazione dell'abbonato o dell'utente del servizio, sono evidentemente assai utili ai fini dell'attività di prevenzione e repressione dei reati. Tanto che il Consiglio ha più volte riconosciuto l'importanza dell'impiego di tali dati per la lotta contro il terrorismo e la criminalità organizzata[40]: ancora una volta, è nella fondamentale Dichiarazione sulla lotta al terrorismo, adottata il 25 marzo 2004, che lo stesso Consiglio europeo ha incaricato il Consiglio di presentare «proposte relative all'istituzione di norme sulla conservazione dei dati relativi al traffico delle comunicazioni da parte dei prestatori di servizi»[41].

Questo invito è stato accolto immediatamente da cinque Stati membri (Repubblica francese, Irlanda, Regno di Svezia, Regno Unito e Irlanda del Nord), che, nell'aprile del 2004, hanno presentato un'iniziativa finalizzata all'adozione di una decisione quadro fondata sugli artt. 31, n. 1, lett. c), TUE e 34, n. 2, lett. b), TUE[42]. La proposta mirava ad agevolare la cooperazione di polizia e giudiziaria in materia penale: al fondo vi era, infatti, la convinzione che un'effettiva cooperazione informativa presuppone «che tutti gli Stati membri provvedano a conservare taluni tipi di dati per un certo periodo di tempo, secondo precisi parametri, a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo»; dati che «dovrebbero essere messi a disposizione degli altri Stati membri conformemente agli strumenti di cooperazione giudiziaria in materia penale adottati a norma del titolo VI del trattato sull'Unione europea» (considerando n. 9)[43]. Inoltre, come si evince dalla nota esplicativa alla proposta,

---

40 Cfr., in particolare, le *Conclusioni sulle tecnologie dell'informazione e indagini e azioni penali relative alla criminalità organizzata*, adottate nel Consiglio «Giustizia e affari interni» del 19 dicembre 2002, nelle quali si riconosce che «a motivo dell'importante aumento delle possibilità offerte dalle comunicazioni elettroniche, i dati relativi all'uso di queste ultime costituiscono attualmente uno strumento particolarmente importante ed utile nelle indagini e nelle azioni penali contro la criminalità e in particolare quella organizzata» (cfr. *Documento del Consiglio n. 15691/02*, 19 dicembre 2002, p. IV).

41 Così, *Documento del Consiglio n. 7906/04*, cit., p. 5.

42 Cfr. *Documento del Consiglio n. 8958/04*, 20 dicembre 2004, <http://register.consilium.europa.eu/pdf/it/04/st08/st08958.it04.pdf>.

43 Si è voluto riportare questo passaggio perché emerge in modo lampante il rapporto strumentale tra canone di conservazione delle informazioni utili ai fini dell'attività di *law enforcement* e quella che si è definita disponibilità in senso lato.

essa intendeva fronteggiare due pericoli: da una parte, il rischio che la notevole divergenza tra le normative nazionali sulla durata dei periodi di conservazione potesse condurre a creare dei «'paradisi dei dati' all'interno dell'Unione europea»; dall'altra parte, il rischio che le evoluzioni tecnologiche e le pressioni commerciali per ridurre i costi portassero i fornitori di servizi a diminuire il periodo di memorizzazione dei dati sulle comunicazioni o addirittura a escludere alla radice la conservazione (come nel caso delle carte prepagate per le comunicazioni mobili o degli abbonamenti forfettari, nei quali i dati del traffico non sono necessari per la fatturazione)[44].

La proposta di decisione – che prescriveva agli Stati membri di conservare i dati per un «periodo non inferiore a 12 mesi e non superiore a 36 mesi a decorrere dalla loro generazione» e consentiva loro di «prevedere tempi di conservazione dei dati più lunghi in funzione dei criteri nazionali, purché tale conservazione costituisca una misura necessaria, adeguata e proporzionata nell'ambito di una società democratica» (art. 4) – è stata criticata dal Parlamento europeo, per la scelta della base giuridica. Questa, infatti, è stata ritenuta incompatibile con la legislazione europea: se, per un verso, la proposta prevedeva misure relative all'accesso e allo scambio dei dati immagazzinati dagli Stati membri e insisteva nell'ambito del "terzo pilastro", per altro verso, nella parte in cui prescriveva la conservazione dei dati a cura del *service provider*, indicava una definizione degli stessi e definiva la durata della loro conservazione, non poteva che incidere su una materia ricadente nell'ambito comunitario. Una materia, peraltro, già disciplinata da una fonte comunitaria, quale la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)[45]. Per modificare il regime stabilito dagli artt. 6, 9 e 15 di tale direttiva non si sarebbe potuti intervenire con uno strumento di "terzo pilastro", pena la violazione dell'art. 47 TUE[46].

È così che la Commissione, a breve distanza dal nuovo invito contenuto nella dichiarazione adottata dal Consiglio straordinario informale del 13 luglio 2005 (a seguito degli attentati di Londra), ha adottato una proposta di direttiva del

---

44 Così, la *Nota esplicativa alla decisione quadro sulla conservazione dei dati relativi alle comunicazioni*, in *Documento del Consiglio n. 8958/04*, cit., p. 3.

45 In *GUUE*, L 201, 31 luglio 2002, p. 37.

46 V. *Draft Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored inconnection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 – C6-0198/2004 – 2004/0813(CNS))*, <http://www.statewatch.org/news/2005/may/ep-data-ret-alvaro-report.pdf>, pp. 6-7; nonché, il *Parere della Commissione giuridica sulla base giuridica*, <http://www.privacy.it/cecA52005-174.html>.

Parlamento europeo e del Consiglio, riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58 (COM (2005) 438 def.), fondata sull'art. 95 CE[47]. La finalità della proposta è stata ricalibrata alla luce della nuova base giuridica: pur riprendendo le considerazioni relative all'utilità della conservazione dei dati esterni delle comunicazioni e all'opportunità di minimizzare il rischio di una progressiva riduzione dei tempi di conservazione – legata al venir meno delle esigenze di fatturazione –, la Commissione ha insistito soprattutto sull'esigenza di armonizzazione delle legislazioni nazionali. Ciò, sulla base dell'assunto che «l'esistenza di differenze sul piano delle disposizioni legislative, regolamentari e tecniche negli Stati membri relativamente alla conservazione dei dati sul traffico costituisce un ostacolo per il mercato interno delle comunicazioni elettroniche, poiché i fornitori di servizi devono rispettare esigenze diverse per quanto riguarda i tipi di dati da conservare e le condizioni di tale conservazione»[48].

Quanto al contenuto, la proposta di direttiva prevedeva la conservazione dei dati esterni delle comunicazioni «a fini di prevenzione, ricerca, accertamento e perseguimento di reati gravi, come il terrorismo e la criminalità organizzata» (art. 1), per un periodo pari a un anno o di sei mesi per i dati relativi a comunicazioni elettroniche che hanno luogo usando interamente o principalmente il protocollo Internet; essa evitava invece di soffermarsi sui profili legati all'accesso e al trasferimento di tali dati alle autorità competenti, per il timore di sconfinare nell'ambito del "terzo pilastro".

Se il Comitato economico e sociale europeo ha espresso una critica radicale al progetto[49], il parere del Garante europeo è stato più equilibrato. Sotto il profilo della necessità della conservazione dei dati relativi al traffico e all'ubicazione per finalità di *law enforcement*, il Garante, pur dando atto che erano state presentate delle analisi – in particolare uno studio effettuato dalla polizia del Regno Unito – dalle quali emergeva che in pratica i dati relativi al traffico richiesti dalle forze dell'ordine risalgono nell'85 per cento dei casi ai sei mesi precedenti e ai fini di

---

47 La proposta è disponibile all'indirizzo <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:IT:PDF>.

48 Così, la *Relazione alla proposta di direttiva del Parlamento europeo e del Consiglio, riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58 (COM(2005) 438 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:IT:PDF>, p. 2.

49 Il riferimento è al *Parere del Comitato economico e sociale europeo in merito alla Proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE*, in *GUUE*, C 69, 21 marzo 2006, p. 16, ove si legge: «La presentazione di una proposta normativa di questo genere, dal contenuto esagerato e che incide sui diritti fondamentali, suscita nel Comitato stupore e preoccupazione. L'approccio della proposta nei confronti dei diritti umani, e in modo particolare del diritto alla privacy è del tutto inadeguato e può creare, in determinati aspetti, dei conflitti».

indagine dei reati più gravi al massimo a un anno, ha espresso qualche perplessità[50]. Con riguardo alla base giuridica, pur condividendo la scelta per la procedura più garantita della codecisione, il Garante ha segnalato la tendenziale inscindibilità delle norme sull'accesso ai dati e sull'uso e lo scambio degli stessi rispetto all'obbligo di conservazione dei dati: a detta del Garante, pertanto, sarebbe stato opportuno affrontare anche il profilo dei limiti all'accesso e all'utilizzazione dei dati[51]. Infine, con riferimento alle singole disposizioni, ha raccomandato di precisare che i dati possono essere forniti solo se necessario in relazione a un reato individuato tra categorie specifiche di reati gravi e che i periodi di conservazione di sei mesi e un anno vanno intesi come periodi massimi di conservazione; inoltre, ha suggerito di specificare che, al termine del periodo, i dati debbono essere cancellati dal fornitore mediante procedimenti automatizzati, almeno su base giornaliera[52].

Il legislatore europeo ha approvato la proposta in tempi davvero brevi. Già nel dicembre 2005, il Parlamento europeo si è espresso in termini favorevoli[53]; mentre il Consiglio ha adottato definitivamente la direttiva 2006/24/CE durante la sessione del 21 febbraio 2006, con voto a maggioranza qualificata (hanno votato contro l'Irlanda e la Repubblica slovacca)[54].

Le citate raccomandazioni del Garante – a differenza di quelle relative alla sicurezza dei dati – non sono state recepite. Anzitutto, non solo non sono stati specificati i reati per i quali è possibile un utilizzo dei dati conservati, ma si fa generico riferimento alla finalità di garantirne «la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale» (art. 1). Anche con riguardo al profilo legato all'individuazione delle autorità competenti alle quali trasmet-

---

50 In tal senso, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della direttiva 2002/58/CE [COM(2005) 438 def.]*, in *GUUE*, C 298, 29 novembre 2005, p. 3.

51 Cfr. *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio*, cit., p. 6.

52 Ancora, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio*, cit., p. 11. In termini non dissimili si è espresso il Gruppo Articolo 29 nell'*Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)*, 21 ottobre 2005, <http://www.statewatch.org/news/2005/nov/WP113.pdf>, p. 8, ove si aggiungeva che «access to data should, in principle, be duly authorised on a case by case basis by a judicial authority without prejudice to countries where a specific possibility of access is authorised by law, subject to independent oversight».

53 Con 378 voti a favore, 197 contrari e 30 astenuti. A favore hanno votato i due gruppi più grandi, del PSE e del PPE, mentre il gruppo dei Greens/EFA e il gruppo GUE/NGL hanno votato contro; il gruppo dell'ALDE si è diviso con 25 parlamentari favorevoli e 37 contrari.

54 In *GUUE*, L 105, 13 aprile 2006, p. 54.

tere i dati e alle procedure da seguire, la direttiva si limita a rinviare alle legislazioni nazionali (art. 4). Per quanto concerne poi il periodo di conservazione, esso è stato raddoppiato, dal momento che i singoli Paesi possono stabilirlo in un arco compreso tra i sei mesi e i due anni (art. 6). Si prevede, inoltre, una valvola di sfogo per quei Paesi che si trovino «ad affrontare circostanze particolari che giustificano una proroga, per un periodo limitato, del periodo massimo di conservazione di cui all'articolo 6» (art. 12). Tale clausola è stata pensata probabilmente per far fronte a circostanze peculiari, quale potrebbe essere un attentato terroristico: la dottrina tende a escludere che possa essere invocata – ad esempio dall'Italia – per giustificare la conservazione prolungata dei dati per finalità di repressione della criminalità organizzata di tipo mafioso, dal momento che questa ha carattere tutt'altro che contingente e transeunte[55]. In realtà, il tenore della disposizione potrebbe forse lasciare qualche spazio per una lettura alternativa: si potrebbe infatti sostenere che ciò che importa è che la deroga al tetto dei due anni abbia durata limitata, per dar modo alla Commissione di valutare la persistenza della situazione di eccezionalità che la giustifica (art. 12, par. 2).

Al di là di tali problemi esegetici, merita porre in rilievo che quella che è stata definita come una decisione storica, in quanto ha introdotto per la prima volta «the Europe-wide obligation to retain, for investigational purposes, billions of data relating to the communications of any and all citizens»[56], ha suscitato numerose reazioni negative, a partire da quella del Garante europeo[57].

Oltre alle svariate prese di posizione di organizzazioni di tutela dei diritti[58], merita segnalare che, nel luglio 2006, l'Irlanda ha presentato ricorso di annullamento della direttiva 2006/24/CE, ai sensi dell'art. 230 TCE: contestava, infatti, la scelta di adottare uno strumento di "primo pilastro" fondato sull'art. 95 TCE. Secondo l'Irlanda, si tratterebbe di una normativa finalizzata unicamente o principalmente ad agevolare l'indagine, l'accertamento e il perseguimento di reati, che avrebbe dovuto essere fondata sul titolo VI del Trattato UE.

---

55 Così, S. Aterno, *Conservazione dei dati informatici e prospettive europee*, citato da C. Conti, "L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova", in *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Padova, Cedam, 2008, p. 16.

56 Così, il Gruppo Articolo 29, nell'*Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data*, cit., p. 4.

57 Cfr. A.L. Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy*, New York, Cornell University Press, 2008, p. 131; nonché, E. Kosta – P. Valcke, *Retaining the data retention directive*, in "Computer Law & Security Report", 2006, pp. 370 sgg.; ritiene invece adeguatamente salvaguardata la privacy, F. Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, in "Chicago Journal of International Law", 2007, pp. 249 sgg.

58 Cfr., al riguardo, la rassegna di documenti curata da Statewatch (intitolata *The surveillance of telecommunications in the EU*) e disponibile all'indirizzo <http://www.statewatch.org/eu-data-retention.htm>.

Recentemente, la Corte del Lussemburgo ha rigettato il ricorso, confermando la correttezza del fondamento giuridico prescelto dal legislatore europeo[59]. Per quel che riguarda il profilo teleologico, ha rilevato che effettivamente la direttiva è volta a ridurre quelle divergenze tra le varie normative nazionali, che potevano avere un'incidenza diretta sul funzionamento del mercato interno (§ 71 e 72); con riguardo al contenuto, invece, ha precisato che la direttiva disciplina «operazioni che sono indipendenti dall'attuazione di qualsiasi eventuale azione di cooperazione di polizia e giudiziaria in materia penale», dal momento che «non armonizza né la questione dell'accesso ai dati da parte delle autorità nazionali competenti in materia di repressione, né quella relativa al ricorso ai medesimi ed al loro scambio fra le autorità in parola» (§ 83)[60].

La direttiva rimane pertanto vincolante e gli Stati membri dovranno completarne il recepimento a livello nazionale, che sta avvenendo tra molte resistenze[61].

---

59 Il riferimento è a Corte giust., 10 febbraio 2009, C-301/06, *Irlanda c. Parlamento europeo e Consiglio dell'Unione europea*, <http://curia.europa.eu/it/content/juris/index.htm>.

60 È interessante notare il passaggio della sentenza nel quale la Corte esclude che le argomentazioni poste a fondamento della sentenza C-317/04 relativa all'accordo sul trasferimento dei dati PNR possano essere estese alla direttiva sulla *data retention*: in un caso, infatti, la decisione 2004/535 aveva a oggetto un trattamento di dati non necessario alla realizzazione di una prestazione di servizi da parte dei vettori aerei, ma indispensabile unicamente per salvaguardare la sicurezza pubblica e a fini repressivi; nel caso della direttiva 2006/24/CE, invece, la normativa riguarda «le attività dei fornitori di servizi nel mercato interno e non comporta alcuna regolamentazione delle attività dei pubblici poteri a fini repressivi» (§ 91).

61 V. C. Fatta, *Tutela della privacy alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, in "Diritto dell'informazione e dell'informatica", 2008, pp. 408 sgg. Va rilevato che, ad esempio, in Germania la legge che ha dato attuazione alla direttiva 2006/24/CE è stata impugnata davanti alla Corte costituzionale e l'impugnativa è stata appoggiata da 30.000 ricorrenti (cfr. L. Pimedinis – E. Kosta, *The impact of the retention of traffic and location data on the internet user*, in "Datenschutz und Datensicherheit", 2008, p. 93); lo stesso è accaduto in Ungheria (cfr. <http://www.statewatch.org/news/2008/may/hungary-data-ret-hclu.pdf>). Cfr., inoltre, per quel che riguarda il contesto francese, S. Barrache – A. Olivier, "L'administration de la preuve pénale et les nouvelles technologies de l'information et de la communication", in *La preuve pénale. Internationalisation et nouvelles technologies*, a cura di O. de Frouville, Parigi, La Documentation française", 2007, pp. 160 sgg.; K. Retzer – K.J. Vanto, *Data Retention: Denmark Is First EU Member State to Implement Controversial Directive*, in "Privacy and Security Law Report", 2007, <http://www.mofo.com/news/updates/bulletins/12271.html>. Per quel che concerne l'ordinamento italiano, cfr. D. Cerqua, "Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche", in *Sistema penale e criminalità informatica*, a cura di L. Lupária, Milano, Giuffrè, 2009, pp. 221 sgg.; C. Conti, *op. cit.*, pp. 14 sgg.; L. Di Paola, "Commento all'art. 132", in *La protezione dei dati personali*, II, a cura di C. M. Bianca e F. D. Busnelli, Padova, Cedam, 2007, p. 1588; L. Lupária, "La disciplina processuale e le garanzie difensive", in L. Lupária - G. Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, Giuffrè, 2007, pp. 179 sgg.; A. Piraino, "Privacy e comunicazioni elettroniche", in *Libera circolazione e protezione dei dati personali*, II, a cura di R. Panetta, Milano, Giuffrè, 2006, p. 1576; nonché, con specifico riferimento al d.lgs. 30 maggio 2008, n. 109, che ha dato attuazione alla direttiva 2006/24/CE, si leggano S. Aterno – A. Cisterna, *Il legislatore interviene ancora sul* data retention*, ma non è finita*, in "Diritto penale e processo", 2009, pp. 282 sgg.; A. Cisterna, *Acquisizioni probatorie ridotte a prescindere dal delitto ipotizzato*, in "Guida al diritto", 2008, n. 39, p. 40.

L'auspicio è che le lacune della direttiva relative alla tutela del diritto alla protezione dei dati possano essere colmate dai legislatori degli Stati membri, come raccomandato sin dall'origine dall'*Article 29 Data Protection Working Party*[62].

62 Cfr. *Opinion 3/2006 on the Directive 2006/XX/EC of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, as adopted by the Council on 21 February 2006*, 25 marzo 2006, <http://www.statewatch.org/news/2006/apr/wp119.pdf>, pp. 2-3.

Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea

STEFANO CIAMPI
Dottore di ricerca in Scienze penalistiche
Università di Trieste

Sommario: 1. Introduzione. – 2. Il Programma dell'Aia. – 3. Dal Programma all'azione. La proposta di decisione quadro della Commissione in materia di protezione dei dati personali (COM (2005) 475 def.). – 4. La proposta di decisione quadro della Commissione sullo scambio d'informazioni in virtù del principio di disponibilità (COM (2005) 490 def.). – 5. La decisione quadro in materia di protezione dei dati personali (2008/977/GAI): la tortuosità dell'itinerario di adozione e il progressivo depauperamento contenutistico. – 6. Il percorso di avvicinamento alla "disponibilità informativa". – 7. L'iniziativa del Regno di Svezia: gli albori del principio di disponibilità. – 8. Il Trattato di Prüm e il suo recepimento nel tessuto connettivo dell'Unione europea (decisione 2008/615/GAI). – 9. La decisione quadro sul principio di disponibilità delle informazioni in "terzo pilastro" (2006/960/GAI). – 10. Riflessioni conclusive.

1. Introduzione

La cooperazione tra le forze di polizia e la cooperazione tra autorità giudiziarie rappresentano, a mente dell'art. 29, par. 2, TUE, gli strumenti-principe[1] a mezzo dei quali perseguire un elevato livello di sicurezza, nello «spazio di libertà sicurezza e giustizia» *ex professo* teorizzato dagli artt. 2, par. 1, 4° capoverso, e 29, par. 1, TUE[2].

---

1 Li affianca il ravvicinamento delle normative degli Stati membri, contemplato dall'ultimo capoverso dell'art. 29 TUE.

2 Per uno spaccato delle molteplici ed eterogenee misure adottate, prima, in seno alle Comunità europee e, poi, dall'Unione europea nella prospettiva della creazione e del progressivo rafforzamento di uno spazio di libertà, sicurezza e giustizia, cfr., *ex plurimis*, E. Aprile, *Diritto processuale penale europeo e internazionale*, Padova, Cedam, 2007, pp. 19 sgg.; A. Bernardi, *Strategie per l'armonizzazione dei sistemi penali europei*, in "Rivista trimestrale di diritto penale dell'economia", 2002, p. 787; P. Bilancia, *Lo Spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria*, in "Rivista italiana di diritto pubblico comunitario", 2004, p. 345; M. Chiavario, *Cooperazione giudiziaria e di polizia in materia penale a livello europeo*, in "Rivista italiana di diritto e procedura penale", 2005, p. 974; Corpus Juris. *Pubblico ministero europeo e cooperazione internazionale* (Atti del Convegno di Alessandria, 19-21 ottobre 2001), a cura di M. Bargis-S. Nosengo, Milano, Giuffrè, 2003, *passim*; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale. Verso un sistema integrato di forme e strumenti di collaborazione tra le autorità giudiziarie*, Milano, Giuffrè, 2007, pp. 27 sgg.; P. de Hert-L. Vandamme, *European Police and Judicial Information-sharing Cooperation: Incorporation into the Community, Bypassing and Extension of Schengen*, in "ERA Forum", 2004, n. 3, p. 425; *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (Atti del Convegno di Catania, 9-11 giugno 2005), a cura di T. Rafaraci, Milano, Giuffrè, 2007, *passim*; A. Laudati, *I delitti transnazionali. Nuovi modelli di incriminazione e di procedimento all'interno dell'Unione europea*, in "Diritto penale e processo", 2006, p. 401; A. Liberatore, *Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union*, in "European Journal on Criminal Policy and Research", 2001, n. 13, p. 109; J. Lodge, *Sustaining freedom, security and justice – from terrorism to immigration*, in "Liverpool Law Review", 2002, n. 24, p. 41; B. Nascimbene, *Cooperazione giudiziaria penale: diritto vigente e orientamenti futuri nel quadro della Costituzione europea*, in "Diritto penale e processo", 2004, p. 1295; B. Piattoli, *Cooperazione giudiziaria e pubblico ministero europeo*, Milano, Giuffrè, 2002, *passim*; R. Plender, *EU Immigration and Asylum Policy – The Hague Programme and the way forward*, in "ERA Forum", 2008, n. 9, p. 301; E. Rosi, "Il reato transnazionale", in *Criminalità organizzata transnazionale e sistema penale italiano. La Convenzione ONU di Palermo*, a cura della stessa A., Milano, Ipsoa, 2007, pp. 94 sgg.; L. Salazar, *La lotta alla criminalità nell'Unione: passi avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il programma dell'Aia*, in "Cassazione penale", 2004, p. 3510; Id., *L'Unione europea e la lotta alla criminalità organizzata da Maastricht ad Amsterdam*, in "Documenti giustizia", 1999, c. 391; E. Selvaggi, "Le nuove forme della cooperazione: un ponte verso il futuro", in *Rogatorie penali e cooperazione giudiziaria internazionale*, a cura di G. La Greca e M.R. Marchetti, Torino, Giappichelli, 2003, p. 465; P. Tonini, "Il progetto di un pubblico ministero europeo nel *Corpus Juris*", in *La giustizia penale italiana nella prospettiva internazionale* (Atti del Convegno di Courmayeur, 8-10 ottobre 1999), Milano, Giuffrè, 2000, p. 109; Id., *Processo penale e norme internazionali: la Consulta delinea il quadro d'insieme*, in "Diritto penale e processo", 2008, p. 417; J.A.E. Vervaele, *L'europeizzazione del diritto penale e la dimensione penale dell'integrazione europea*, trad. it. di R. D'Antoni, in "Rivista trimestrale di diritto penale dell'economia", 2005, p. 129.

Prima di calarsi *in medias res*, converrà ricordare che il fine di armonizzare le norme del TCE e del TUE a mezzo di un nuovo atto normativo primario – anzitutto allo scopo di adeguarle alle esigenze mutate di un'Unione "a ventisette" – è stato, *in primis*, perseguito tramite l'ormai eclissata Costituzione europea[3] e, successivamente, dal Trattato di Lisbona, sottoscritto dai rappresentanti degli Stati membri il 13 dicembre 2007. In ambedue i trattati di riforma, sfumano i confini che, attualmente, separano le principali aree d'intervento dell'Unione e che giustificano l'iconografia dei "tre pilastri"[4]. Questo futuribile profondo riassetto potrebbe far dubitare dell'opportunità di impostare l'analisi secondo le coordinate dall'ordito normativo attualmente vigente e, in particolare, del Titolo VI TUE. Sennonché, è agevole notare come, anche in prospettiva *de iure condendo*, la materia della *law enforcement cooperation* non perda affatto la propria autonomia topografica e funzionale; viene piuttosto ridisciplinata in seno ad un nuovo titolo («Spazio di libertà, sicurezza e giustizia»), compendiante cinque Capi: nel Trattato di Lisbona si distinguono «Disposizioni generali», «Politiche relative ai controlli alle frontiere, all'asilo e all'immigrazione», «Cooperazione giudiziaria in materia civile», «Cooperazione giudiziaria in materia penale», «Cooperazione di polizia». Nulla sembra, dunque, ostare a un'indagine che, *ratione materiae*, continui a fare riferimento al "terzo pilastro" dell'Unione europea, anche perché, dopo il naufragio del Trattato che adotta una Costituzione per l'Europa e alla luce dell'esito referendario irlandese del 13 giugno 2008, non vi è alcuna possibilità che lo stesso Trattato di Lisbona entri in vigore secondo gli auspici, *id est* prima del giugno 2009, data del rinnovo del Parlamento europeo.

Tornando al tema, preme richiamare l'attenzione sul fatto che il Trattato sull'Unione europea mostra di concepire lo strumento cooperativo in due modi

---

3 Con particolare riguardo al tema del coordinamento e della cooperazione tra le autorità di *law enforcement* nel perimetro del Trattato che adotta una Costituzione per l'Europa, vedansi M. Bargis, *Costituzione per l'Europa e cooperazione giudiziaria in materia penale*, in "Rivista italiana di diritto e procedura penale", 2005, p. 144; G. De Amicis-G. Iuzzolino, *Lo spazio comune di libertà, sicurezza e giustizia nelle disposizioni penali del Trattato che istituisce una Costituzione per l'Europa*, in "Cassazione penale", 2004, p. 3067; B. Nascimbene, *Cooperazione giudiziaria penale*, cit., p. 1295; Id., "Lo spazio di libertà, sicurezza e giustizia in una prospettiva costituzionale europea", in *Il Progetto di Trattato-Costituzione. Verso una nuova architettura dell'Unione europea*, a cura di L.S. Rossi, Milano, Giuffrè, 2004, pp. 273 sgg.; C. Ponti, "La cooperazione giudiziaria in materia penale e di polizia", in *Il trattato che adotta una Costituzione per l'Europa: quali limitazioni all'esercizio dei poteri sovrani degli Stati?*, a cura di G. Adinolfi-A. Lang, Milano, Giuffrè, 2006, p. 285; *Profili del processo penale nella Costituzione europea*, a cura di M.G. Coppetta, Torino, Giappichelli, 2005, *passim* (in partic. pp. 149 sgg.); L. Salazar, *La lotta alla criminalità nell'Unione*, cit., p. 3529.

4 Segnatamente, quanto alla cooperazione di polizia e giudiziaria in materia penale, la modifica di maggiore impatto consiste nella soppressione del titolo ad essa riservato in seno al TUE (Titolo VI) e nella riscrittura del Titolo IV TCE, dedicato a «visto, asilo, immigrazione ed altre politiche connesse con la libera circolazione delle persone».

diversi. Il primo si basa su un rapporto diretto tra le singole autorità di *law enforcement* nazionali e delinea una forma di cooperazione che potrebbe definirsi "immediata": in questo senso depone l'art. 29, par. 2, TUE, quando *expressis verbis* contempla «una più stretta cooperazione fra le forze di polizia, le autorità doganali e le altre autorità competenti degli Stati membri», nonché «una più stretta cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri». Il secondo fa perno su organismi propriamente europei, deputati a fungere – con varietà di poteri e missioni – da *trait d'union* fra le autorità giudiziarie o di polizia degli Stati membri: i rinvii testuali all'opera di Europol sul versante di polizia e ad Eurojust su quello giudiziario, contenuti nell'art. 29, par. 2, TUE, configurano una forma di cooperazione che chiameremo "mediata".

Nonostante tali differenze organizzative e strutturali, le due ipotesi risultano accomunate dal fatto che i capisaldi della cooperazione transfrontaliera sono rappresentati, in entrambe le fattispecie, dalla condivisione e dallo scambio di informazioni; caratteristica, questa, che configura le "politiche" europee in esame quale *species* di un *genus* molto più vasto, comprensivo di rapporti internazionali che fanno perno sull'*information sharing* e che coinvolgono anche numerosi Stati estranei all'Unione europea. Basterà ricordare Interpol[5], la Convenzione ONU contro il crimine organizzato transnazionale (c.d. Convezione di Palermo, del 15 novembre 2000), insieme ai tre Protocolli allegati[6], nonché la Convenzione del Consiglio d'Europa sulla criminalità informatica (c.d. Convenzione di Budapest, del 23 novembre 2001)[7].

Il denominatore comune a queste forme di cooperazione è rappresentato, dunque, dalla condivisione di *law enforcement informations*, ciò che inevitabilmente

---

5 Scaturita, non da uno strumento pattizio sottoscritto e ratificato da più Paesi, bensì da un accordo raggiunto, nel 1923, tra le autorità di polizia. Per una sintesi, v. A. Manganelli-F. Gabrielli, *Investigare. Manuale pratico delle tecniche di indagine*, Padova, Cedam, 2007, pp. 314 sgg.; F. Storelli, *Diritto penale comunitario. Profili sostanziali, processuali, collaborazione investigativa e giudiziaria*, Torino, Itaedizioni, 2006², p. 137. Per un quadro sinottico delle materie trattate e delle attività svolte da Interpol, da cui si evince la preminenza della politica di *information sharing*, si rinvia allo schema elaborato da A. Manganelli-F. Gabrielli, *op. cit.*, pp. 331 sgg.

6 Sulla Convenzione, ratificata dall'Italia con legge 16 marzo 2006, n. 146, e sui Protocolli, rispettivamente dedicati alla lotta contro la tratta delle persone, il traffico di migranti e quello di armi da fuoco, v., per tutti, *Criminalità organizzata transnazionale*, cit., *passim*; G. De Amicis, *op. cit.*, pp. 255 sgg.

7 La Convenzione è stata ratificata dall'Italia con legge 18 marzo 2008, n. 48. In tema, cfr. L. Lupária, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in "Diritto penale e processo", 2008, p. 717; A. Novellino, *Il Viminale può chiedere di conservare i dati*, in "Guida al diritto", 2008, n. 16, p. 69; C. Sarzana di S. Ippolito, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in "Diritto penale e processo", 2008, p. 1562; E. Selvaggi, *Cooperazione giudiziaria veloce ed efficace*, in "Guida al diritto", 2008, n. 16, p. 72; Id., *Task force operativa 24 ore al giorno*, *ivi*, 2008, n. 16, p. 74; *Sistema penale e criminalità informatica*, a cura di L. Lupária, Milano, Giuffrè, 2009.

anima la delicata questione afferente alla tutela dei dati trattati, la quale si presta ad essere analizzata seguendo due distinti scorci prospettici[8].

In primo luogo, l'attenzione si sofferma sugli interessi, di matrice prettamente individualistica, facenti capo alla persona cui le informazioni si riferiscono: interesse a mantenere la propria privacy o, in alternativa, ad essere informata della raccolta del dato; interesse ad accedere all'informazione archiviata, onde verificarne la completezza e la correttezza; interesse a sollecitarne l'eventuale rettifica, modifica, aggiornamento o cancellazione; se del caso, interesse a coinvolgere un'autorità garante del trattamento o ad adire l'autorità giudiziaria. In secondo piano, si staglia un interesse che potrebbe definirsi "collettivo", "oggettivo", "pubblicistico", in quanto la raccolta, la collezione e l'analisi dei dati rivelano la propria utilità fintanto che le informazioni immagazzinate e scambiate siano corrette, complete e aggiornate. Se, viceversa, non esistono garanzie affinché i dati vengano raccolti in modo preciso ed esaustivo; se non si scongiura il pericolo che la stessa circolazione ne adulteri il contenuto; se non si consentono tempestivi interventi correttivi e, comunque, non si assicura l'apprestamento di meccanismi funzionali a un costante aggiornamento, qualsiasi impianto circolatorio rischia di autoconfutarsi: l'accumulazione di un'enorme quantità d'informazioni, sulle cui veridicità e correttezza non è dato fare affidamento, può dar vita al paradosso di un'attività di prevenzione o repressione fuorviata proprio da ciò che principalmente la indirizza e alimenta. Sicché, si peccherebbe d'ingenuità teorizzando una relazione di proporzionalità diretta fra il mero indice numerico dei dati personali archiviati e le chance di ottenere proficui risultati investigativi[9].

---

8 Per una panoramica sulla disciplina italiana ed europea in materia di tutela dei dati personali quando s'incrocia il piano della lotta al crimine, anche al fine di individuare le ascendenze di rango *meta*-primario della disciplina in parola, cfr. A. Adam, *L'échange de données à caractère personnel entre l'Union européenne et les Etats-Unis*, in "Revue trimestrielle de droit européen", 2006, p. 411; *Banche dati, telematica e diritti della persona*, a cura di G. Alpa-M. Bessone, Padova, Cedam, 1984, *passim*; A. Blasi, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in "Rivista internazionale dei diritti dell'uomo", 1999, p. 543; M. Bonetti, *Riservatezza e processo penale*, Milano, Giuffrè, 2003, pp. 38 sgg.; G. Busia, "Privacy, attività di indagine e cooperazione internazionale in materia di giustizia e sicurezza", in *Equo processo: normativa italiana ed europea a confronto*, a cura di L. Filippi, Padova, Cedam, 2006, pp. 29 sgg.; G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, Giuffrè, 1997, pp. 3 sgg.; S. Gonella, *Uno sguardo all'evoluzione del diritto alla riservatezza: la tutela penale*, in "Diritto penale e processo", 2007, p. 531; D. Negri, "La circolazione del '*curriculum criminale*' tra i procedimenti penali", in *Contrasto al terrorismo interno e internazionale*, a cura di R.E. Kostoris e R. Orlandi, Torino, Giappichelli, 2006, p. 64; P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffrè, 2002, *passim*; *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. Negri, Roma, Aracne, 2007, *passim*; S. Rodotà, *La "privacy" tra individuo e collettività*, in "Politica del diritto", 1974, p. 545.

9 Cfr. anche G. Busia, *op. cit.*, pp. 43 sgg., che si sofferma su alcuni "falsi miti" legati all'idea che quanto più ampio è lo spettro delle informazioni raccolte tanto maggiore è l'ausilio per le attività di prevenzione e repressione dei reati.

Il confronto tra l'esigenza che le informazioni siano prontamente archiviate e circolino capillarmente e celermente, da un lato, e, dall'altro, la necessità di apprestare adeguati meccanismi di tutela del dato – sia per soddisfare l'interesse "soggettivo" del titolare, sia per ragioni "oggettive", legate all'importanza che non deambulino informazioni qualsivoglia, ma solo quelle corrette e aggiornate – rappresenta l'asse di equilibrio per ogni meccanismo informativo deputato a trattare un numero elevato di dati[10]. Lo si coglie chiaramente anche nelle trame del Programma dell'Aia, ove, rilevato il connotato bifronte di questo tema, alla tutela del dato nel "terzo pilastro" dell'Unione europea viene accordata la precedenza rispetto all'attuazione del principio di disponibilità delle informazioni[11].

2. Il Programma dell'Aia

Sul piano della cooperazione informativa, il modello offerto dal TECS di Europol, dall'EPOC-III di Eurojust, dal SIS (oramai pervenuto alla seconda generazione) e dal SID è, in estrema sintesi, raffigurabile tramite una struttura radiale, imperniata su una banca dati centrale (gestita, sia pure con modalità e obiettivi volta a volta diversi, da un organismo sovranazionale[12]) collegata a plurime unità nazionali, dislocate nei singoli Paesi UE (nel caso di Eurojust, è il membro nazionale a raccogliere informazioni nel Paese d'origine per veicolarle all'Aia[13]). Accanto a queste forme di cooperazione "accentrata", "canalizzata", si può collocare un secondo paradigma concettuale, ispirato a una logica di maggiore diffusività, cioè di scambio o accesso immediato e capillare ai dati. L'idea-madre è quella di consentire ai servizi di polizia e alle autorità giudiziarie di uno Stato di ottenere direttamente dalle autorità di polizia o giudiziarie di altri Stati le informazioni di cui necessitino nell'esercizio delle proprie funzioni, senza dover tener conto delle differenti classificazioni degli illeciti o della ripartizione delle competenze tra i servizi di polizia e le autorità giudiziarie d'oltre confine. Idea-madre che si ritrova in seno al c.d. Programma dell'Aia, adottato dal Consiglio europeo riunito-

10 Cfr. G. Busia, *op. cit.*, pp. 37 sg.; L. Salazar, *La lotta alla criminalità nell'Unione*, cit., p. 3537.

11 Quanto ai sistemi informativi che fanno capo ad Europol ed Eurojust, nonché al SIS e al SID, va detto che essi sono riguardati da apposite discipline a tutela dell'autodeterminazione informativa, contenute nelle rispettive fonti costitutive (cfr. *infra*, F. Decli-G. Marando, "Le banche dati dell'Unione europea istituite per finalità di sicurezza e di giustizia", § 2-5). Recentemente, si è tuttavia affacciata l'ipotesi che la disciplina generale, contenuta nella decisione quadro sulla tutela dei dati personali in "terzo pilastro", possa interessare anche i meccanismi circolatori che fanno capo ad Europol e ad Eurojust, nonché il SID; sul punto, vedi *infra*, § 5.

12 Europol, Eurojust, l'unità centrale del SIS e del SID (rispettivamente, C-SIS e C-SID).

13 I dovuti approfondimenti su SIS, SID, Europol ed Eurojust sono svolti *infra*: cfr. F. Decli-G. Marando, *op. cit.*

si a Bruxelles il 4 e il 5 novembre 2004[14] e inteso, tramite l'identificazione di una serie di priorità da realizzare nei successivi cinque anni, al «Rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea»[15].

Prima di procedere oltre e per completezza, va ricordato che una tappa fondamentale, nell'itinerario seguito dall'Unione europea in materia di cooperazione di polizia e giudiziaria, è rappresentata dal Consiglio europeo di Tampere (15-16 ottobre 1999), le cui conclusioni integreranno quello che viene identificato come il primo programma pluriennale (*recte*, quinquennale) del Consiglio europeo inteso a definire gli interventi prioritari volti alla creazione di uno spazio di liberà, sicurezza e giustizia[16]. Merita inoltre precisarsi che la strategia della condivisione capillare di *law enforcement informations* è rintracciabile, sia pure *in nuce*, nella Convenzione sull'assistenza giudiziaria in materia penale che, il 29 maggio 2000, è stata adotta dal Consiglio dell'Unione, col dichiarato intento di sviluppare le modalità cooperative delineate dalla Convenzione di Strasburgo del 20 aprile 1959[17]. Il principio generale ivi affermato, infatti, è quello secondo cui le richieste di assistenza giudiziaria e tutti gli scambi di informazioni dovrebbero avvenire con rapporti diretti tra le autorità giudiziarie territorialmente competenti per la presentazione delle istanze e della loro esecuzione. Il problema della Convenzione e del relativo Protocollo aggiuntivo – inteso a rafforzare le possibilità di assistenza in settori quali la lotta contro la criminalità organizzata, il riciclaggio del "denaro sporco" e la criminalità in campo finanziario – è la lentezza, se non, in certi casi, la riluttanza degli Stati membri (fra cui l'Italia) a ratificare i documenti in parola.

Il Programma dell'Aia risulta suddiviso in tre *macro*-aree.

Ad una, introduttiva, fa seguito quella dedicata agli «orientamenti generali», dove si trovano compendiati interessanti indicazioni circa i rapporti tra Unione europea e diritti fondamentali della persona, ai nostri fini rilevanti anzitutto nell'ottica del diritto alla riservatezza e all'autodeterminazione informativa. Più precisamente, il Consiglio europeo afferma, ragionando di futuribili, che l'integrazione della Carta di Nizza nel Trattato che adotta una Costituzione per l'Europa (come Parte II dello stesso) e l'adesione dell'Unione alla Convenzione europea

---

14 Il Programma è pubblicato in *GUUE*, C 53, 3 marzo 2005, p. 1.

15 In dottrina, cfr. le sintesi operate da E. Aprile, *op. cit.*, pp. 35 sgg.; L. Salazar, *La lotta alla criminalità nell'Unione*, cit., p. 3533; F. Spiezia, *Crimine transnazionale e procedure di cooperazione giudiziaria*, Milano, Il Sole 24 Ore – Pirola, 2006, pp. 110 sgg.

16 Sul "Programma di Tampere" <http://www.consilium.europa.eu/ueDocs/cms__Data/docs/pressData/it/ec/00200-rl.i9.htm>, efficacemente definito da L. Salazar, *La lotta alla criminalità nell'Unione*, cit., p. 3511, «il '*big bang*' della cooperazione tra gli Stati membri dell'Unione nel settore della Giustizia e degli Affari interni», v., *ex plurimis*, G. Calesini, *Diritto europeo di polizia*, Roma, Laurus Robuffo, 2007, pp. 37 sgg.; L. Salazar, *La costruzione di uno spazio di libertà, sicurezza e giustizia dopo il Consiglio europeo di Tampere*, in "Cassazione penale", 2000, p. 1114; F. Storelli, *op. cit.*, pp. 147 sgg.; J.A.E. Vervaele, *op. cit.*, pp. 142 sgg.

17 Brevi cenni in E. Aprile, *op. cit.*, pp. 48 sgg.

di salvaguardia dei diritti dell'uomo e delle libertà fondamentali comporteranno, per l'Unione e le sue istituzioni, l'obbligo di garantire che, in tutti i settori di competenza, i diritti fondamentali siano, non solo rispettati, ma anche attivamente promossi[18]. Affermazioni, queste, di cui si rischia di perdere le tracce quando, dal piano declamatorio, si passa a quello operativo e, più precisamente, alle travagliate vicende interistituzionali della (solo recentemente approvata) proposta di decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[19].

La terza parte del Programma è riservata agli «orientamenti specifici». Il momento di maggiore interesse si colloca in seno alle politiche di «rafforzamento della sicurezza» e, in particolare, alla prospettiva di miglioramento dello scambio di informazioni. Il Consiglio europeo, infatti, si proclama convinto che il rafforzamento della libertà, della sicurezza e della giustizia richieda un «approccio innovativo»[20] nei confronti dello «scambio transfrontaliero di informazioni in materia di applicazione della legge» («cross-border exchange of law enforcement information»): «il fatto che le informazioni attraversino le frontiere», si legge nel Programma, «non dovrebbe più, di per sé, essere rilevante»[21]. Più in dettaglio, dal 1° gennaio 2008, lo scambio di informazioni dovrebbe rispettare le condizioni che il Consiglio enuncia, plasmando il «principio di disponibili-

---

18 Sui rapporti tra Convenzione europea dei diritti dell'uomo (ratificata da tutti i ventisette Stati UE, insieme ad alcuni Protocolli addizionali), c.d. Carta di Nizza e Unione europea, vedansi, *ex plurimis*, E. Aprile, *op. cit.*, p. 141; B. Conforti, *Note sui rapporti tra diritto comunitario e diritto europeo dei diritti fondamentali*, in "Rivista internazionale dei diritti dell'uomo", 2000, p. 423; R. Mastroianni, *Il contributo della Carta europea alla tutela dei diritti fondamentali nell'ordinamento comunitario*, in "Cassazione penale", 2002, p. 1873; B. Piattoli, *Diritto giurisprudenziale C.e.d.u., garanzie europee e prospettive costituzionali*, in "Diritto penale e processo", 2008, p. 262; H. Tretter, "La Convenzione europea sui diritti dell'uomo e la Carta dei diritti fondamentali dell'Unione europea", in *La Carta e le Corti. I diritti fondamentali nella giurisprudenza europea multilivello*, a cura di G. Bronzini-V. Piccone, Taranto, Chimienti, 2007, p. 258; U. Villani, *I diritti fondamentali tra Carta di Nizza, Convenzione europea dei diritti dell'uomo e progetto di Costituzione europea*, in "Il diritto dell'Unione europea", 2004, p. 73. Oggi il tema è oggetto di attenzione nel Trattato di Lisbona, che così riscrive l'art. 6 TUE: «1. L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, [...] che ha lo stesso valore giuridico dei trattati. [...] 2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. [...] 3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali».

19 V. *infra*, § 3 e 5.

20 Degno di nota l'aggettivo («innovativo») che, nel rimarcare il tratto di novità insito nella forma cooperativa prospettata, implicitamente la distingue da quelle oramai divenute "tradizionali", in quanto imperniate su unità centrali di coordinamento e collegamento tra plurime unità nazionali, come sono Europol, Eurojust, SIS e SID.

21 Particolarmente eloquente il testo inglese che ricorre all'aggettivo *mere* («the mere fact that information crosses borders should no longer be relevant»), ad indicare che, nell'ottica del Programma, il passaggio di informazioni da uno Stato all'altro sarebbe un "mero fatto".

tà» («principle of availability»): si tratta di assicurare che, in tutta l'Unione, un «ufficiale di un servizio di contrasto» («a law enforcement officer») di uno Stato membro che ha bisogno di informazioni nell'esercizio delle proprie funzioni sia in condizione di ottenerle («can obtain») da un altro Stato membro; *rectius*, sia in condizione di ottenerle direttamente dall'autorità di contrasto straniera, posto che, per il Consiglio europeo, è «il servizio di contrasto nell'altro Stato membro» («the law enforcement agency in the other Member State») che dispone di tali informazioni ad essere tenuto a renderle disponibili («will make it available») per i fini dichiarati.

Sebbene il Consiglio europeo si esprima con tono "leggero", evitando accenti enfatici, lo scenario che dipinge è rivoluzionario. Basti dire che lo stesso Programma sancisce che lo scambio di informazioni dovrebbe avvenire «attraverso l'accesso reciproco o l'interoperabilità di basi di dati nazionali» («through reciprocal access to or interoperability of national databases»), mentre solo in alternativa è contemplato «l'accesso diretto (on-line) [...] alle basi di dati centrali dell'UE già esistenti quali il SIS» e la creazione di nuove banche dati centralizzate a livello europeo viene subordinata all'elaborazione «di studi che ne dimostrino il valore aggiunto». La via maestra è, dunque, quella dell'accesso diretto (e reciproco), seguendo la quale un qualsiasi *law enforcement officer*, cioè un qualsiasi ufficiale di un'autorità di contrasto (come sono per eccellenza le forze di polizia, ma non va esclusa *a priori* l'autorità giudiziaria[22]), verrebbe messo in condizione di accedere direttamente alle banche dati di *law enforcement* straniere. Meno perspicuo, invece, il testuale riferimento all'interoperabilità fra i database nazionali[23]: il tentativo di ascrivervi un significato autonomo suggerisce un assetto di rapporti in cui l'autorità di contrasto di uno Stato membro viene posta in condizione, non solo di accedere direttamente all'archivio straniero, ma anche di integrarlo, aggiornarlo o correggerlo a mezzo di modifiche apportate a una banca dati nazionale, "interoperante", appunto, con l'archivio d'oltre confine.

Evidente il divario che intercorre tra queste direttrici prospettiche e quella dello scambio di informazioni a mezzo di sistemi che fanno perno su un'unità centrale di collezione o analisi del dato (Europol, Eurojust, SIS, SID), i quali ri-

---

22 Cfr., in particolare, quanto si dirà a proposito dell'iniziativa del Regno di Svezia, *infra*, § 7.

23 Il concetto di "interoperabilità" compare anche nella comunicazione COM (2005) 597 def. (disponibile all'indirizzo <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0597:IT:HTML>), che la Commissione ha rivolto al Consiglio e al Parlamento europeo il 24 novembre 2005, concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni. Ivi, l'interoperabilità è definita come la «capacità dei sistemi informatici, e dei processi operativi da questi supportati, di scambiare dati e di condividere informazioni e conoscenze» («ability of information technology systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge»). Facile convenire che non si tratta di una descrizione illuminante, soprattutto se l'intento è quello di tracciare una linea di demarcazione rispetto al concetto di accesso reciproco.

spondono alla logica secondo cui i dati appartengono anzitutto all'autorità nazionale che li raccoglie e li detiene, collocandosi in un momento successivo ed eventuale l'ipotesi dell'inserimento in un sistema informativo transnazionale.

A ben considerare, la prospettiva delineata dal Consiglio europeo nel novembre 2004 finisce per stravolgere il concetto stesso di banca dati nazionale, posto che, almeno in astratto, gli utenti di un archivio creato all'interno di uno Stato divengono, indistintamente, le autorità di contrasto degli altri Stati membri («reciprocal access to [...] national databases»), le quali, inoltre, sembrano legittimate a modificarne i contenuti, al pari delle autorità nazionali, sfruttando l'interoperabilità. Sicché, la banca dati, "nazionale" per ragioni topografiche (dal luogo in cui si trova materialmente il database) e genealogiche (perché concepita da un'autorità di uno Stato membro), diviene "europea" sul piano funzionale e operativo, in quanto fruibile e, al limite, modificabile nei contenuti anche dalle autorità straniere[24]. In tal modo, la cooperazione di polizia e giudiziaria in materia penale che si attua nelle forme dell'*information sharing* non risulta più condizionata al "*good will*" delle autorità di *law enforcement* nazionali chiamate, o a rispondere a specifiche domande provenienti da oltre confine, o a inserire in sistemi informativi sovranazionali (come il SIS o il SIS) determinate categorie di informazioni. In forza del principio di disponibilità, quando un archivio viene forgiato, arricchito, aggiornato o corretto a livello nazionale è *in re ipsa* la possibilità che di tali integrazioni o modifiche fruiscano e beneficino anche le autorità straniere.

Non servirà spiegare perché questa politica di accesso diretto, reciproco, prodromo dell'interoperabilità, se, da un lato, si candida a innovare il metodo tradizionale di cooperazione strategica di polizia e giudiziaria in materia penale, dall'altro, acuisce i problemi legati alla tutela della privacy e dell'autodeterminazione informativa. Nell'ottica del soggetto cui il dato si riferisce, ci si trova *ex abrupto* catapultati da una dimensione spaziale nazionale ad una dimensione europea: l'informazione personale raccolta nel Paese di origine è, in potenza, accessibile e utilizzabile da parte di qualsiasi autorità di *law enforcement* europea. L'interesse a che non siano archiviati propri dati personali al di fuori dei casi previsti dalla legge; l'interesse a che i dati, se raccolti, risultino corretti e completi; l'interesse all'aggiornamento e all'eventuale cancellazione; l'interesse al rispetto del principio di finalità limitata, sono tutte pretese che il Programma dell'Aia alimenta e amplifica, poiché, giusta il principio di disponibilità, eventuali errori e abusi rischiano di diffondersi e proliferare in Europa. Non manca poi di interferire la dimensione "oggettiva" e pubblicistica della tutela del dato. Le "cattive

24 F. Gandini, *Il Trattato di Prüm articolo per articolo. Ecco le nuove frontiere per la sicurezza. Banche dati antiterrorismo e interventi congiunti in 7 Stati Ue*, in "Diritto e giustizia", 2006, n. 37, p. 58, condivisibilmente afferma che, giusta il principio di disponibilità, «non ha più alcuna rilevanza il luogo in cui i dati e le informazioni sono detenuti poiché essi devono essere posti nella disponibilità di tutte le autorità interessate, per lo svolgimento delle rispettive attribuzioni».

informazioni", infatti, non sono in genere *ictu oculi* riconoscibili e, se circolano liberamente, mescolandosi ai dati corretti, rischiano di vanificare anche l'utilità di questi ultimi: discorso valido sul piano nazionale, ma che acquista viepiù rilevanza se ci si colloca in una dimensione europea. In quest'ultima, del resto, non ci si può nemmeno nascondere che, soprattutto le ipotesi di accesso diretto on-line[25], scontano le gravi difficoltà che un ufficiale di contrasto di uno Stato membro può incontrare quando, in prima persona, sia chiamato a ricercare, selezionare, estrapolare informazioni in banche dati straniere, ove alla differenza linguistica si sommano le diverse esperienze e sensibilità giuridiche e culturali: il rischio (molto concreto) è che un dato, sia pure corretto, venga frainteso dalla autorità straniera che lo attinge.

Consapevole di ciò, il Consiglio europeo invita la Commissione a formulare, entro la fine del 2005, proposte relative all'attuazione del principio di disponibilità che «dovrebbero osservare rigorosamente»[26] una serie di condizioni fondamentali, compiutamente elencate dal Programma. Tra le altre, meritano esplicita menzione le previsioni secondo cui: «lo scambio [potrà] avere luogo soltanto ai fini della corretta esecuzione di compiti stabiliti dalla legge»; dovranno essere garantiti «l'integrità dei dati oggetto dello scambio» e «il controllo del rispetto della protezione dei dati [...] prima e dopo lo scambio»; «le persone [dovranno] essere tutelate contro l'uso improprio dei dati e [...] avere il diritto a richiedere la correzione dei dati errati»[27]. Così facendo, il Consiglio europeo arriva a configurare un corredo di diritti e garanzie, relativi alla protezione dei dati personali, quale condizione per attuare correttamente il principio di disponibilità[28].

---

25 Per un esempio, vedasi la proposta di decisione quadro della Commissione n. 490 del 2005, *infra*, § 4.

26 Discutibile, sul piano semantico, questo accostamento tra l'avverbio «rigorosamente» e la coniugazione del servile al condizionale, «dovrebbero»; analogo il testo inglese: «the following key conditions should be strictly observed».

27 Per alcune sintetiche notazioni su queste garanzie di base, v. G. Busia, *op. cit.*, pp. 72 sgg.

28 Il Consiglio europeo non manca di soffermarsi su numerose altre questioni rilevanti nell'ottica della cooperazione di polizia e giudiziaria in materia penale e, sovente, allude a forme d'intenso scambio di informazioni. Tuttavia, rispetto alla portata generalizzata del principio di disponibilità, queste ulteriori statuizioni si pongono in un rapporto di *species ad genus*. Ad esempio, ai fini di un'efficace prevenzione e lotta al terrorismo, la prospettiva dell'*information sharing* arriva ad involgere anche i servizi segreti («security services»), viceversa non menzionati testualmente a proposito del principio di disponibilità, rispetto al quale compare il solo (per quanto generico) riferimento alle *law enforcement authorities*.

3. Dal Programma all'azione. La proposta di decisione quadro della Commissione in materia di protezione dei dati personali (COM (2005) 475 def.)

Il 10 maggio 2005, la Commissione rivolgerà una comunicazione al Consiglio e al Parlamento europeo[29], intesa ad avviare l'attuazione organica del Programma dell'Aia[30]. Trattasi di un piano d'azione che si compone di due parti, l'una intesa a sintetizzare le finalità e alcuni degli aspetti di maggior rilievo del Programma[31], l'altra consistente in un allegato che elenca le misure e le azioni concrete prospettate per i successivi cinque anni. È sotto l'intitolazione «tutela della vita privata e della sicurezza in sede di scambio di informazioni: trovare il giusto equilibrio» che la Commissione, in premessa, definisce «inammissibile»[32] che il mantenimento effettivo dell'ordine pubblico e le indagini relative alla criminalità transfrontaliera vengano ostacolati, in uno spazio di libera circolazione, da procedure gravose in materia di scambio di informazioni. Perciò, l'Unione viene chiamata ad avviare

---

29 COM (2005) 184 def., intitolata «Il Programma dell'Aia: dieci priorità per i prossimi cinque anni. Partenariato per rinnovare l'Europa nel campo della libertà, sicurezza e giustizia», <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0184:FIN:IT:PDF>.

30 Su quest'ultimo e sulla comunicazione in parola si esprimerà, con accenti parzialmente critici e un'impostazione nettamente "ridimensionante", il Comitato economico e sociale europeo (CESE), il cui parere, del 15 dicembre 2005 (in *GUUE*, C 65, 17 marzo 2006, p. 120), esordisce con la notazione secondo cui, dopo cinque anni, gli obiettivi fissati a Tampere (v. *supra*, § 2) non si possono dire raggiunti e l'Unione europea non può ancora considerarsi uno spazio comune di libertà, sicurezza e giustizia. Il Comitato, in altri termini, esprime, rispetto all'attuazione del Programma di Tampere, un giudizio globale negativo, constatando che plurimi obiettivi specifici allora decisi non sono stati raggiunti e che la qualità di molte delle politiche adottate non è pari alle aspettative. In questo scenario, il Programma dell'Aia subentra nel difficile compito di consolidare e favorire la creazione di uno spazio comune di libertà, sicurezza e giustizia. Tuttavia, secondo il CESE, a differenza del Programma del 1999, quello del 2004 non contiene politiche innovative e ha una portata poco ambiziosa, in quanto si basa sulla necessità di applicare e valutare in modo più efficace le politiche già esistenti (nello stesso senso, in dottrina, L. Salazar, *La lotta alla criminalità nell'Unione*, cit., p. 3513). Notazione, quest'ultima, che non sembra però valere per il principio di disponibilità. Invero, a detta dello stesso Comitato, uno degli elementi più innovativi del Programma dell'Aia è il principio *de quo loquimur*, anche se reputa tutt'altro che chiari l'esatto contenuto, l'impatto reale, l'ambito di applicazione e le modalità di attuazione di questo principio (espressamente definito «rivoluzionario»). Perché sia operativo, osserva il Comitato, occorrerà un elevato livello di fiducia reciproca tra le autorità di polizia dei rispettivi Paesi, fiducia che, tuttavia, non può darsi per scontata, dato che è proprio la sua mancanza ad aver rappresentato in passato uno degli elementi che più ha ostacolato la cooperazione sul piano europeo. Per il CESE, sarà dunque necessario potenziare la cooperazione tra le agenzie, le istituzioni e gli operatori dell'Unione europea, responsabili in materia di sicurezza, libertà e giustizia, e si dovrà inoltre garantire il controllo giudiziario sul funzionamento del principio di disponibilità e sulle attività che esso comporta nella pratica.

31 In pratica, vengono definite dieci priorità specifiche sulle quali la Commissione reputa opportuno concentrare gli sforzi nell'arco del successivo quinquennio, priorità definite «equamente importanti e che ricomprendono l'intera gamma degli obiettivi dell'Aia».

32 Con ciò rievocando l'*incipit* dell'iniziativa legislativa svedese del giugno 2004, su cui ci si intratterrà *infra*, § 7.

un dialogo costruttivo, al fine di trovare soluzioni equilibrate, che sappiano combinare l'assoluto rispetto dei diritti fondamentali relativi alla tutela della privacy e dei dati personali col principio di disponibilità delle informazioni.

Di lì a poco, il Consiglio e la Commissione adotteranno congiuntamente un Piano d'azione «sull'attuazione del Programma dell'Aia inteso a rafforzare la libertà, la sicurezza e la giustizia dell'Unione europea»[33] che, nella sostanza, ricalca i contenuti della immediatamente pregressa comunicazione della Commissione, ma che da questa si distingue per il *quid pluris* rappresentato dalla convergenza d'intenti col Consiglio.

È su queste solide basi strategiche che, nell'ottobre 2005, la Commissione avanza e indirizza al Consiglio due proposte di decisione quadro relative, l'una alla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (COM (2005) 475 def., del 4 ottobre 2005[34]), l'altra allo scambio d'informazioni in virtù del principio di disponibilità (COM (2005) 490 def., del 12 ottobre 2005, su cui ci si soffermerà ampiamente in seguito[35]). La Commissione non mancherà di definire la prima il *pendant* indispensabile alle proposte dirette ad attuare il principio *de quo loquimur*[36]: parole che l'esperienza degli anni successivi avrà modo di smentire ampiamente.

Merita segnalarsi come la Relazione che accompagna la proposta n. 475 del 2005 si apra con un'interessante panoramica sulle fonti europee rilevanti in materia di autodeterminazione informativa e tuttavia inidonee (sia pure per motivi

---

33 L'adozione risale al 2-3 giugno 2005; la pubblicazione avverrà in *GUUE*, C 198, 12 agosto 2005, p. 1.

34 *Documento del Consiglio n. 2005/0202 (CNS)*, 4 ottobre 2005, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0475:FIN:IT:PDF>.

35 Cfr. § 4.

36 Cfr. la «Relazione sull'attuazione del programma dell'Aia per il 2005» (COM (2006) 333 def., 28 giugno 2006, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0333:FIN:IT:PDF>), comunicazione rivolta al Consiglio e al Parlamento europeo. Davvero degne nota le conclusioni cui perviene la Commissione a proposito delle politiche di giustizia, libertà e sicurezza (GLS) in primo e terzo pilastro. Infatti, premesso che, a livello di fonti normative europee di diritto derivato, l'attuazione del Programma sembra procedere spedita (in particolare, ove vige il c.d. metodo comunitario, cioè, salvo qualche eccezione, in "primo pilastro"), la Commissione conclude affermando che il bilancio è molto più esiguo se si guarda all'attuazione a livello nazionale degli strumenti adottati. Notazione critica riproposta un anno più tardi (nell'omologa Relazione COM (2007) 373 def., 3 luglio 2007, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0373:FIN:IT:PDF>), in cui si osserva che anche il secondo esercizio di monitoraggio del Programma dell'Aia rivela una notevole disparità tra il livello dell'adozione (UE) e il livello dell'attuazione (nazionale) dei singoli strumenti: l'adozione istituzionale è stata generalmente positiva, quantomeno nelle materie del Titolo IV TCE (mentre quelle di terzo pilastro rivelano indici piuttosto negativi); l'attuazione nazionale è, invece, carente in tutti i settori.

volta a volta diversi[37]) a dettare una disciplina di riferimento per la protezione dei dati personali nel perimetro della cooperazione di polizia e giudiziaria in materia penale[38]. Disciplina che, negli intendimenti della Commissione, non dev'essere intesa esclusivamente come un baluardo per il soggetto interessato dal trattamento del dato, posto che essa integra (anche) una condizione irrinunciabile, affinché lo scambio di *law enforcement informations* non sia intralciato dai diversi livelli di protezione dei dati, altrimenti apprestati dai singoli Stati membri.

Dalla Relazione si evince che, prima di varare il testo della proposta, sono stati consultati i governi dei Paesi interessati, le Autorità nazionali responsabili della protezione dei dati, nonché i rappresentati del Garante europeo della privacy, di Europol, di Eurojust e del Segretariato delle Autorità di controllo comuni. Al qual riguardo, non passa inosservato come solo il Parlamento europeo e le autorità garanti si siano dimostrati estremamente favorevoli all'adozione di uno strumento giuridico sulla protezione dei dati personali nell'ambito del "terzo pilastro", mentre i rappresentanti dei governi, di Europol e di Eurojust non hanno espresso una posizione comune in materia; hanno semmai genericamente convenuto che l'attuazione del principio di disponibilità deve essere accompagnata da adeguate norme di compensazione nel settore della protezione dei dati. Più precisamente, alcuni Stati membri hanno giudicato più logico definire, prima, le modalità dello scambio di informazioni e, solo successivamente, occuparsi delle norme per la protezione dei dati; altri hanno, invece, proposto l'inserimento di una serie di disposizioni specifiche nell'atto relativo al principio di disponibilità. Non a caso, quindi, un documento di lavoro della Commissione, allegato al testo della proposta di decisione quadro[39], contempla una serie di opzioni alternative, concernen-

---

37 Gioverà svolgere un breve richiamo ad alcune notazioni concernenti la direttiva 95/46/CE. Condivisibilmente, infatti, la Commissione osserva che l'inapplicabilità della direttiva non è solo una questione formale, legata all'architettura a "pilastri" dell'Unione o a disposizioni specifiche (quali l'art. 3, par. 2), ma discende dal fatto che la direttiva è stata concepita prendendo a riferimento attività diverse da quelle di *law enforcement*. E se non si nega che i princìpi di base, relativi al trattamento dei dati e alla loro protezione, siano a grandi linee i medesimi, sia in primo che in terzo pilastro, si reputa comunque che quest'ultimo necessiti di una disciplina *ad hoc*. Più precisamente, si teme che, ove si estendesse la direttiva 95/46/CE alle attività di contrasto alla criminalità, gli Stati membri, giusta l'art. 13 (che legittima deroghe alle forme di tutela apprestate in via generale, quando vengano in gioco esigenze di *law enforcement*), di fatto non risulterebbero vincolati all'adozione di normative interne ispirare da standard europei.

38 Più generale la portata, ma, al contempo, meno nitida la valenza prescrittiva nell'ambito del diritto dell'Unione europea dell'art. 8 C.e.d.u. e della relativa giurisprudenza della Corte di Strasburgo, della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (Convenzione del 28 gennaio 1981, n. 108), del suo Protocollo aggiuntivo dell'8 novembre 2001 relativo alle autorità di controllo e ai flussi transfrontalieri, nonché della raccomandazione R (87) 15 del Comitato dei ministri del Consiglio d'Europa (17 settembre 1987) che si occupa dell'uso dei dati personali nel settore di polizia.

39 *Documento n. SEC (2005) 1241*, 4 ottobre 2005, <http://www.europarl.europa.eu/meetdocs/2004_2009/documents/sec/com_sec(2005)1241_/com_sec(2005)1241_en.pdf>.

ti il tema della tutela dell'autodeterminazione informativa nel contesto del c.d. terzo pilastro, riservando ad ognuna una specifica riflessione su pregi e difetti. Si va dal polo dell'astensione *tout court* dall'intervento normativo («option 1: No legislative initiative») all'ipotesi dell'applicazione *in subiecta materia* della direttiva afferente al pilastro comunitario («option 2: Application of Directive 95/46/EC»); dall'idea di posticipare la disciplina della privacy rispetto all'attuazione del principio di disponibilità («option 3: Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined») a quella di inserire la disciplina in parola nello strumento normativo relativo al suddetto principio («option 4: Specific provisions in a legal instrument on the exchange of information under the principle of availability»); si contempla poi l'idea di una decisione quadro che involga ogni forma di trattamento di dati nel contesto del Titolo VI TUE («option 5: Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union»), per culminare nel progetto di un'iniziativa legislativa che coinvolga tutti i sistemi informativi e tutti gli organismi centralizzati dell'Unione europea («option 6: Legislative initiative involving all existing EU information systems or bodies – Europol, Eurojust»). Come si avrà subito modo di vedere, le preferenze della Commissione convergono sull'opzione n. 5; la pluralità di strategie alternative suggerite dai rappresentanti degli Stati membri, per converso, si fa segno premonitore delle difficoltà che la proposta di decisione quadro in commento incontrerà in sede di adozione da parte del Consiglio[40].

Il testo della proposta di decisione quadro n. 475 del 2005 compendia, nella parte iniziale, oltre ad alcuni "considerando" degni di nota[41], l'eloquente identificazione della base giuridica dell'atto. Per la Commissione, ad essere interessate dalle disposizioni sulla protezione dei dati personali sono tanto le azioni comuni

---

40 V. *amplius infra*, § 5.

41 Nel "considerando" n. 6, si legge che uno strumento giuridico, relativo a norme comuni per la protezione dei dati personali, trattati ai fini della prevenzione e della lotta contro la criminalità, deve dimostrarsi coerente con la politica generale dell'Unione europea in materia di privacy e protezione dei dati personali. Esso dovrebbe, pertanto, rifarsi, per quanto possibile e tenendo conto della necessità di migliorare l'efficacia delle attività di *law enforcement*, a princìpi e definizioni esistenti, segnatamente a quelli contenuti nella direttiva 95/46/CE del Parlamento europeo e del Consiglio, a quelli che riguardano lo scambio di informazioni di Europol ed Eurojust, e a quelli trattati mediante il sistema di informazione doganale o altri strumenti affini. In altre parole, la Commissione, una volta chiarito che, da un punto di vista tecnico-giuridico, gli strumenti esistenti non coprono l'area della cooperazione di polizia e giudiziaria in materia penale che avvenga secondo la logica del principio di disponibilità delle informazioni, si premura di chiarire che, comunque, tali strumenti debbono fungere da modello e da termine di riferimento generale in questo settore. Infine, non mancano regole di coordinamento con altri strumenti rilevanti in materia di protezione del dato personale ("considerando" nn. 19 sgg.), né disposizioni dedicate alla posizione particolare del Regno Unito, dell'Irlanda, dell'Islanda, della Norvegia e della Svizzera ("considerando" nn. 27 sgg.).

nel settore della cooperazione di polizia, ai sensi dell'art. 30, par. 1, lett. *b*) TUE, quanto le azioni comuni nel settore della cooperazione giudiziaria in materia penale, di cui all'art. 31 par. 1, lett. *a*) TUE: oggetto di attenzione è, in altri termini, il trattamento di informazioni personali che, in materia penale, avviene, vuoi nel contesto della cooperazione di polizia (art. 30 TUE), vuoi nel contesto della cooperazione giudiziaria (art. 31 TUE). Precisazione tutt'altro che ridondante, posto che il riferimento testuale del Programma dell'Aia allo scambio di informazioni tra "autorità di contrasto" (*law enforcement authorities*) non è univoco, legittimando sia esegesi restrittive, polarizzate sulle sole autorità di polizia, sia altre, più late, che coinvolgano anche l'autorità giudiziaria. Ebbene, la proposta di decisione quadro della Commissione scavalca l'ostacolo, non discriminando tra autorità di polizia e autorità giudiziarie. Se ne trae conferma dall'art. 3, secondo cui la decisione quadro si applica al trattamento, automatizzato o meno, di dati personali, posto in essere da quella che viene chiamata «autorità competente» ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati penali. "Autorità competente" che l'art. 2 lett. *j*) definisce in modo esplicito, menzionando sia le autorità giudiziarie, sia quelle doganali e di polizia.

È chiaro, insomma, che la decisione quadro si candida a pervadere, tanto il campo della cooperazione giudiziaria in materia penale, quanto quello della cooperazione di polizia. Come chiarisce il "considerando" n. 20, le disposizioni della decisione quadro non si applicano, invece, ai trattamenti dei dati personali effettuati dall'Ufficio europeo di polizia (Europol), dall'Unità europea di cooperazione giudiziaria (Eurojust) e dal Sistema di Informazione delle Dogane (SID), in quanto i relativi circuiti informativi sono interessati da un'apposita disciplina, posta a tutela dell'autodeterminazione informativa (su questo versante, tuttavia, si registreranno in seguito dei cambiamenti di rotta[42]). Peculiare il caso del SIS e del SIS II: i "considerando" nn. 21 e 22 prevedono una sostituzione della loro disciplina in tema di protezione dei dati ad opera della decisione quadro *de qua loquimur* (scelta che, tuttavia, non verrà confermata dal "considerando" n. 39 della decisione quadro 2008/977/GAI).

Ai sensi dell'art. 2 lett. *b*), il concetto di «trattamento» dei dati personali[43] sposato dalla Commissione appare letteralmente onnivoro, posto che ricomprende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, relative ai dati in parola. Vi rientrano la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissio-

---

42 Cfr. *infra*, § 5.

43 L'art 2 lett. *a*) definisce "dato personale" qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

ne, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione. Ciò premesso, e al fine di assicurare che i Paesi membri si adoperino affinché i dati vengano trattati «correttamente e lecitamente», la Commissione stila anzitutto una serie di «principi relativi alla qualità dei dati».

Gli Stati vengono sollecitati, oltre che a rispettare scrupolosamente il principio di "finalità limitata"[44], a distinguere le informazioni in categorie, a seconda dei diversi livelli di accuratezza del trattamento e di affidabilità delle rispettive fonti, in particolare sceverando i dati basati su fatti specifici da quelli basati su opinioni o considerazioni personali. Questa opzione si coniuga con la disciplina riservata allo scambio *cross-border* di informazioni[45], ove è imposto agli Stati di provvedere affinché la qualità dei dati personali sia verificata, nei limiti del possibile, prima che questi siano trasmessi o resi disponibili. Mette conto di dire che corre una precisa differenza tecnica fra "trasmettere" e "rendere disponibile". Nel primo caso, l'autorità che detiene il dato riceve una richiesta e a questa risponde, trasmettendo l'informazione. Quando invece quest'ultima è inserita in un archivio direttamente compulsabile dall'autorità straniera, si dirà che l'informazione, dal momento dell'inserimento nel database, è "resa disponibile".

Come si vede, la proposta di decisione quadro mira a dimostrarsi onnipervasiva, di modo che, quali che siano le scelte compiute sul fronte attuativo del principio di disponibilità (che potrebbe incentrarsi sul meccanismo della domanda-risposta o su quello dell'accesso immediato on-line), le proprie regole si dimostrino agevolmente applicabili. In particolare, ogniqualvolta un dato debba essere trasmesso, dovranno indicarsi, se possibile, le decisioni giudiziarie, o quelle con cui si è deciso di non procedere («judicial decisions as well as decisions not to prosecute»), dalle quali il dato è ricavato; altrimenti, nell'ipotesi di dati basati su opinioni o considerazioni personali, dovrà effettuarsi una verifica alla fonte prima della trasmissione, precisandosi anche il livello di accuratezza e affidabilità. Con i dovuti adeguamenti, la stessa *ratio* ispira le prescrizioni afferenti ai dati resi disponibili mediante accesso diretto automatico: gli Stati membri disporranno affinché la qualità dei dati sia regolarmente verificata al fine di

---

44 Secondo cui i dati dovranno essere rilevati per finalità determinate, esplicite e legittime nonché, successivamente, trattati in modo non incompatibile con tali finalità. Dovranno inoltre risultare adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono stati rilevati e/o per le quali vengano successivamente trattati; dovranno essere esatti e, se necessario, aggiornati. In generale, le informazioni dovranno conservarsi in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono state rilevate.

45 Cfr. l'art. 9; disposizione che, a ben guardare, rappresenta la versione meglio profilata di quanto sancito all'art. 5, par. 5, della raccomandazione R (87) 15 del Comitato dei ministri del Consiglio d'Europa, <http://www.privacy.it/CER-87-15.html>.

garantire che gli stessi, cui si consente l'accesso diretto da parte delle autorità straniere, siano precisi e costantemente aggiornati.

Si prevedono garanzie destinate ad operare *a priori* e *a posteriori*. *Ex ante*, gli Stati devono assicurare che i dati personali, se non più precisi o aggiornati, non vengano punto trasmessi o resi disponibili. *Ex post*, devono disporre affinché l'autorità competente, che ha trasmesso o reso disponibili i dati personali a un'autorità competente di un altro Stato membro, informi immediatamente quest'ultima qualora accerti, di propria iniziativa o in seguito a una richiesta della persona cui si riferiscono i dati, che questi non dovevano essere trasmessi o resi disponibili, o che sono stati trasmessi o resi disponibili dati imprecisi o non aggiornati: l'autorità competente "ricevente", informata nei modi appena indicati, cancellerà o rettificherà i dati in questione. Non è escluso, del resto, il percorso inverso, poiché l'autorità ricevente, la quale accerti che i dati ottenuti sono imprecisi, è tenuta a rettificarli e a informare immediatamente l'autorità competente che li ha trasmessi o resi disponibili. Peculiare il caso del c.d. contrassegno: lo si appone alle informazioni che, stando alla persona interessata, sono imprecise o scorrette, qualora non vi siano le condizioni per accertare se ciò corrisponda a verità. Il contrassegno verrà rimosso solo previo consenso dell'interessato o sulla base di un provvedimento giurisdizionale o dell'autorità di controllo competente.

Sotto diverso prospetto, gli Stati membri sono tenuti a provvedere, affinché i dati raccolti risultino chiaramente distinguibili in ragione dello status dei soggetti cui afferiscono. *Inter cetera*, sono contemplate: le persone sospettate di aver commesso un reato (nel nostro ordinamento processuale, vengono in gioco le persone sottoposte a indagini preliminari e gli imputati, salva l'ipotesi della condanna, che rientra nella categoria successiva); le persone condannate in sede penale (la decisione quadro non si riferisce alle sole condanne definitive); le persone che danno adito a ritenere che commetteranno un reato (l'ambito è quello pregresso all'acquisizione di una *notitia criminis*; si tratta di soggetti ritenuti pericolosi, di cui si sospetta, non tanto che abbiano delinquito, quanto che stiano per commettere reati; non servirà dire della delicatezza e dell'ambiguità di questa categoria, fondata sul mero sospetto).

In sintesi, la Commissione sposa la logica della differenziazione, acciocché l'enorme mole dei dati immagazzinati non appaia, nel complesso, come una congerie, ma si riveli viceversa strutturata secondo un ordine che, in un ipotetico sistema di riferimento cartesiano a tre dimensioni, risulterebbe dettato dalle coordinate dello status del soggetto interessato, della natura della fonte della notizia archiviata e del livello di accuratezza del trattamento riservatole.

In ogni caso, i Paesi membri dovranno adoperarsi affinché, al trattamento dei dati in oggetto, si proceda soltanto se vi siano ragionevoli motivi per credere, sulla base di fatti specifici, che le informazioni personali in questione rendano possibili, agevolino o accelerino la prevenzione, le indagini, l'accertamento o il perseguimento di un reato, sempre che non risultino altri mezzi meno invasivi per la persona cui i dati si riferiscono e il trattamento non si riveli comunque

eccessivo rispetto al reato in questione. Detto altrimenti, nella logica della proposta di decisione quadro[46], il trattamento dei dati personali e, segnatamente, la circolazione *cross-border* degli stessi, sono considerati come un'*extrema ratio* nel variegato *genus* degli strumenti intesi alla prevenzione e alla repressione dell'illecito criminale.

Discorso, questo, che, se è valido in generale, acquista massima centralità rispetto ai dati c.d. sensibili, cioè idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché profili concernenti la salute o la vita sessuale. Non a caso, dunque, l'art. 6 ne vieta in linea di principio il trattamento, mentre la risoluzione legislativa del Parlamento del 27 settembre 2006[47] contemplerà una serie di garanzie aggiuntive concernenti i dati biometrici e i profili DNA, interpolando un nuovo par. 2-*ter* in seno all'art. 6[48].

Gli Stati membri sono chiamati a garantire che i dati personali, ricevuti da "oltre confine", non rimangano immagazzinati *sine die*, ma vengano cancellati a determinate condizioni, precisate in seno alla proposta[49]. A rimarcare che la cancellazione del dato integra essenzialmente una garanzia soggettiva ("diritto all'oblio"), la previsione secondo cui le informazioni personali non vengono cancellate, bensì "bloccate", conformemente al diritto nazionale, se vi sono motivi ragionevoli per credere che tale cancellazione possa nuocere alla (*recte*, «possa compromettere gli interessi legittimi della») persona cui le informazioni si rife-

---

46 Cfr., in particolare, l'art. 4, par. 4, confermato dal tenore degli artt. 5 e 7.

47 *Risoluzione n. P6_TA(2006)0258*, 27 settembre 2006, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2006-0258+0+DOC+PDF+V0//IT>. La risoluzione legislativa *de qua*, sia pure approvando nel complesso la proposta della Commissione, introdurrà cospicui emendamenti, sollecitando il Consiglio a tenerne conto e ad informarlo qualora intendesse discostarsi dal testo rivisitato. In particolare, viene fatto oggetto di censura l'art. 4, par. 4, poiché, secondo il Parlamento europeo, la disciplina ivi contenuta non rispetta i criteri stabiliti dalla giurisprudenza della Corte EDU in relazione all'art. 8 CEDU: per i giudici di Strasburgo, si dice, sarebbe possibile imporre restrizioni al diritto alla privacy unicamente se ciò appare necessario in una società democratica «e non al fine di agevolare o di accelerare il lavoro delle autorità di polizia o giudiziarie». Da qui, la proposta di sostituire gli artt. 4 e 5, secondo le precise indicazioni fornite dal Parlamento stesso.

48 «Gli Stati membri prevedono specifiche garanzie supplementari per i dati biometrici e i profili DNA, al fine di garantire che: – i dati biometrici e i profili DNA vengano utilizzati solo sulla base di norme tecniche ben definite ed interoperabili; – il livello di precisione dei dati biometrici e dei profili DNA venga attentamente preso in considerazione e possa essere facilmente contestato dalla persona interessata; – sia pienamente garantito il rispetto della dignità e dell'integrità delle persone».

49 Segnatamente: *a*) se tali dati non avrebbero dovuto essere trasmessi, resi disponibili o ricevuti; *b*) dopo un termine stabilito dalla legislazione dell'altro Stato membro, se l'autorità che ha trasmesso o reso disponibili i dati in questione ha informato l'autorità ricevente di tale termine quando sono stati trasmessi o resi disponibili tali dati, a meno che i dati personali non servano ulteriormente per un procedimento giudiziario; *c*) se tali dati non sono o non sono più necessari per il fine per cui erano stati trasmessi o resi disponibili.

riscono («could affect the interests of the data subject worthy of protection»). «I dati bloccati [potranno] essere utilizzati o trasmessi solo per lo scopo per il quale non sono stati cancellati», recita l'art. 9, par. 9: formula piuttosto involuta per significare che i dati in questione potranno essere attinti soltanto quando il loro utilizzo si riveli funzionale alla tutela dell'interesse individuale che ne ha evitato la cancellazione; a qualsiasi altro scopo, quelle informazioni dovranno considerarsi *tamquam non essent*.

La proposta della Commissione si preoccupa anche di assicurare che il dato, una volta trasmesso, lasci dietro di sé una "scia elettronica" che consenta di rintracciarlo ai fini di eventuali correzioni o cancellazioni: potrebbe parlarsi di "tracciabilità" dell'informazione itinerante[50]. Al qual riguardo, non passa inosservato il fatto che, all'aumentare del numero dei *cross-border exchanges*, aumentano le difficoltà relative alla tutela dell'autodeterminazione informativa. Donde una serie di regole[51], riservata alle condizioni da rispettarsi, affinché sia legittima l'ulteriore trasmissione di dati, cioè quella che interviene tra l'originario instante-ricevente (che, ora, diviene trasmittente) e nuovi interessati. Sono così articolate discipline specifiche, via via più scrupolose e restrittive a seconda che il nuovo destinatario sia un'autorità competente di un altro Stato membro, un'autorità diversa dalle autorità competenti di uno Stato membro, un privato di un altro Stato membro, un'autorità competente di un Paese terzo o un organismo internazionale.

Un intero Capitolo viene riservato ai diritti e alle garanzie del soggetto cui i dati trattati si riferiscono, forgiando un vero e proprio statuto dell'interessato dal trattamento, che dà grande risalto alla componente "soggettiva" della tutela del dato personale[52]. *In primis*, si riserva il debito spazio al diritto all'informazione (su chi sia il responsabile del trattamento, su quali siano le finalità e la *legal basis* dello stesso, ecc.[53]), prevedendo, oltre alle regole generali, i casi di possibile deroga e teorizzando, rispetto a questi ultimi, la legittimazione dell'interessato, a fronte di presunte indebite compressioni della garanzia informativa in parola, ad adire l'autorità nazionale di controllo. Fondamentale, poi, la prospettiva del

---

50 A mente dell'art. 10, gli Stati dovranno assicurare che qualsiasi trasmissione automatica di dati personali, segnatamente mediante accesso diretto automatico, venga registrata, al fine di garantire la successiva verifica dei motivi della trasmissione, dei dati trasmessi, del momento in cui sono stati trasmessi, delle autorità coinvolte e, per quanto riguarda l'autorità ricevente, delle persone che hanno ricevuto i dati e delle persone che ne avevano fatto richiesta. Agli stessi fini, dovranno essere altresì documentati qualsiasi trasmissione e ricevimento non automatici di dati personali. L'autorità che ha registrato o documentato tali informazioni è tenuta a comunicarle immediatamente alle autorità competenti di controllo su richiesta di queste ultime.

51 Compendiate nell'apposita Sezione II del Capo III.

52 V. *supra*, § 1.

53 L'art. 19 si concentra sui «casi in cui la raccolta dei dati viene effettuata presso l'interessato e quest'ultimo ne è a conoscenza», mentre l'art. 20 contempla le fattispecie residue, in cui i dati non siano stati ottenuti dall'interessato in persona o siano stati ottenuti da esso senza che ne fosse a conoscenza o senza che fosse consapevole del fatto che i dati raccolti lo riguardassero.

diritto di accesso, delineata dall'art. 21, che impone agli Stati membri di garantire a qualsiasi persona interessata di ottenere dal responsabile del trattamento: *a*) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi, la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono stati comunicati i dati; *b*) la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati; *c*) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della decisione quadro, in particolare a causa del carattere incompleto o inesatto dei dati stessi; *d*) la notificazione a terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera *c*), se non si dimostra che è impossibile o implica uno sforzo sproporzionato[54]. Sono tuttavia previste anche ampie deroghe ai diritti in parola, in genere da giustificarsi ad opera del responsabile del trattamento; l'autorità di controllo potrà adirsi ove si sospetti una violazione delle regole *de quibus*.

Restando sul versante dell'interesse "soggettivo" alla tutela del dato, non va dimenticato che, in seno alla summenzionata risoluzione legislativa del settembre 2006, il Parlamento europeo proporrà, a mezzo di un emendamento, l'introduzione di un'ulteriore disciplina *lato sensu* garantistica: poiché l'esperienza dimostra che è sempre più frequente il trattamento automatizzato di dati personali, viene affrontato il problema delle decisioni basate unicamente su trattamenti automatizzati dei dati stessi[55]. Il Parlamento, infatti, reputa che tali decisioni debbano essere sottoposte a condizioni e a misure di protezione molto rigorose quando producano concrete ripercussioni sulla sfera giuridica di una persona. In particolare, dovrebbero essere consentite soltanto in via di eccezione, in casi tassativamente previsti dalla legge e dovrebbero apprestarsi misure adeguate, volte a proteggere gli interessi della persona coinvolta[56].

---

54 Giusta l'art. 22, gli Stati membri dispongono affinché vengano prese misure adeguate per garantire che, nei casi in cui il responsabile del controllo rettifichi, blocchi o cancelli dati personali a seguito di una richiesta, venga elaborato automaticamente un elenco dei fornitori e dei destinatari di tali dati. Il responsabile del controllo è tenuto a garantire che le persone presenti in tale elenco vengano informate dei cambiamenti effettuati riguardo ai dati personali.

55 Per un inquadramento del tema, leggasi F. Martines, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'Unione europea*, in "Rivista italiana di diritto pubblico comunitario", 2000, p. 719.

56 In questa prospettiva, viene concepito un nuovo art. 22-*bis*, che merita di essere riportato testualmente: «Gli Stati membri concedono il diritto a ogni persona di non essere soggetta a una decisione o azione che produca effetti giuridici che la riguardino o che la interessino in modo significativo e che sia basata soltanto sull'elaborazione automatizzata di dati allo scopo di valutare alcuni aspetti personali che la riguardano, come la sua affidabilità, il suo comportamento, ecc. 2. Fatti salvi gli altri articoli della presente decisione quadro, gli Stati membri stabiliscono

Cambia decisamente la visuale prospettica, quando viene in gioco il tema della sicurezza e della riservatezza del trattamento, che pone alla ribalta (anche) l'interesse "oggettivo" della tutela del dato personale[57]. La Commissione si sofferma, infatti, sulla necessità che i dati non siano esposti al rischio di accessi indesiderati, modifiche ad opera di soggetti non legittimati *et similia*. Interessante, al proposito, la regola generale secondo cui l'incaricato del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento, non deve elaborare i dati personali ai quali ha accesso, se non dietro istruzione del responsabile stesso, oppure in virtù di obblighi giuridici[58]. Tutti coloro che lavorano con un'autorità competente di uno Stato membro o al suo interno sono vincolati da norme severe di riservatezza.

Da ultimo, la proposta di decisione quadro non si risparmia nell'apprestare tutela sul piano sanzionatorio, vuoi civilistico, vuoi penalistico, a fronte di trattamenti illeciti. Sul primo versante, gli Stati membri dovranno far sì che chiunque subisca un danno, cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della decisione quadro in commento, abbia il diritto di ottenere il risarcimento del pregiudizio subìto dal responsabile del trattamento. Quest'ultimo potrà essere esonerato in tutto o in parte da tale responsabilità soltanto se sarà in grado di dimostrare che l'evento dannoso non gli è imputabile. Significativo che un'autorità competente, che abbia ricevuto i dati personali da oltre confine, si riterrà "oggettivamente" responsabile nei confronti del soggetto leso per i danni causati dall'uso di dati imprecisi e non aggiornati: non potrà cioè escludere la propria responsabilità, giustificandola con il fatto che i dati ricevuti erano *ab origine* imprecisi o non aggiornati. Ove ciò accada, tuttavia, l'autorità competente che li ha trasmessi dovrà risarcire completamente l'importo pagato per tali danni dall'autorità ricevente. Sul fronte penalistico, i Paesi membri dovranno adottare le misure appropriate per garantire la piena applicazione delle disposizioni della decisione quadro e, in particolare, dovranno prevedere sanzioni efficaci, commisurate e dissuasive, da applicare in caso di violazione delle disposizioni di attuazione in parola. Più in dettaglio, gli Stati membri sono chiamati a comminare sanzioni penali efficaci per i reati

---

che una persona può essere soggetta a una decisione del tipo a cui si fa riferimento al paragrafo 1, solo se tale decisione o azione è autorizzata da una legge che stabilisca anche misure di salvaguardia degli interessi legittimi dell'interessato, come mezzi facilmente disponibili che gli permettano di essere informato in merito alla logica relativa all'elaborazione automatica di dati che lo riguardano e di esporre il suo punto di vista, a meno che ciò non sia incompatibile con gli scopi per cui i dati sono stati elaborati».

57 V. *supra*, § 1.

58 L'art. 2 lett. *d*) definisce «responsabile del trattamento» la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. «Incaricato del trattamento», *ex* art. 2 lett. *e*), è, invece, la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento.

commessi intenzionalmente che comportino violazioni gravi delle disposizioni adottate conformemente alla decisione quadro, segnatamente le disposizioni finalizzate a garantire la riservatezza e la sicurezza del trattamento.

La Commissione non manca poi di contemplare a chiare lettere l'obbligo per gli Stati di ammettere ricorsi giurisdizionali: fatti salvi i ricorsi amministrativi che possono essere esperiti, di regola dinanzi all'autorità di controllo di cui all'art. 30, prima che sia adita l'autorità giudiziaria, gli Stati membri sono invitati ad assicurare il diritto di chiunque a presentare un ricorso giurisdizionale in caso di violazione di prerogative garantitegli dal diritto nazionale applicabile, ai sensi della decisione quadro, al trattamento in questione.

Infine, è previsto che ogni Stato membro incaricherà una o più autorità pubbliche di sorvegliare, nel proprio territorio, l'applicazione delle disposizioni di attuazione della decisione quadro, adottate dallo stesso Stato membro, autorità che dovranno essere pienamente indipendenti nell'esercizio delle funzioni loro attribuite. Svariati i poteri delle autorità di controllo, delle quali la proposta di decisione quadro statuisce tra l'altro che: *a*) abbiano poteri investigativi, come la facoltà di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio delle loro funzioni di controllo; *b*) siano titolari di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti e di dar loro adeguata pubblicità, o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i parlamenti o altre istituzioni politiche nazionali; *c*) abbiano il potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della decisione quadro ovvero di adire per dette violazioni le autorità giudiziarie. È inoltre sancito che le autorità di sorveglianza cooperano tra loro e con le autorità di controllo di cui al Titolo VI TUE, nonché con il Garante europeo della protezione dei dati nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.

4. La proposta di decisione quadro della Commissione sullo scambio d'informazioni in virtù del principio di disponibilità (COM (2005) 490 def.)

Come anticipato, nell'ottobre 2005 la Commissione prende una seconda iniziativa[59], ispirata al paradigma concettuale secondo cui le informazioni necessarie

59 COM (2005) 490 def., 12 ottobre 2005, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0490:FIN:IT:PDF>, niente affatto indifferente alle contingenze storiche. La Relazione al testo, infatti, spiega che il Consiglio GAI del 13 luglio 2005, riunitosi in sessione straordinaria dopo gli attentati terroristici del 7 luglio a Londra, ha chiesto alla Commissione di anticipare la presentazione della proposta sul principio di disponibilità, onde fornire all'Unione

per prevenire e reprimere i reati devono poter valicare agevolmente le frontiere interne dell'Unione.

Si intende, in pratica, eliminare l'incertezza dei meccanismi di scambio tradizionali, basati sul diritto dello Stato interpellato: gli Stati UE sono chiamati a "condividere" i dati con gli altri Paesi membri e con Europol. Più precisamente, il progetto ideato dalla Commissione intende garantire alle singole autorità di contrasto degli Stati membri, oltreché ai funzionari di Europol, l'accesso alle informazioni di *law enforcement* detenute da altri Paesi, seguendo due percorsi alternativi: permettendone la consultazione integrale e diretta on-line, ovvero assicurando l'accesso on-line ai soli dati di indice, cui potrà seguire una richiesta di trasmissione delle informazioni correlate al *reference index* che abbia fornito un proficuo riscontro. Tutto ciò, senza obliare il rispetto della privacy e la protezione dei dati di carattere personale. Secondo la Commissione, infatti, il trattamento dei dati personali ai sensi della decisione quadro «avverrà [...] in conformità della decisione quadro 2006/XX/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale»[60]. Con una sorta di meccanismo autoreferenziale, insomma, la Commissione europea chiude il cerchio: la proposta di decisione quadro sul principio di disponibilità rinvia espressamente alla (ipotizzata) decisione quadro sulla tutela del dato, che dovrebbe germinare, negli auspici dell'istituzione europea, dalla propria iniziativa in materia, avanzata con qualche giorno di anticipo.

Stando alla Relazione che accompagna la proposta n. 490 del 2005, la forma di cooperazione ivi delineata va al di là dello scambio d'informazioni previsto dalla Convenzione di Schengen e non rientra nel correlativo *acquis* (com'è noto, introdotto nell'Unione europea da un Protocollo allegato al Trattato di Amsterdam); pertanto, non ne costituisce formalmente uno sviluppo, rappresentando viceversa una radicale innovazione[61]. La Commissione richiama espressamente l'art. 39 della Convenzione di applicazione degli accordi di Schengen per osservare come esso contempli, sì, uno scambio di informazioni (su richiesta) tra le forze di polizia, ma non imponga agli Stati interpellati di rispondere. Sicché, alle lungaggini procedurali si aggiunge il carattere aleatorio dei risultati. Per di più, le domande e le risposte vengono inoltrate attraverso le autorità centrali e gli scambi diretti tra i funzionari competenti avvengono solo in casi eccezionali. Diversamente, la proposta in commento privilegia i canali diretti per lo scambio di informazioni

---

gli strumenti di cooperazione necessari per prevenire e combattere il terrorismo in modo più efficace.

60 Così recita il testo della Relazione alla proposta, ma cfr. anche i "considerando" nn. 5, 11, 19 e 20, nonché gli artt. 8, 17 e 18.

61 Merita precisarsi che un'impostazione diversa si ritrova nella Relazione che accompagna COM (2005) 475 def. in tema di protezione dei dati personali; vedasi, colà, il "considerando" n. 31.

e prevede un obbligo generalizzato di *information sharing*, fatto salvo un numero limitato di motivi di rifiuto armonizzati.

La Commissione si riferisce espressamente, in virtù della contiguità contenutistica, anche all'iniziativa del Regno di Svezia[62] e al Trattato di Prüm[63], ammettendo che il progetto svedese riesce nell'intento di armonizzare il contesto legislativo per lo scambio di dati e a contenere i tempi di risposta. Tuttavia, reputa che la proposta ora in commento renda più mirata la ricerca dei dati, consentendo di accertare previamente la disponibilità delle informazioni, onde formulare domande di accesso meglio strutturate. I motivi di rifiuto vengono inoltre tipizzati, cosicché l'incertezza legata alle richieste di informazioni è ridotta al minimo. Quanto al Trattato di Prüm, la Commissione, pur riscontrando svariate similitudini con la propria iniziativa (*in apicibus*, il sistema di indice), giudica la seconda più funzionale alle esigenze dell'Unione europea, posto che il primo risulta «more limited in scope», oltre che sottoscritto, almeno in origine, solo da sette Stati membri.

Degno di nota il fatto che, nella Relazione illustrativa, la Commissione si riferisca testualmente alle autorità «di contrasto» («law enforcement authorities», «law enforcement officer») e alla fase definita «pre-processuale» («pre-trial phase») o «che precede l'avvio di un procedimento giudiziario» («prior to the commencement of a prosecution»[64]), sollevando dubbi interpretativi – sulla natura delle autorità coinvolte e sui profili funzionali dell'*information sharing* – che rievocano quelli destati dalla nomenclatura del Programma dell'Aia[65].

Tuttavia, sul versante dei soggetti coinvolti, in forza dell'individuazione della base giuridica dell'iniziativa nel solo art. 30 TUE, con esclusione dell'art. 31 TUE, è possibile asserire che l'iniziativa della Commissione concepisce il principio di disponibilità come un fenomeno che coinvolge direttamente le autorità di polizia, non quelle giudiziarie (che, quindi, potranno beneficiarne solo mediatamente[66]). Nello stesso senso depone l'art. 3, lett. *b*), ove il concetto di «autorità competente» viene *claris verbis* ricondotto al solo primo trattino dell'art. 29 TUE (oltre che ad Europol), *id est* a quello riservato alle forze di polizia e alle autorità doganali.

Quanto all'area d'impatto del principio di disponibilità, rileva la precisazione secondo cui lo scambio transfrontaliero di informazioni è finalizzato, tanto alla prevenzione del crimine («prevention […] of criminal offences»), quanto

62 Su cui v. *infra*, § 7.

63 Cfr. *infra*, § 8.

64 V. anche l'art. 2, par. 1.

65 V. *supra*, § 2.

66 Del resto, l'art. 2, par. 4, sancisce che le disposizioni della decisione quadro in commento lasciano impregiudicati gli strumenti applicabili all'assistenza giudiziaria reciproca o al riconoscimento reciproco delle decisioni in materia penale.

all'«individuazione e [al]l'investigazione dei reati prima che inizi il procedimento giudiziario»[67].

Perciò, si può concludere che il progetto elaborato della Commissione contempla una disponibilità informativa che coinvolge le autorità di polizia, sia sul fronte della prevenzione dei reati, che su quello investigativo. Viceversa, esclude le autorità giudiziarie e, sul piano funzionale, la fase processuale in senso stretto, cioè quella successiva all'elevazione dell'accusa. Più precisamente, i "considerando" nn. 10 e 19 sanciscono che l'autorità competente, ottenute le informazioni da oltre confine, potrà utilizzarle esclusivamente «allo scopo per il quale sono state fornite» (*rectius*, a mente dell'art. 7, «solo per la prevenzione, l'individuazione e l'investigazione dei reati per i quali sono fornite») e comunque non potrà utilizzarle «come prova di un reato», senza l'autorizzazione preventiva di un'autorità giudiziaria dello Stato membro d'origine[68]. Da ciò, è lecito desumere un ferreo vincolo di destinazione: di regola (*id est*, salvo un'espressa autorizzazione ad opera dell'autorità giudiziaria dello Stato trasmittente), l'informazione ottenuta da oltre confine non sarà utilizzabile come prova nel corso di un processo *stricto sensu* (al qual riguardo, non sembra fuori luogo evocare, sia pure con i dovuti accorgimenti, il concetto, ben noto all'interno del nostro ordinamento processuale, di cause di inutilizzabilità "fisiologica" o "funzionale"), mentre rileverà ai fini di operazioni di *intelligence*, intese a scongiurare la commissione di un reato o a scoprire determinate attività illecite[69], ovvero nella fase delle indagini preliminari, quando il lavoro è incentrato su una *notitia criminis*. Anche in questi frangenti, tuttavia, non mancano le barriere ostative: nella fase di prevenzione o d'indagine, l'utilizzabilità sarà limitata alle attività di *law enforcement* direttamente connesse alle esigenze che hanno suffragato l'originaria richiesta, giusta il principio di "finalità limitata".

In questo contesto va ricordato anche l'art. 12, contemplante eventuali "istruzioni per l'uso" che l'autorità trasmittente voglia fornire al quella instante. È, infatti, previsto che la prima, nel rispondere, possa apporre dei limiti vincolanti all'uso delle informazioni trasmesse, se vengono in gioco determinate esigenze, tassativamente descritte: evitare di compromettere il buon esito di un'indagine in corso; tutelare una fonte di informazioni o l'integrità fisica di una persona; tutelare la riservatezza delle informazioni a un qualsiasi stadio del trattamento. Degno di attenzione il fatto che questa triade può essere invocata anche a un fine diverso, cioè quello di rifiutare *tout court* la trasmissione del dato: così dispone l'art. 14, che (si avrà modo di vederlo in seguito) aggiunge una quarta, possibile causa di rifiuto.

---

67 Cfr. il "considerando" n. 6 e l'art. 1, par. 1.

68 Art. 13, par. 2.

69 Per le dovute puntualizzazioni sul significato da ascriversi al concetto di "*intelligence*" nelle fonti europee oggetto di questo studio, v. *amplius infra*, § 7.

Quanto alle modalità di circolazione delle informazioni, è data un'alternativa.

Da un lato, si collocano le banche dati nazionali, contenenti informazioni che sono accessibili on-line per le autorità di polizia dello Stato membro. In questa ipotesi, tali archivi dovranno essere resi accessibili on-line anche alle autorità competenti omologhe degli altri Stati membri e ad Europol: una sorta di transustanziazione, in virtù della quale l'archivio, da nazionale, diviene europeo, in quanto direttamente compulsabile per via telematica, tanto dalle autorità dello Stato d'origine, quanto dalle omologhe d'oltre confine.

Sull'altro fronte, l'ipotesi in cui, nel territorio dello Stato d'origine, archivi, contenenti informazioni di *law enforcement*, siano, sì, accessibili ad opera delle autorità di polizia nazionali, ma non a mezzo di accesso diretto on-line. In tal caso, gli Stati dovranno assicurare che le autorità competenti omologhe straniere ed Europol abbiano un accesso on-line ai dati di indice relativi alle informazioni contenute negli archivi in parola, dati di indice che saranno consultabili mediante una *routine* di ricerca. Lo scopo è quello di assicurare che, ad esito di quest'ultima, l'autorità interessata rilevi se, oltre confine, esistono o meno dati di indice corrispondenti a quelli oggetto di attenzione. Nell'ipotesi affermativa, l'*index data* specificherà la tipologia delle informazioni di riferimento e l'autorità designata che le controlla o le gestisce. Questa, cui dovrà rivolgersi un'apposita domanda di accesso alle informazioni, sarà tenuta a rispondere entro termini prestabiliti, fornendo le informazioni all'autorità straniera richiedente[70], oppure spiegando perché non è in grado di fornirle o non è in grado di fornirle immediatamente. Laddove, a norma della legislazione nazionale, il trasferimento delle informazioni debba essere autorizzato da un'autorità diversa da quella che le controlla, spetterà a quest'ultima attivarsi, onde ottenere l'autorizzazione per conto dell'organo di contrasto dell'altro Stato membro che ha bisogno delle informazioni. In generale, il trasferimento a seguito di una domanda di informazioni sarà un atto dovuto: potrà essere rifiutato esclusivamente per i motivi tassativamente indicati dall'art. 14 (evitare di compromettere il buon esito di un'indagine in corso; tutelare una fonte di informazioni o l'integrità fisica di una persona; tutelare la riservatezza delle informazioni a un qualsiasi stadio del trattamento; tutelare i diritti e le libertà fondamentali delle persone i cui dati sono oggetto di trattamento), ciò che differenzia sensibilmente l'apparato circolatorio in esame da quello concepito dagli accordi di Prüm, in cui la seconda fase – quella successiva alla richiesta, inoltrata all'autorità che controlla o gestisce le informazioni – rimane regolata dalle norme che sovrintendono alla cooperazione giudiziaria internazionale[71].

---

70 Se del caso, lo si è già segnalato nel testo, subordinando l'uso delle informazioni a istruzioni vincolanti per l'autorità competente che ha presentato la domanda.

71 V. *infra*, § 8.

Questa combinazione fra accesso diretto on-line alle informazioni e consultazione dei dati indice (seguita dall'eventuale domanda di integrazione) sembra tradurre in atto, in modo efficace e convincente, un'esigenza primaria nel quadro della cooperazione *cross-border*: quella di consentire ad un'autorità di polizia un'agevole identificazione oltre confine dell'esistenza di informazioni utili ai fini dello svolgimento dei propri compiti. Si assicura, cioè, la "*visibility*" del dato, fattore strategicamente decisivo in una politica di *information sharing*: come si avrà modo di chiarire meglio in seguito[72], né l'iniziativa del Regno di Svezia, né la decisione quadro n. 960 del 2006 si rivelano altrettanto efficaci sotto questo prospetto, mentre un giudizio positivo meritano *in parte qua* gli accordi di Prüm e, conseguentemente, la decisione 2008/615/GAI, in virtù delle procedure di consultazione o comparazione poste in essere dai punti di contatto nazionali.

Ma la proposta di decisione quadro in commento non si rivela attenta soltanto alla "*visibility*" del dato, riconoscendo anche un'ampia "*readability*" dello stesso, facilitando cioè un compiuto apprendimento dell'informazione archiviata: quest'ultima, o è resa direttamente accessibile on-line, oppure, una volta che il *reference index* ne abbia svelato l'esistenza, deve essere comunicata a seguito di apposita domanda, i motivi di rifiuto risultando tassativamente predeterminati dall'art. 14. Sotto questo prospetto, l'iniziativa svedese e la decisione quadro n. 960 si distinguono per un tratto molto marcato, in quanto non contemplano forme di accesso diretto on-line ai database nazionali, bensì fanno leva sul meccanismo della domanda e della risposta (prevedendo motivi tassativi di rifiuto). Quanto agli accordi di Prüm, vi si è fatto cenno poco sopra, la fase successiva alla richiesta, inoltrata all'autorità che controlla o gestisce le informazioni, rimane regolata dalle norme che sovrintendono alla cooperazione giudiziaria internazionale.

È perciò possibile concludere che, seguendo lo scorcio prospettico della visibilità (*visibility*) e dell'accesso (*readability*) all'informazione, la proposta di decisione quadro n. 490 del 2005 si dimostra innovativa, audace ed efficace, distinguendosi sotto più di un profilo dalle altre iniziative che, a partire dal 2004, si affacciano sulla scena europea nell'orbita del principio di disponibilità.

Affinché il meccanismo ideato dalla Commissione funzioni, agli Stati membri viene richiesto di notificare alla stessa, entro un breve termine dall'entrata in vigore della decisione quadro, un compendio piuttosto ricco d'indicazioni, concernenti l'assetto interno delle autorità "di contrasto" e di quelle "designate"[73]: questa

---

72 *Infra*, § 7 segg.

73 *In primis*, quali siano, nei rispettivi territori, le «autorità competenti» (cioè le autorità di polizia), indicandone le competenze specifiche previste dalla legislazione nazionale. Inoltre, dovranno indicarsi le «autorità designate» per ciascun tipo di informazioni o di dati di indice connessi, nonché il depositario di ciascun tipo di informazioni e dei relativi dati di indice, insieme alle modalità di accesso a ciascun tipo di informazioni e di dati, precisando in particolare se le informazioni siano accessibili on-line. Gli Stati dovranno precisare lo scopo per il quale ciascun tipo di informazioni può essere trattato nel territorio nazionale e le competenze delle

operazione serve anzitutto a ricostruire, Stato per Stato, le trame dei rapporti tra autorità di polizia e informazioni di *law enforcement*. Ma non solo. Negli intendimenti della Commissione, infatti, questa formalità si rivela funzionale anche allo scopo, ulteriore, di instaurare una precisa corrispondenza biunivoca fra autorità omologhe di Stati diversi. Più precisamente, non appena le suddette istruzioni siano disponibili rispetto ai vari Paesi europei, diventa possibile elaborare una "tavola di equivalenza" tra autorità di contrasto[74] e, quindi, specificare: *a*) per ciascun tipo di informazioni accessibile on-line alle autorità nazionali competenti di uno Stato membro, quali autorità degli altri Stati membri (con competenze equivalenti) siano autorizzate ad accedervi on-line, nel pieno rispetto dello scopo per il quale le informazioni vengono trattate nello Stato d'origine; *b*) per ciascun tipo di dati di indice, connessi alle informazioni di *law enforcement* accessibili alle autorità nazionali competenti di uno Stato membro, quali autorità competenti degli altri Stati UE, avendo competenze equivalenti, siano autorizzate a consultare l'indice.

Non è da escludere che sia questo il vero punto debole della proposta in esame: tenere ferma una rigida ripartizione delle sfere di competenza e funzionali delle autorità di *law enforcement* anche quando esse si adoperano nella ricerca oltre confine di informazioni utili allo svolgimento dei propri compiti istituzionali. Vero che l'opzione sembra rispondere a un'esigenza di par condicio (diversamente, si finirebbe per riconoscere alle autorità straniere un potere di accesso alle banche dati nazionali più ampio e generalizzato di quello spettante alle autorità interne), ma questa logica dell'alter ego d'oltre confine non sembra ascrivere il giusto peso alle difficoltà e alle complicazioni cui si va incontro quanto la ricerca e l'apprendimento di informazioni deve avvenire in un contesto in cui i fattori linguistico, culturale e, soprattutto, tecnico-giuridico differiscono da quelli "d'origine" per l'autorità di polizia impegnata nell'indagine.

Da ultimo, ma non certo per importanza, il ruolo che, entro questa cornice, riveste l'Allegato II alla proposta di decisione quadro, contemplante i «tipi di informazioni che possono essere ottenuti [...] per la prevenzione, l'individuazione e l'investigazione dei reati». Infatti, l'iniziativa in commento, oltre a concentrare l'attenzione sulla cooperazione di polizia (relegando fuori campo l'autorità giudiziaria), non teorizza una disponibilità informativa "a tutto tondo", bensì la limita a specifiche categorie di dati[75] e cioè: ai profili DNA, alle impronte digitali, ai dati balistici, ai veicoli immatricolati, ai numeri di telefono e agli altri dati relativi alle

---

autorità dello Stato membro che possono ottenere le informazioni a norma della legislazione nazionale. Se la comunicazione delle informazioni è subordinata all'autorizzazione preventiva di una data autorità, dovrà indicarsi anche quest'ultima, unitamente alla procedura applicabile. Se del caso, dovrà specificarsi il canale per il trasferimento di ciascun tipo di informazioni a cui si riferiscono i dati di indice.

74 Cfr. l'art. 5, che rinvia ai criteri stilati nell'apposito Allegato III.

75 Cfr. l'art. 3 lett. *a*).

comunicazioni (escluso il contenuto), ai dati minimi per l'identificazione delle persone iscritte nei registri anagrafici. È quindi rispetto a queste sole *species* di informazioni che, negli intendimenti della Commissione, gli Stati membri dovrebbero provvedere affinché le autorità competenti omologhe degli altri Paesi membri ed Europol possano accedere direttamente on-line, ovvero (se le informazioni non sono *ex se* contenute in banche dati elettroniche compulsabili "in rete") accedere ai dati di indice, in vista dell'eventuale formulazione di richieste di ulteriori informazioni.

Questa forma di disponibilità "selettiva" rievoca il Trattato di Prüm, ove l'attenzione è polarizzata su profili DNA, *fingerprints* e veicoli. Non va, però, dimenticato che il Trattato contempla espressamente per i firmatari un obbligo di istituzione di tre banche dati centralizzate (a livello nazionale) compendianti tutti i dati di indice DNA, *fingerprints* e veicoli, mentre l'iniziativa della Commissione affianca alla ricerca su archivi che raccolgono i *reference index*, la possibilità dell'accesso immediato on-line alle informazioni disponibili.

Infine, una puntualizzazione in merito alle categorie di informazioni destinate alla circolazione in virtù del principio di disponibilità. L'Allegato II alla proposta di decisione quadro in commento, nel riferirsi ai profili DNA, precisa trattarsi di un codice alfanumerico stabilito in base ai sette marcatori del DNA della serie europea standard, definiti in una risoluzione del Consiglio del 25 giugno 2001, sullo scambio dei risultati delle analisi del DNA[76]. Il fatto che i marcatori non contengano informazioni su specifiche caratteristiche ereditarie è opzione che verrà valutata positivamente dal Garante europeo per la protezione dei dati, nel parere, reso il 28 febbraio 2006[77], sulla proposta in commento. Ivi il GEPD rimarcherà con forza l'importanza di distinguere il concetto di "profilo" da quello di "campione" di DNA. Infatti, i campioni, spesso prelevati e conservati dalle autorità di *law enforcement*, devono essere considerati particolarmente "sensibili", in quanto possono più facilmente contenere l'intero corredo genetico e, quindi, fornire informazioni – sulle caratteristiche genetiche e sullo stato di salute di una persona – in potenza del tutto estranee agli scopi di prevenzione o repressione dei reati. I profili di DNA contengono, invece, soltanto alcune informazioni parziali, estratte dal campione di DNA: esse possono essere utilizzate per verificare l'identità di una persona, ma, in linea di massima, non ne rivelano le caratteristiche genetiche. Tuttavia, osserva condivisibilmente il Garante, non va dimenticato che i progressi scientifici tendono ad accrescere sensibilmente il numero di informazioni ricavabili dai singoli profili; cosicché, quello che in un dato momento è considerato, dal punto di vista della privacy, un profilo di DNA "innocuo", può, col passare del tempo, divenire la fonte di informazioni incalcolabili *ab origine*. Le informazioni che possono essere ottenute dai profili di DNA,

76 La risoluzione è pubblicata in *GUCE*, C 187, 3 luglio 2001, p. 1.

77 Pubblicato in *GUUE*, C 116, 17 maggio 2006, p. 8.

pertanto, andrebbero sempre considerate come variabili "dinamiche", il che impone, *in subiecta materia*, di usare una particolare cautela sul fronte della raccolta e dell'archiviazione.

5. La decisione quadro in materia di protezione dei dati personali (2008/977/GAI): la tortuosità dell'itinerario di adozione e il progressivo depauperamento contenutistico

Per quanto sinora visto, è facile convenire sul fatto che, a circa un anno di distanza dal Consiglio europeo di Bruxelles, l'itinerario attuativo del Programma dell'Aia si presentava, sul fronte dell'*information sharing*, come una strada in discesa: elaborato dalla Commissione e dal Consiglio, nell'estate del 2005, un esaustivo Piano d'azione, nell'ottobre dello stesso anno due proposte di decisione quadro, pressoché coeve, venivano rivolte dalla Commissione al Consiglio dell'Unione. È del 4 ottobre 2005 la proposta relativa alla protezione dei dati personali, trattati nelle materie rientranti nel c.d. terzo pilastro dell'Unione europea; del 12 ottobre, quella concernente il principio di disponibilità. Il sia pur minimo divario temporale rivelava un preciso significato, perché la proposta più recente (concernente il principio di disponibilità) si rifaceva *claris verbis* alla prima, ai fini della identificazione delle garanzie di contesto essenziali per la tutela dell'autodeterminazione informativa, da assicurarsi proprio rispetto ai dati circolanti giusta il principio di disponibilità. Con queste coordinate di riferimento, il Programma dell'Aia risultava rispettato, non solo per quanto riguarda la tempistica delle iniziative volte ad attuarlo, ma anche rispetto alla precedenza che veniva accordata alla tutela del dato personale rispetto alla politica della disponibilità informativa.

Sennonché, facendo un balzo temporale in avanti di tre anni, si deve prendere atto che le rosee previsioni, facilmente elaborabili nell'ottobre 2005, sono state in parte contraddette. Infatti, fino all'autunno 2008, sul piano della tutela del dato personale (negli auspici, il primo a doversi consolidare), si registrerà un disarmante "nulla di fatto".

Di primo acchito, è facile imputare l'inerzia legislativa alla difficoltà, per gli esecutivi nazionali, di raggiungere un accordo unanime (necessario *ex* art. 34, par. 2, TUE) in un settore, quello della lotta al crimine, in cui la tutela dell'autodeterminazione informativa può essere percepita come un ingombrante ostacolo. Tuttavia, a spiegare l'inconcludenza in questa materia concorrono anche motivi di matrice diversa. Va detto, infatti, che, col passare del tempo, intorno al problema della protezione dei dati personali in seno al "terzo pilastro" dell'Unione europea ha finito per coagularsi una massa proteiforme di iniziative e provvedimenti di varia natura che, inevitabilmente, ha complicato il quadro normativo su cui avrebbe dovuto convergere il voto del Consiglio: oltre a tre pareri del Garante europeo della protezione dei dati personali e a quattro interventi delle *European data protection authorities*, si annoverano tre risoluzioni legislative del Parlamento

europeo e una cinquantina di interventi riconducibili alla Presidenza del Consiglio UE.

Per capire cosa abbia determinato una simile frenesia, conviene muovere da una nota diffusa dalla Presidenza del Consiglio dell'Unione il 13 ottobre 2006, in cui ci s'interroga sull'area d'impatto della proposta di decisione quadro COM (2005) 475[78]. In particolare, si tratta di chiarire se vi rientri anche il trattamento delle informazioni di *law enforcement* interno ai confini nazionali dei singoli Stati membri. Interrogativo più che giustificato, dato che, ad esempio, i "considerando" da 10 a 13, l'art. 1 e l'intero Capo III[79] della proposta n. 475 sembrano deporre in senso nettamente contrario. La Presidenza mette così alla ribalta un problema che era già stato còlto dal Garante europeo per la protezione dei dati, nell'ambito del primo parere adottato in materia[80], e rimarcato dal Parlamento europeo, nella propria risoluzione legislativa del settembre 2006: ivi, gli emendamenti da 24 a 42 stravolgevano il Capo III della proposta di decisione quadro della Commissione, assegnando un peso decisivo al problema concernente la circolazione delle informazioni di *law enforcement* all'interno dei confini nazionali, problema che affianca quello dei *cross-border exchanges* e che, per molti versi, da questo si diversifica. Perspicui, nell'intervento della Presidenza, l'intitolazione del relativo paragrafo («Only international or also domestic processing of data?»), nonché l'interrogativo e l'invito con cui l'intervento si conclude: «Do delegations agree that all provisions from the DPFD, with the exception of Articles 9, 10, 11, 15 and 18, should apply to domestic data processing?».

Ciò che preme rimarcare è che questa prospettiva, di sostanziale ripensamento dei contenuti e, soprattutto, del grado di pervasività della decisione quadro, diviene il *Leitmotiv* delle successive vicende interistituzionali in tema di autodeterminazione informativa. A cominciare dalla primavera del 2007, la Presidenza del Consiglio dell'Unione europea emette, in rapida sequenza, una serie di documenti[81], ciascuno dei quali contenente la bozza (volta a volta rielaborata) di una nuova proposta di decisione quadro del Consiglio «on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters»[82]. Il che val quanto dire che, col trascorrere del tempo, rispetto al "terzo

78 *Documento del Consiglio n. 13918/06*, 13 ottobre 2006, <http://www.statewatch.org/news/2006/oct/eu-dp-issues-13918-06.pdf>.

79 Artt. da 8 a 18.

80 Il parere è del 19 dicembre 2005 (in *GUUE*, C 47, 25 febbraio 2006, p. 27). Secondo il Garante, è «essenziale che la decisione quadro, per conseguire il suo obiettivo, riguardi tutti i dati giudiziari e di polizia, anche se tali dati non sono trasmessi o messi a disposizione dalle autorità competenti di altri Stati membri».

81 Datati 13 marzo, 13 luglio, 1°, 12 e 16 ottobre, 11 dicembre 2007, 24 giugno 2008.

82 Gli stessi Garanti della protezione dei dati, riunitisi a Cipro l'11 maggio 2007, preciseranno di essere informati della seria discussione in corso, circa l'ambito di applicazione della proposta decisione quadro («Should it apply only to data exchanged between Member States or should

pilastro" dell'Unione europea si sono venute profilando la stesura e l'approvazione di una disciplina generale della protezione dei dati innovativa rispetto a quella dell'ottobre 2005.

In che modo gli scenari siano progressivamente cambiati, lo si evince, anzitutto, dalla bozza di proposta di decisione quadro formulata dalla Presidenza del Consiglio UE il 13 marzo 2007[83]. A livello di "considerando", ivi si afferma che «Member States will also apply the rules of the Framework Decision to national data-processing, in order that the conditions for transmitting data may already be met when the data are collected»[84]; e si aggiunge che «The Framework Decision also aims to combine the existing data protection supervisory bodies, which have hitherto been established separately for the Schengen Information System, Europol, Eurojust, and the third-pillar Customs Information System,

---

it apply to all processing activities by police and judicial authorities»). Premesso che, limitando l'area d'impatto della decisione quadro ai dati che vengono o possono venir scambiati tra Stati membri, si corre il rischio che il campo di applicazione della decisione stessa risulti alla fine particolarmente malsicuro e incerto, i Garanti affermeranno con forza «that only a comprehensive scope covering all types of processing of personal data could provide individuals with the necessary protection» (<http://www.statewatch.org/news/2007/may/eu-dpa-declaration-may-cyprus.pdf>). Ad esito della summenzionata riunione, i Garanti adotteranno una "posizione comune" «on the use of the concept of availability in law enforcement», la quale culmina in uno schema di sintesi, configurato come una sorta di questionario funzionale a orientare un giudizio su qualsiasi misura intesa a realizzare il concetto di disponibilità nel contesto di *law enforcement* (<http://www.cnpd.pt/bin/relacoes/declaration.pdf>). Gioverà anche ricordare che, il 29 novembre 2006, il Garante europeo della protezione dei dati era tornato sull'argomento (dopo l'opinione del dicembre 2005), formulando un secondo parere (in *GUUE*, C 91, 26 aprile 2007, p. 9). Nell'occasione, il GEPD si diceva preoccupato per la direzione che i lavori stavano prendendo. I testi in discussione nell'ambito del Consiglio, infatti, non tenevano conto, secondo il Garante, degli emendamenti proposti dal Parlamento europeo nel settembre 2006 (menzionati *supra*, § 3) e dei pareri espressi dal GEPD medesimo, oltre che dalla Conferenza delle autorità europee per la protezione dei dati: in alcuni casi, le disposizioni della proposta della Commissione, che prevedevano essenziali garanzie per i cittadini, risultavano addirittura soppresse o fortemente svuotate di contenuti. Da qui, il timore che il livello di protezione risultasse inferiore a quello assicurato dalla direttiva 95/46/CE o anche dalla più generica Convenzione n. 108 del 1981 (che pure è vincolante per gli Stati membri del Consiglio d'Europa), tanto da indurre il Garante a raccomandare al Consiglio di riservare maggior tempo ai negoziati, allo scopo di raggiungere un risultato in grado di offrire una protezione sufficiente. Fra l'altro, non può sfuggire che, tra i vari nervi scoperti rimarcati (qualità dei dati, finalità limitata, diritti delle persone interessate dal trattamento, scambio di dati con privati o autorità di Paesi terzi, ruolo delle autorità responsabili della protezione dei dati, regole *ad hoc* per dati biometrici e profili DNA, garanzie circa la "sicurezza" del dato immagazzinato e messo in circolazione), quello su cui più s'intrattiene il Garante concerne l'applicabilità della decisione quadro al trattamento interno, arrivando ad affermare che «un campo d'applicazione più limitato è impraticabile e, se introdotto, esigerebbe distinzioni difficoltose e precise all'interno delle basi dati delle autorità incaricate dell'applicazione della legge, non facendo altro che causare costi e complessità supplementari per dette autorità e per di più pregiudicando la certezza giuridica delle persone fisiche».

83 *Documento del Consiglio n. 7315/07*, 13 marzo 2007, <http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/892.pdf>.

84 Considerando n. 6a.

into a single data protection supervisory authority»[85]; infine, si chiarisce che «Improving data protection within the third pillar depends on the Framework Decision covering the whole of the third pillar, including Europol, Eurojust and the third-pillar Customs Information System»[86]. Ciò significa, da un lato, prendere posizione, sia pure in maniera ancora estremamente cauta (dato che, oltre al summenzionato "considerando" n. 6a, non sono molte le statuizioni sul punto), in favore dell'attitudine della disciplina contenuta nella decisione quadro in parola a condizionare, per i singoli Stati, il trattamento delle informazioni di *law enforcement* anche *intra moenia*, cioè, non solo nelle ipotesi di scambi transfrontalieri, ma anche a livello di trattamento interno ai confini nazionali. In secondo luogo, si affaccia la prospettiva dell'istituzione di un'unica autorità di controllo in materia di protezione dei dati trattati nell'ambito del c.d. terzo pilastro, che assuma quindi su di sé le funzioni e, perciò, esautori le omologhe autorità già esistenti e operanti nell'ambito di sistemi informativi, quali il SIS, il SID, o quelli facenti capo a Europol ed Eurojust. Ancora, si prospetta che la decisione quadro copra le attività delle istituzioni e degli organismi centralizzati europei nel "terzo pilastro": la proposta allude espressamente ai dati trattati da Europol, Eurojust e in seno al SID, ma il testo normativo non consente di escludere un'estensione a tutte le istituzioni europee operanti nel quadro del Titolo VI TUE, quali il Consiglio e la Commissione[87].

Va detto, tuttavia, che, nonostante questo possibile ampliamento tridimensionale dell'ambito d'incidenza della decisione quadro, l'articolato normativo appare piuttosto scarno, riducendosi il numero degli articoli (e, con esso, il contenuto prescrittivo dell'iniziativa legislativa) dai trentasei dell'originaria proposta dell'ottobre 2005 a ventinove. Così, appaiono fondate le critiche mosse dal Garante europeo per la protezione dei dati personali a mezzo di un'opinione (la terza in materia di privacy in "terzo pilastro") resa nell'aprile 2007[88]. Il Garante, nonostante l'approvazione per la scelta della Presidenza d'imprimere nuovo slancio al tema in commento, giudica il testo riformato non all'altezza delle aspettative. Svariate le ragioni di tale censura. *In primis*, il testo indebolirebbe il livello di protezione dei cittadini, essendo state soppresse varie disposizioni essenziali in argomento, viceversa contenute nella proposta della Commissione. Cosicché, per molti aspetti, il livello di protezione offerto dalla proposta riveduta risulterebbe inferiore a quello fissato dalla Convenzione del Consiglio d'Europa

85 Considerando n. 18.

86 Considerando n. 20.

87 Si prospetta, in altri termini, uno scenario simile a quello che, in "primo pilastro", è raffigurato dal regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, «concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati».

88 In *GUUE*, C 139, 23 giugno 2007, p. 1.

del 28 gennaio 1981, n. 108, sulla «protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», rivelandosi pertanto non solo insoddisfacente, ma addirittura incompatibile con gli obblighi internazionali assunti dagli Stati membri del Consiglio d'Europa. *In secundis*, il fatto che l'iniziativa copra anche i dati trattati da Europol, Eurojust e SID, pur svelando un intento in sé encomiabile, complica sensibilmente il quadro generale, riaprendo il dibattito sui controlli all'interno di tali sistemi informativi. E il Garante si chiede se la decisione quadro in commento costituisca lo strumento giuridico più appropriato per affrontare e risolvere tali delicatissime questioni. Ancora, la qualità legislativa del testo non è giudicata soddisfacente (letteralmente, viene "deplorata"): in particolare, il testo non appare redatto in modo chiaro, semplice e preciso, impedendo di identificare in maniera inequivocabile i diritti e gli obblighi facenti capo ai soggetti interessati dal trattamento dei propri dati personali. Il GEPD non si nasconde certo le difficoltà che, sul piano istituzionale, possono ostare al raggiungimento *in subiecta materia* dell'unanimità in seno al Consiglio. Tuttavia, esclude che l'ostacolo rappresentato dalla procedura decisionale possa rappresentare un alibi per un approccio di tipo minimalista che, sul piano dei risultati, lederebbe i diritti fondamentali dei cittadini dell'Unione e ostacolerebbe, di fatto, le attività di *law enforcement*[89].

Queste notazioni critiche riecheggiano in un progetto di relazione al Parlamento europeo del 4 maggio 2007[90], destinato a fungere da linea-guida per una successiva risoluzione legislativa del Parlamento stesso (effettivamente approvata il 7 giugno 2007[91]), in cui è pressante l'esigenza di rendere più chiare le indicazioni concernenti l'attitudine della decisione quadro a regolamentare anche il trattamento a livello nazionale delle informazioni di *law enforcement*. E siccome è ormai chiaro che questo rappresenta uno dei punti più dolenti in materia, si suggerisce di adottare la strategia dei "piccoli passi", *id est* degli interventi scaglionati nel tempo: fra le proposte di emendamento, compare un nuovo par. 5-*bis* inter-

---

89 Il basso livello di protezione, offerto dalla proposta, non è giudicato funzionale alla creazione di uno spazio di libertà, sicurezza e giustizia in cui le forze di polizia e le autorità giudiziarie possano scambiarsi informazioni valicando agevolmente le frontiere nazionali: difettando un livello di protezione dei dati elevato e uniforme, la proposta finirebbe per lasciare gli scambi di informazioni assoggettati alle diverse «norme di origine», configurando «doppi standard» nazionali, che rischierebbero di compromettere l'efficacia della cooperazione nelle materie di "terzo pilastro".

90 Progetto (<http://www.europarl.europa.eu/meetdocs/2004_2009/documents/pr/665/665822/665822it.pdf>) poi approvato, da un apposito comitato parlamentare, il 21 maggio (<http://www.europarl.europa.eu/oeil/resume.jsp?id=5279032&eventId=995965&backToCaller=NO&language=en>) e sfociato in una (pressoché pedissequa) bozza di risoluzione legislativa, varata il successivo 24 maggio 2007 (<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2007-0205+0+DOC+PDF+V0//IT>).

91 *Documento n. P6_TA(2007)0230*, 7 giugno 2007, in <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2007-0230+0+DOC+WORD+V0//IT>.

polato nell'art. 1, secondo cui, entro i tre anni successivi all'entrata in vigore della decisione quadro, la Commissione potrà presentare proposte al fine di ampliarne il campo di applicazione, involgendo il trattamento dei dati di carattere personale nel quadro della cooperazione giudiziaria e di polizia a livello nazionale[92]. Inoltre, vengono dal Parlamento decisamente potenziate le garanzie da assicurarsi al soggetto interessato dal trattamento del dato[93], tanto che si allegano al testo della futuribile decisione quadro[94] l'elencazione e l'esplicazione (a volte piuttosto analitica) di quelli che vengono definiti i «quindici principi sulla protezione dei dati personali trattati nel quadro della cooperazione giudiziaria e di polizia in campo penale», principi generali mutuati da un'iniziativa del 28 marzo 2007 del commissario europeo Franco Frattini[95].

Tentando un'opera di sintesi, si può dire che i settori in cui è più deciso l'intervento del Parlamento europeo sono: quello degli ambiti di incidenza della decisione quadro, con l'attenzione polarizzata sul trattamento che avviene all'interno dei confini statali; quello del trattamento dei dati, ulteriore rispetto agli scopi che presiedono all'originaria raccolta o trasmissione[96]; quello del trasferimento verso Paesi estranei all'Unione europea[97]; quello della trasmissione di dati a privati

---

92 Emendamento motivato dalla Relazione affermando che l'estensione del campo di applicazione della decisione quadro all'insieme dei dati trattati all'interno degli Stati membri è essenziale, se si vuole garantire un livello armonizzato di protezione dei dati. Perciò, in mancanza di accordo su questa questione in seno al Consiglio, tale emendamento consente, quantomeno, di sollecitare una nuova discussione a medio termine.

93 Si vedano, in particolare, le modifiche prospettate all'art. 3.

94 Cfr. l'emendamento n. 60.

95 Nel marzo 2007, il commissario Frattini ha infatti sottoposto alla relatrice in Parlamento, l'onorevole Martine Roure, un progetto di testo che, appunto, sintetizza in quindici principi generali gli aspetti essenziali dell'*acquis* relativo alla protezione dei dati personali trattati nel quadro della cooperazione di polizia e giudiziaria in materia penale, quali emergono dalle convenzioni internazionali e dal diritto europeo in materia. La Relatrice dimostrerà, non solo di aderire ai principi in parola, ma proporrà il loro utilizzo come canovaccio per i lavori legislativi in questo settore, oltre che come base per i negoziati con Paesi terzi, ritenendo, peraltro, che tali principi dovrebbero essere oggetto di una presa di posizione formale da parte delle altre istituzioni europee.

96 Muovendo dall'idea che quello di "finalità limitata" rappresenti un principio fondamentale della protezione dei dati, si reputa che l'ulteriore trattamento degli stessi per qualunque altra finalità, previsto all'art. 12 lett. *d*), sia irrispettoso di tale principio. Inoltre, si osserva che la nozione di consenso della persona interessata, aggiunta dal Consiglio come fattore discriminante nel caso in cui il trattamento dei dati abbia finalità diverse rispetto a quelle che presiedono alla loro raccolta, non risulti plausibile, posto che, nell'ambito della cooperazione di polizia e giudiziaria, non esisterebbe un consenso realmente libero.

97 Il testo proposto dal Consiglio non conteneva più alcun riferimento alla necessità di assicurare un livello adeguato di protezione dei dati scambiati con i Paesi terzi, a norma dell'art. 2 del Protocollo aggiuntivo alla Convenzione n. 108 del 1981. Così, si propone di reintrodurre tale elemento, affinché la decisione quadro non adotti standard inferiori rispetto a quelli che disciplinano attualmente la protezione dei dati. Inoltre, si prevede *in parte qua* un coinvolgimento dell'istituenda autorità di controllo comune.

e dell'accesso ai dati da parte di privati; quello del ruolo della nuova autorità di controllo comune e delle autorità nazionali[98].

Rimane fermo, comunque, che il fattore più critico, emerso da questi accidentati lavori preparatori, è quello relativo alle forme di trattamento *purely domestic*. Ebbene, proprio l'estrema delicatezza della questione sta probabilmente alla base di una svolta repentina: in una comunicazione rivolta al Consiglio il 13 settembre 2007[99], la Presidenza dell'Unione, onde evitare che la paralisi in materia si protragga ancora per lungo tempo, propone di riscrivere i "considerando" nn. 6 e 6a, in modo che sia chiaro che «The scope of the Framework Decision is limited to the processing of personal data transmitted or made available between Member States» e che «To facilitate data exchanges in the European Union, Member States intend to ensure that the standard of data protection achieved in national data-processing matches that provided for in this Framework Decision». Il che vuol dire circoscrivere l'area d'impatto della futuribile decisione quadro a quella concernente gli scambi transfrontalieri di informazioni, mentre, per quanto concerne il trattamento interno, si menziona un generico impegno, che gli Stati si assumono, di assicurare un livello di tutela in linea con quello teorizzato dalla decisione quadro[100]. Davvero degno di nota che, da questo momento in poi, tale opzione diviene una costante nelle bozze di proposta di decisione quadro varate dalla Presidenza: così è in quelle del 21 settembre e del 1° ottobre 2007, indirizzate al Gruppo multidisciplinare sul crimine organizzato; in quelle del 12 e del 16

98 Com'è noto, la direttiva 95/46/CE sulla protezione dei dati nel quadro del primo pilastro impone già da tempo la creazione di autorità nazionali di protezione dei dati. Ebbene, reputando opportuno sfruttare l'esperienza delle autorità esistenti, si propone l'ampliamento delle competenze di queste ultime al terzo pilastro. Quanto all'autorità di controllo comune, si afferma che essa sarà realmente efficace, soltanto se riunirà le autorità nazionali e il garante europeo per la protezione dei dati, sicché si suggerisce di specificarne la composizione nel testo della decisione quadro.

99 *Documento del Consiglio n. 12154/2/07*, 13 settembre 2007, <http://www.statewatch.org/news/2007/sep/eu-dp-12154-07-rev2.pdf>.

100 Viene anche dedicata attenzione al tema dello scambio con Paesi estranei all'Unione europea, facendo leva, in linea di principio, sul consenso dello Stato che ha in origine raccolto il dato. Questo, il testo dei proposti "considerando" nn. 12a e 12b: «Where personal data are transferred from a Member State of the European Union to third countries or international bodies, such transfer can, in principle, take place only after the Member State from which the data were obtained has given its consent to the transfer. Each Member State may determine the modalities of such consent, including, for example, by way of general consent for categories of information or for specified countries»; «The interests of efficient law enforcement cooperation demand that where the nature of the threat to the public security of a Member States or a third State is so immediate as to render it impossible to obtain prior consent in good time, the competent authority may forward the relevant personal data to the third State concerned without such prior consent. The same could apply where other essential interests of a Member State of equal importance are at stake, for example where the critical infrastructure of a Member State could be the subject of an imminent threat or where a Member State's financial system could be seriously disrupted».

ottobre, rivolte alle delegazioni dei Paesi membri; in quella del 23 ottobre 2007, rivolta al COREPER e, quindi, al Consiglio[101].

Così, da questo frenetico laboratorio uscirà, nel dicembre 2007, una nuova bozza di decisione quadro che sembra finalmente catalizzare il consenso dei membri del Consiglio[102], bozza il cui testo, sostanzialmente confermato, verrà meglio profilato da un punto di vista stilistico in un documento del giugno 2008[103]. Sennonché, l'accordo politico, raggiunto in via programmatica dal Consiglio UE sulla bozza in parola, differisce parzialmente, nei contenuti, sia dalla proposta originaria della Commissione, sia dal testo, in precedenza varato dal Consiglio stesso, su cui il Parlamento europeo era stato consultato. Donde, un ricoinvolgimento di quest'ultimo.

Nel marzo 2008, viene pubblicato dalla Commissione per le libertà civili, la giustizia e gli affari interni un nuovo progetto di relazione da sottoporre ai rappresentanti dei cittadini europei[104], progetto tradottosi in una relazione definitiva nel luglio dello stesso anno[105]. Tra i passaggi che meritano attenzione, va anzitutto annoverato il riferimento all'art. 16 del Trattato sul funzionamento dell'Unione europea (sottoscritto a Lisbona), il quale fornirebbe una chiara base giuridica per l'adozione di norme specifiche sulla protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia. Da qui, la conclusione che, entro sei mesi dalla data di entrata in vigore del Trattato di Lisbona, si renderà probabilmente necessaria una revisione della decisione quadro, in particolare al fine di estenderne il campo di applicazione, fino a ricomprendere i dati trattati a livello nazionale. *In secundis*, si ricorda che il Parlamento europeo ha sempre insistito sull'adozione di una decisione quadro forte e protettiva, che garantisca un livello di protezione dei dati quantomeno equivalente a quello assicurato nell'ambito

---

101 Cfr., per una sintesi, B. Piattoli, *Sistema di protezione dei dati personali nel terzo pilastro: esigenze di tutela e di rafforzamento delle indagini*, in "Diritto penale e processo", 2007, p. 1687.

102 *Documento del Consiglio n. 16069/07*, 11 dicembre 2007, <http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/970.pdf>. A tale bozza ne viene allegata una seconda, concernente una "*declaration*" del Consiglio UE relativa all'istituzione di un'unica autorità di controllo in materia di protezione dei dati trattati nell'ambito del c.d. terzo pilastro. Vi si legge che «The Council will examine how, in the future, [...] the functions performed by the existing joint data protection supervisory authorities, which have been established separately for the Schengen Information System, Europol, Eurojust, and the Customs Information System, could be combined within a single data protection supervisory authority, including the function of acting in an advisory capacity, whilst taking account of the specific nature of these systems and bodies».

103 *Documento del Consiglio n. 9260/08*, 24 giugno 2008, <http://register.consilium.europa.eu/pdf/it/08/st09/st09260.it08.pdf>.

104 Il documento, del 10 marzo 2008, può leggersi in <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-402.702+02+DOC+PDF+V0//EN&language=EN>.

105 *Documento n. A6-0322/2008*, 23 luglio 2008, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0322+0+DOC+PDF+V0//EN>.

del "primo pilastro" dalla direttiva 95/46/CE e dalla Convenzione del Consiglio d'Europa n. 108 del 1981. Pertanto, si esprime rammarico a fronte della scelta del Consiglio di svuotare la proposta originale della Commissione di alcuni significativi contenuti, raggiungendo un accordo politico sulla base del minimo comune denominatore. Si lamenta, in altri termini, che il livello di protezione dei dati, garantito dal testo più recente, è troppo basso e lascia sopravvivere lacune molto gravi, tali da far dubitare, sotto certi punti di vista (in particolare, quello della proporzionalità), che gli standard stabiliti dalla Convenzione n. 108 siano rispettati.

Ne consegue la prospettazione di una serie d'importanti emendamenti che gravitano intorno ad alcuni temi essenziali, che affiancano quello, centralissimo, del trattamento interno ai confini nazionali: assicurare più compiutamente i principi di proporzionalità e di finalità limitata; riservare una disciplina particolarmente restrittiva al trattamento dei dati c.d. sensibili; disciplinare in modo specifico il tema del trasferimento dei dati a Paesi terzi ovvero a soggetti privati; fornire maggiori puntualizzazioni sui diritti di accesso alle informazioni immagazzinate; riservare maggiore attenzione ai gruppi di lavoro[106] e alle autorità nazionali per la protezione dei dati.

Con qualche variazione, il testo della relazione in parola è stato approvato dal Parlamento europeo con una risoluzione legislativa del settembre 2008[107]. Ivi, spicca l'interpolazione della lettera *c*-bis) nell'art. 1, par. 2, della proposta di decisione quadro, così da estenderne *claris verbis* l'ambito applicativo fino a comprendere, oltre alle informazioni oggetto di *cross-border exchanges*, anche i dati che «sono trattati a livello nazionale».

Il lungo itinerario che, dopo la pubblicazione del Programma dell'Aia, ha preso formalmente avvio nell'ottobre 2005 con la proposta della Commissione n. 475 è, a questo punto, a un passo dalla conclusione.

Infatti, nel novembre 2008[108], il Segretariato generale del Consiglio chiede esplicitamente al Comitato dei Rappresentati Permanenti (COREPER) «di invitare il Consiglio ad adottare il progetto di decisione quadro [...] quale figura nel doc. 9260/08», cioè nel summenzionato testo del 24 giugno 2008: ciò che puntualmente avverrà il 27 novembre dello stesso anno, data dell'approvazione, da parte del Consiglio UE, della decisione quadro 2008/977/GAI sulla protezione

106 Sul modello di quello costituito, nell'ambito del primo pilastro, a norma dell'art. 29 della direttiva 95/46/CE: Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali.

107 *Documento n. P6__TA-PROV(2008)0436*, 23 settembre 2008, in <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2008-0436>.

108 *Documento del Consiglio n. 15213/08*, 5 novembre 2008, in <http://register.consilium.europa.eu/pdf/it/08/st15/st15213.it08.pdf>.

dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[109].

Ad esito di questo complesso itinerario ricostruttivo a proposito della protezione dei dati personali in "terzo pilastro", dovrebbe risultare sufficientemente chiaro che il consesso degli esecutivi nazionali ha raggiunto l'unanimità dei consensi su un testo reputato per certi aspetti insoddisfacente dalle altre istanze europee. A partire dall'autunno 2007, le prospettive *de iure condendo* in tema di autodeterminazione informativa hanno imboccato e percorso, sulla scena europea, strade diverse. Più precisamente, i governi dei Paesi membri e la Presidenza del Consiglio UE hanno pragmaticamente puntato ad aggirare i maggiori ostacoli incontrati *in subiecta materia*, patrocinando la causa di un testo "minimalista", in grado cioè di assicurare una soglia-base di tutela all'autodeterminazione informativa in "terzo pilastro", sia pure abdicando (almeno in questa prima fase) al perseguimento di obiettivi più ambiziosi. In particolare, il profilo saliente che si è deciso di accantonare è quello del trattamento delle informazioni di *law enforcement* all'interno dei confini nazionali, cioè quando non vengono in gioco fenomeni di scambio transfrontaliero. Proprio su questo aspetto, si è registrato il più forte attrito con l'altra impostazione, propugnata dal Garante europeo della protezione dei dati e del Parlamento europeo, convinti che, fin da subito, la disciplina in commento avrebbe dovuto aspirare alla regolamentazione di tutti i fattori critici. Così, oltre al trattamento "domestico" dei dati, vengono in gioco i versanti della proporzionalità e della finalità limitata, dell'utilizzabilità dei dati sensibili, del *cross-border exchange* che coinvolga Paesi terzi rispetto all'Unione europea ovvero che interessi soggetti privati, per terminare con l'ampiezza del diritto di accesso da assicurarsi all'interessato e col ruolo da riconoscere alle autorità nazionali per la protezione dei dati.

Di tutto ciò si trova inequivocabile conferma nelle reazioni alla notizia dell'avvenuta approvazione della decisione quadro. Meritano di essere riportate testualmente le parole spese del Garante europeo in una nota pubblicata all'indomani dell'adozione: «I welcome the adoption of the Framework Decision as an important first step forward in a field where common standards for data protection are very much needed. Unfortunately, the level of data protection achieved in the final text is not fully satisfactory. In particular, I regret that the Framework Decision only covers police and judicial data exchanged between Member States, EU authorities and systems, and does not include domestic data. Further steps are therefore needed – either or not under the Lisbon Treaty – to increase the level of protection provided by the new instrument»[110]. Oltre al problema del

---

109 In *GUUE*, L 350, 30 dicembre 2008, p. 60. L'art. 29, par. 1, stabilisce che gli Stati abbiano tempo fino al 27 novembre 2010 per conformarsi alle disposizioni della decisione quadro *de qua*.

110 *Press release*, 28 novembre 2008, in <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2008/EDPS-2008-11__DPFD__EN.pdf>.

trattamento interno ai confini nazionali, il Garante rimarca altri tre fondamentali punti critici, ribadendo posizioni già esplicitate nei propri pareri sul tema: *a*) «the need to distinguish between different categories of data subjects, such as suspects, criminals, witnesses and victims, to ensure that their data are processed with more appropriate safeguards»; *b*) «ensuring an adequate level of protection for exchanges with third countries according to a common EU standard»; *c*) «providing consistency with the first pillar's Data protection Directive 95/46/EC, in particular by limiting the purposes for which personal data may be further processed».

Merita un cenno anche l'intervento del *Working Party on Police and Justice*, incaricato dalle Autorità europee di protezione dei dati[111] di "monitorare" gli sviluppi della materia in relazione alla cooperazione giudiziaria e di polizia. Il Gruppo, per il tramite del Presidente, Francesco Pizzetti, afferma di «aver preso atto della adozione della Decisione Quadro sulla protezione dei dati nel III pilastro da parte del Consiglio GAI» e di averla salutata positivamente: il tono piuttosto "freddo" rivela una certa dose di insoddisfazione dovuta, ancora una volta, al giudizio parzialmente negativo sui contenuti del provvedimento. In particolare, il Gruppo rimarca «che gli emendamenti formulati dal Parlamento Europeo non sono stati recepiti nel testo adottato né sono stati presi in considerazione i commenti espressi dalle Autorità nazionali di protezione dei dati» e «si rammarica che la Decisione Quadro nel testo adottato non preveda l'istituzione di un raccordo, con finalità consultiva, fra le autorità nazionali di protezione dati e le autorità di controllo europee, in modo da assicurare l'applicazione armonizzata delle disposizioni rilevanti in materia, con particolare riferimento alla valutazione dell'adeguatezza del livello di protezione dati in vista del loro trasferimento a paesi terzi»[112].

---

111 Le Autorità garanti, istituite nei singoli Paesi UE giusta la direttiva 95/46/CE, potrebbero entro breve tempo veder estese le proprie competenze dal primo al terzo pilastro. I "considerando" nn. 34 e 35, infatti, focalizzano l'attenzione su di esse, stabilendo che «Le autorità di controllo già istituite negli Stati membri ai sensi della direttiva 95/46/CE dovrebbero poter essere incaricate anche dei compiti che devono essere adempiuti dalle autorità di controllo nazionali da istituire a norma della presente decisione quadro. Le autorità di controllo dovrebbero disporre dei mezzi necessari all'adempimento dei loro compiti, compresi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali. Tali autorità di controllo dovrebbero contribuire alla trasparenza dei trattamenti effettuati nello Stato membro da cui dipendono. Tuttavia, i poteri di tali autorità non dovrebbero interferire con le norme specifiche stabilite per i procedimenti penali o con l'indipendenza della magistratura».

112 *Comunicato stampa*, 28 novembre 2008, <http://www.garanteprivacy.it/garante/doc.jsp?ID=1570344>.

6. Il percorso di avvicinamento alla "disponibilità informativa"

Chiusa la parentesi sull'opera, fino a pochissimo tempo fa incompiuta, relativa a privacy e autodeterminazione informativa in "terzo pilastro", va ripreso il filo conduttore del principio di disponibilità. Qui, il discorso, cominciato con il Programma dell'Aia, rivela movenze sensibilmente diverse, non foss'altro perché il Consiglio dell'Unione europea ha tempestivamente raggiunto l'unanimità dei consensi, richiesta dall'art. 34 TUE: da più di due anni, è in vigore la decisione quadro 2006/960/GAI del 18 dicembre 2006[113]. Anche in questo settore, tuttavia, non mancano le complicazioni, dato che la decisione quadro in parola non si radica nella già esaminata proposta della Commissione n. 490 del 2005. Invero, fino ad ora si sono volutamente (onde non confondere le trame dell'indagine) omessi due fattori, estranei all'ordine ideale rappresentato dalla sequenza "Programma dell'Aia" (Consiglio europeo) – "Piano di azione" (Commissione e Consiglio UE) – "coppia di proposte di decisione quadro" (Commissione) – "decisioni quadro" (Consiglio UE): trattasi di un'iniziativa del Regno di Svezia concernente il principio di disponibilità (sarà questa la musa ispiratrice del Consiglio dell'Unione europea) e della sottoscrizione degli accordi di Prüm. È giunto il momento di completare il mosaico.

7. L'iniziativa del Regno di Svezia: gli albori del principio di disponibilità

Nel giugno 2004, cioè qualche mese prima che il Consiglio europeo di Bruxelles stilasse il Programma dell'Aia, il Regno di Svezia prendeva un'iniziativa[114] «in vista dell'adozione di una decisione quadro relativa alla semplificazione dello scambio di informazioni ed intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge, in particolare con riguardo ai reati gravi, compresi gli atti terroristici». Scopo dell'iniziativa è quello di garantire che le informazioni e l'*intelligence* siano scambiate con rapidità all'interno dell'Unione, in modo che non siano le difficoltà, pratiche o tecnico-giuridiche, sul piano dell'*information sharing* ad ostacolare, di per sé, la prevenzione dei reati o le indagini in materia criminale.

Significativo lo spettro delle definizioni, che concentra, sì, l'attenzione sulle autorità di polizia, piuttosto che su quelle giudiziarie, ma che non esclude *in toto* queste ultime (come invece farà la Commissione nella propria iniziativa dell'ottobre 2005[115]). Stando all'art. 2 lett. *a*), per «autorità competente incaricata dell'applicazione della legge» («competent law enforcement authority»), si intendono

113 V. *infra*, § 9.

114 Pubblicata in *GUUE*, C 281, 18 novembre 2004, p. 5.

115 Lo si è visto *supra*, § 4.

la polizia, i servizi doganali o altra autorità nazionale che, in forza della legislazione interna, è competente per individuare, prevenire o indagare su reati o attività criminali, esercitare l'autorità e adottare misure coercitive nell'ambito di tali funzioni. Ma non solo: anche un'autorità giudiziaria («a judicial authority») può considerarsi "autorità competente incaricata dell'applicazione della legge". Per l'iniziativa svedese, infatti, ciò accade se le informazioni o l'*intelligence* sono detenute, ai sensi della legislazione nazionale, soltanto da detta autorità, ovvero se solo essa può accedervi.

La proposta di decisione quadro non manca di operare una testuale distinzione tra «indagine penale» e «operazione di intelligence criminale», funzionale, tra l'altro, a circoscrivere l'area di operatività del principio di disponibilità.

Si considera «indagine penale» («crime investigation») un quadro giuridico («a legal framework») in cui le autorità incaricate dell'applicazione della legge e le autorità giudiziarie competenti adottano misure per individuare e accertare i fatti, le persone sospette e le circostanze in ordine a uno o più «atti criminali accertati» («identified concrete criminal acts»). Non c'è dubbio che, traducendo queste formule nel lessico del codice di rito penale italiano, venga in gioco la fase delle indagini preliminari e, con essa, il sinergismo delle attività poste in essere dalle forze di polizia e dall'autorità giudiziaria inquirente.

Diversamente, è «operazione di intelligence criminale» («criminal intelligence operation»), un quadro giuridico («a legal framework») in cui, in una fase precedente all'indagine penale sovrintesa dalle autorità giudiziarie, un'autorità competente incaricata dell'applicazione della legge, ai sensi della legislazione nazionale, ha facoltà di raccogliere, elaborare e analizzare informazioni su reati o attività criminali, al fine di stabilire se sono stati commessi o possono essere commessi atti criminali concreti. In altri termini, si allude all'attività, tipica delle forze di polizia, che si svolge per finalità preventive o che è intesa ad acquisire eventuali notizie di reato e che, comunque, precede la formale acquisizione di queste ultime (dopo, se del caso, iniziano le *crime investigations*).

Il concetto di "*intelligence* criminale", dunque, non deve intendersi nell'accezione, più comune e restrittiva, di «attività informativa espletata dal personale appartenente ai Servizi per le informazioni e la sicurezza militare e democratica [...] volt[a] alla comprensione e alla previsione di eventi, fenomeni e comportamenti, tutti meritevoli di attenzione per i loro contenuti di minaccia attuale o potenziale alla sicurezza dello Stato»[116]; deve invece riferirsi alle attività che le forze di polizia pongono in essere per scongiurare la commissione di reati ovvero per scoprire attività illecite già poste in essere, momento a partire dal quale potranno prendere formalmente avvio le "indagini penali". Piuttosto, resta da stabilire se il concetto di «criminal intelligence operation», pur non implicando

116 M.L. Di Bitonto, "Raccolta di informazioni e attività di *intelligence*", in *Contrasto al terrorismo interno e internazionale*, cit., p. 253.

necessariamente il coinvolgimento dei servizi segreti, consenta di comprenderli ovvero imponga di escluderli. La laconicità del testo proposto dal Regno di Svezia non suffraga l'opzione restrittiva; sarà invece il Consiglio dell'Unione europea a prendere chiaramente posizione sul punto[117].

Vale la pena di ricordare che, su questo piano, eminentemente funzionale, l'iniziativa della Commissione n. 490 del 2005 non si discosterà in maniera rilevante, posto che farà riferimento ai «compiti legittimi per la prevenzione, l'individuazione e l'investigazione dei reati», così riferendosi alla fase preventiva come a quella repressiva (purché *pre*-processuale). Né le due iniziative divergono quando escludono l'obbligo, per gli Stati membri, di fornire informazioni e *intelligence* da utilizzare come prove in senso stretto (cioè nel corso di un processo, ad accusa formalmente elevata) e, consequenzialmente, vietano alle autorità riceventi di utilizzarle a tal fine. Se l'autorità di uno Stato membro ottenesse informazioni o *intelligence* in virtù del principio di disponibilità e intendesse utilizzarle come prove in un processo penale, dovrebbe chiedere e ottenere il consenso dello Stato membro che ha fornito le informazioni o l'*intelligence*, ricorrendo agli ordinari strumenti di assistenza giudiziaria internazionale.

Nell'iniziativa svedese, a mente dell'art. 2 lett. *d*), «informazioni e intelligence» sono *nomina iuris* bulimici, in quanto ricomprendono qualsiasi tipo di informazioni o dati esistenti – siano essi valutati, elaborati, analizzati o meno – che potrebbero essere utilizzati in un'indagine penale o in un'operazione di *intelligence* criminale.

Quanto alle fonti da cui possono essere attinte, rilevano, in primo luogo, i registri e gli archivi tenuti dalle stesse autorità competenti incaricate dell'applicazione della legge. Ciò vuol dire che, giusta il principio di disponibilità, l'autorità nazionale di *law enforcement* che crea e cura una banca dati è, in linea di principio, tenuta a condividerne i contenuti con le omologhe autorità straniere. Essa vi accede liberamente e senza condizioni; sicché, se riceve una domanda da oltre confine, in via di regola è tenuta a consultare il proprio archivio e a metterne a disposizione dell'instante i contenuti, rispondendo prontamente. Vengono poi in gioco le informazioni catalogate in registri o archivi tenuti da autorità diverse da quelle di *law enforcement* (si pensi, ad esempio, a un ente pubblico territoriale o alla motorizzazione civile), cui però quelle incaricate dell'applicazione della legge hanno accesso, direttamente o indirettamente (cioè formulando un'apposita istanza all'ente che le detiene): il principio di disponibilità fa sì che le autorità di contrasto straniere possano accedere a tali archivi alle stesse condizioni delle autorità di contrasto nazionali. In terzo luogo, vengono espressamente menzionate alcune tipologie di dati, che entrano *ex se* nella sfera d'incidenza del principio di disponibilità: trattasi delle informazioni su titolari (in elenco o fuori elenco) di abbonamenti a telefono fisso, telefono cellulare, telex, fax, e-mail o sito web, de-

117 V. *infra*, § 9.

tenute dagli operatori di telecomunicazioni, cui si aggiungono le informazioni, detenute da vettori, su persone o merci. Infine, una clausola dalla portata amplissima, volta a ricomprendere «informazioni, intelligence o dati di altro tipo, siano essi valutati, elaborati, analizzati o meno, che siano stati ottenuti nel quadro di un'indagine penale o di un'operazione di intelligence criminale o che possano essere ottenuti senza coercizione» («any other information or intelligence or data; appraised, processed and analysed or not, that has been obtained within the framework of a criminal investigation or a criminal intelligence operation or that may be obtained without the use of coercive powers»). Questa previsione suggerisce che, per certi versi, il principio di disponibilità concepito dall'iniziativa svedese si autoalimenta: da un lato, favorendo l'*information sharing*, accresce le potenzialità di prevenire e reprimere i reati; dall'altro, tali aumentate potenzialità si traducono (anche) in una maggiore capacità di raccogliere ulteriori informazioni, le quali, proprio perché ottenute svolgendo attività di *law enforcement*, sono per ciò stesso considerate "disponibili".

In parte qua, è piuttosto netta la differenza che separa, quanto alle strategie adottate, l'iniziativa del Regno di Svezia da quella della Commissione che, come già si è detto[118], circoscrive le categorie dei dati, interessate dal principio di disponibilità, alle sole s*pecies* contemplate dall'apposito Allegato. Tuttavia, non appena si rammenti che queste ultime comprendono profili DNA, *fingerprints*, tabulati telefonici, dati concernenti veicoli e dati balistici, nonché informazioni essenziali tratte dai registri anagrafici, è subito chiaro che all'iniziativa della Commissione non sfuggono certo le categorie di informazioni più rilevanti sul fronte della prevenzione e della repressione dei reati.

Nella proposta del Regno di Svezia, le informazioni e l'*intelligence* sono comunicate su richiesta formulata da un'autorità competente incaricata dell'applicazione della legge che svolge, oltre confine, un'indagine penale o un'operazione di *intelligence* criminale, purché l'attività preventiva o repressiva concerna «reati puniti dalle leggi dello Stato membro richiedente con una pena privativa della libertà o con una misura di sicurezza privativa della libertà non inferiore nel massimo a dodici mesi»[119]. Nell'iniziativa svedese, quindi, il principio di disponibilità è incentrato sul meccanismo della domanda e della risposta, non su quello dell'accesso diretto alle banche dati straniere. Ben diversamente dalla proposta della Commissione, dove si distingue tra l'accesso on-line alle informazioni *tout court* e la consultazione on-line dei soli dati di indice, cui potrà far seguito una richiesta di ulteriori informazioni (modello, quest'ultimo, che rievoca quello degli accordi di Prüm[120]).

---

118 *Supra*, § 4.

119 Non servirà aggiungere che l'art. 3, fissando una soglia di pena così bassa, rende pressoché onnipervasiva la prospettiva dell'*information sharing* in materia di lotta al crimine.

120 V. *infra*, § 8.

Questa la quintessenza del meccanismo circolatorio ideato dal Regno di Svezia: gli Stati membri provvedono a che le informazioni e l'*intelligence*, detenute "personalmente" dalle autorità di contrasto o cui esse possono accedere senza il ricorso a misure coercitive, vengano comunicate alle autorità di *law enforcement* straniere in base a condizioni che non risultino più gravose di quelle applicabili a livello nazionale. In pratica, il meccanismo è innescato da una domanda dell'autorità di contrasto interessata, da cui scaturisce l'obbligo per l'autorità richiesta di trasmettere le informazioni di cui dispone direttamente, ovvero di accedere, per conto dell'instante, a quelle detenute da altre autorità. Uniche eccezioni al dovere di trasmissione, quelle compendiate dall'art. 11, secondo cui l'autorità di *law enforcement* potrà rifiutarsi di fornire informazioni o *intelligence* «solo nel caso in cui sussistano ragioni di fatto per ritenere che: *a*) la comunicazione di tali informazioni o intelligence pregiudicherebbe interessi fondamentali della sicurezza nazionale dello Stato membro richiesto; o *b*) la comunicazione di tali informazioni o intelligence metterebbe a repentaglio il buon esito di un'indagine o di un'operazione di intelligence criminale in corso; o *c*) le informazioni e l'intelligence richieste sono palesemente sproporzionate o irrilevanti per lo scopo per cui sono state richieste».

Vi è un altro profilo degno della massima attenzione, non essendovi traccia di quella che, nella proposta avanzata dalla Commissione, sarà la "tavola di corrispondenza" tra autorità omologhe[121]: nell'iniziativa svedese, l'*information sharing* non viene concepita come un fenomeno che mette in contatto autorità che esercitano, all'interno dei rispettivi confini nazionali, funzioni similari. Viceversa, come spiega a tutte lettere il "considerando" n. 5, si considera «importante che le possibilità per le autorità incaricate dell'applicazione della legge di ottenere informazioni ed intelligence su reati gravi e atti terroristici da altri Stati membri siano viste orizzontalmente e non in termini di differenze in ordine ai tipi di reato o alla suddivisione delle competenze tra autorità incaricate dell'applicazione della legge e autorità giudiziarie». Non è affatto da escludere che questa si sia rivelata una differenza decisiva nel decretare, in seno al Consiglio UE, la maggiore fortuna dell'iniziativa del Regno di Svezia rispetto a quella della Commissione.

Un fattore che solleva più di un interrogativo, invece, consiste nel fatto che la proposta svedese non si sofferma sul modo in cui l'autorità straniera interessata può identificare oltre confine quella cui richiedere le informazioni necessarie[122]. L'art. 5, par. 1, liquida, piuttosto sbrigativamente, la questione, affermando che «le informazioni e l'intelligence possono essere richieste [...] laddove vi sia motivo di ritenere che [esse] siano disponibili in altri Stati membri». In questo progetto di decisione quadro manca, in sostanza, l'ideazione di uno o più "motori di ricerca", capaci di rivelare una corrispondenza tra il quesito di un'autorità di

121 Cfr. *supra*, § 4.

122 Il problema è rilevato anche da G. Calesini, *op. cit.*, p. 208.

contrasto, che ha bisogno di determinate informazioni, e la presenza di queste ultime in un altro Stato dell'Unione, ivi accessibili per le autorità di *law enforcement*. Al riguardo, forniscono qualche delucidazione le regole riservate, nell'art. 7, ai canali di comunicazione, anche in ragione del coinvolgimento di Europol e dei Sistemi Informativi Doganale e Schengen. È, infatti, previsto che lo scambio di informazioni e *intelligence* può, anzitutto, aver luogo tramite gli uffici SIRENE o in conformità degli artt. 4, par. 4 (il riferimento è agli ufficiali di collegamento) e 5, par. 4 (il riferimento è alle unità nazionali) della Convenzione Europol o, ancora, tramite gli uffici centrali di cui all'art. 5, par. 1, della Convenzione relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali; infine, non si esclude «qualsiasi altro quadro» («any other framework») stabilito a livello bilaterale o multilaterale tra gli Stati membri dell'Unione europea ("quadro" da notificarsi al Segretariato generale del Consiglio entro tre mesi dall'entrata in vigore della decisione quadro e che va successivamente reso noto agli altri Paesi). Solo in seconda battuta, è precisato che gli Stati membri possono convenire, caso per caso o in generale, che, per lo scambio di informazioni e *intelligence*, si utilizzino altri canali, senza escludere che lo scambio possa avvenire direttamente tra le autorità centrali o locali incaricate dell'applicazione della legge[123].

In sostanza, si offre un'alternativa. Da un lato, è contemplato il coinvolgimento delle unità nazionali dei sistemi informativi già operanti in materia penale, quali gli uffici SIRENE (che fanno parte del SIS), le unità N-SID e le unità nazionali di Europol. Com'è ovvio, in questo caso le unità in parola non verranno contattate dalle autorità di contrasto di uno Stato membro per accedere ai dati trattati da Europol o contenuti nel SIS o nel SID (ciò che avviene da tempo giusta la disciplina dei singoli sistemi informativi in parola); gli uffici SIRENE, le unità N-SID e le unità nazionali di Europol divengono, invece, il punto di riferimento per veicolare una richiesta che è mirata ad ottenere le informazioni e l'*intelligence* detenute direttamente o comunque accessibili per le autorità di contrasto di un altro Stato membro. Il principio di disponibilità, quindi, viene attuato per mezzo di una "canalizzazione" che coinvolge le articolazioni dei sistemi informativi che rappresentano il paradigma della cooperazione "mediata"[124]. Non si tratta comunque dell'unica via. L'alternativa offerta dall'iniziativa svedese è quella che gli Stati convengano, caso per caso o in generale, che lo scambio di informazioni e *intelligence* avvenga direttamente tre le autorità centrali o locali incaricate dell'applicazione della legge. Questa, che si può chiamare disponibilità "pura", è l'ipotesi in cui è più pressante l'interrogativo circa le strategie che un'autorità di contrasto debba seguire per identificare l'autorità straniera cui rivolgere una richiesta di infor-

123 Quando le informazioni o l'*intelligence* non vengono scambiate ai sensi degli artt. 4 e 5 della Convenzione Europol, i dati devono essere comunicati anche all'Europol, purché lo scambio riguardi un reato o un'attività criminale di sua competenza.

124 Cui si è fatto cenno *supra*, § 1.

mazioni che abbia un minimo di possibilità di successo. Sotto questo prospetto, sembra ragionevole concludere che il Regno di Svezia, rinviando a futuri accordi tra gli Stati membri, intenda lasciare a queste intese bi- o multi-laterali la risoluzione di un problema di primissimo piano nell'ottica dell'*information sharing*.

La proposta svedese, non avendo (come invece sarà per quella della Commissione) un *pendant* sul versante della protezione dei dati, a quest'ultimo tema dedica *ex professo* una qualche attenzione. In particolare, si prevede che ciascuno Stato membro assicurerà che le norme e gli standard fissati in materia di protezione dei dati per l'utilizzo dei canali di comunicazione di cui all'art. 7, par. 1 (si tratta dei Sistemi Informativi Schengen, Doganale ed Europol) siano applicati anche nella procedura per lo scambio di informazioni e *intelligence* prevista dalla presente decisione quadro, quando di tali canali di comunicazione ci si avvalga. Equivalenti standard dovranno del resto assicurarsi anche qualora si utilizzi un canale di comunicazione di cui all'art. 7, par. 2 (il riferimento è all'«any other framework» stabilito a livello bilaterale o multilaterale tra gli Stati membri), mentre rimane scoperta l'ipotesi della disponibilità "pura", che cioè vede lo scambio intervenire direttamente fra le autorità di *law enforcement* nazionali o locali. Il vuoto di disciplina è tutt'altro che marginale e non vi ovvia certo l'art. 9, par. 3, quando fissa, per le autorità riceventi, dei formali limiti di utilizzabilità. Non si tratta, infatti, di limitazioni stringenti, dato che le autorità in parola possono utilizzare le informazioni ricevute: *a*) nei procedimenti che hanno determinato lo scambio di informazioni in forza della decisione quadro; *b*) in altri procedimenti di *law enforcement*, purché direttamente connessi a quelli *sub a*); *c*) ai fini della prevenzione di minacce concrete e gravi alla sicurezza pubblica; *d*) per qualsiasi altro scopo, compresi i procedimenti penali o amministrativi, purché l'autorità competente incaricata dell'applicazione della legge che ha fornito le informazioni o l'*intelligence* abbia dato preventivamente il proprio consenso esplicito. Al riguardo, deve aggiungersi che, nel fornire le informazioni e l'*intelligence*, l'autorità competente incaricata dell'applicazione della legge può essa stessa imporre, ai sensi della legislazione nazionale, condizioni per l'utilizzo di dette informazioni e *intelligence* all'autorità ricevente, che ne risulterà vincolata.

Non vi è dubbio che, sul versante della tutela dell'autodeterminazione informativa, l'iniziativa svedese sfiguri, quanto ai contenuti, se messa al cospetto della proposta della Commissione n. 475 del 2005. Sennonché, viste le difficoltà cui quest'ultima è andata incontro sul piano della concreta adozione da parte del Consiglio, il pur scarno corredo di regole concepite dalla Svezia in seno alla matrice del principio di disponibilità non manca di esercitare una qualche suggestione. *A fortiori*, ciò vale se si tiene conto che, nell'estate del 2005, il Parlamento europeo ha emesso, a' termini dell'art. 39 TUE, una risoluzione legislativa circa l'iniziativa del Regno di Svezia[125]. Se, nel complesso, il giudizio sarà di ap-

125 *Documento n. P6 _ TA(2005)0216*, del 7 giugno 2005, in *GUUE*, C 124 E, 25 maggio 2006, p. 215.

provazione, il Parlamento apporterà alcuni significativi emendamenti, invitando il Consiglio ad informarlo ove decidesse di non recepirli. Ebbene, il fronte di maggiore impatto dell'intervento parlamentare sarà proprio quello della tutela del dato personale, in forza di espliciti riferimenti alla direttiva 95/46/CE[126] e la stesura di una fitta trama di regole concernenti, in particolare, la raccolta e il trattamento del dato[127], il diritto di accesso dell'interessato[128], le possibilità di rifiutare la trasmissione oltre confine[129], per culminare nell'istituzione di un'autorità comune di controllo[130]. Tutte garanzie, merita appena ricordarlo, che troveranno, sì, compiuta estrinsecazione in seno alla proposta della Commissione n. 475, di qualche mese successiva, ma che, se fossero state recepite (insieme all'articolato normativo svedese) nel testo della decisione quadro sul principio di disponibilità avrebbero quantomeno evitato che, al varo di quest'ultimo, si accompagnasse, per un biennio, la pressoché totale assenza di regole deputate alla protezione del dato personale nel "terzo pilastro" dell'UE.

8. Il Trattato di Prüm e il suo recepimento nel tessuto connettivo dell'Unione europea (decisione 2008/615/GAI)

Il 27 maggio 2005, Germania, Francia, Belgio, Lussemburgo, Olanda, Spagna e Austria sottoscrivono il Trattato di Prüm[131], con l'intento di assumere un ruolo pionieristico nel raggiungimento di un elevato livello di cooperazione di polizia e giudiziaria in materia penale. Al qual riguardo, non sono mancate voci[132] intese a rimarcare alcune criticità, rilevando come il carattere prettamente intergovernativo della cooperazione instaurata a Prüm si riveli per certi aspetti in antitesi con la prospettiva di uno sviluppo armonico, progressivo e condiviso delle politiche di *law enforcement cooperation* nel perimetro dell'Unione europea[133].

---

126 Emendamento n. 3.

127 Emendamento n. 18.

128 Emendamento n. 19.

129 Emendamento n. 14.

130 Emendamenti nn. 20 e 21.

131 Per una raffigurazione di sintesi sui contenuti degli accordi di Prüm, cfr. G. Calesini, *op. cit.*, pp. 199 sgg.; F. Gandini, *op. cit.*, p. 56, *passim*.

132 *Ex multis*, T. Balzacq-D. Bigo-S. Carrera-E. Guild, "Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats", 1° gennaio 2006, <http://www.ceps.eu>.

133 Ai sensi dell'art. 51, l'accordo è aperto alla sottoscrizione da parte degli altri Stati membri dell'UE. Numerosi Paesi hanno manifestato formalmente il proprio interesse ad aderire ancor prima che il trattato entrasse in vigore (ciò che è accaduto il 1° novembre 2006 tra Austria e Spagna); alcuni di essi hanno proceduto anche alla formale ratifica: così, ad esempio, è stato per Finlandia e Slovenia, rispetto alle quali l'accordo è entrato in vigore il 17 giugno e il 2 luglio 2007, rispettivamente. Quanto alle prospettive di adesione dell'Italia, l'intenzione del nostro

Vari gli strumenti ideati per rafforzare la cooperazione tra gli Stati firmatari, tra cui emerge la strategia di scambio di informazioni. Donde l'interesse ai fini della nostra indagine: l'accordo in commento attinge la sfera dell'*information sharing*, concependo una forma *sui generis* di disponibilità informativa, la quale, facendo la propria comparsa sulla scena europea già nel maggio 2005, non può assumersi indifferente rispetto alle sorti delle proposte di decisione quadro *in subiecta materia* del Regno di Svezia e della Commissione. Inoltre, è da poco divenuta tangibile realtà la prospettiva del recepimento, pressoché generalizzato, del Trattato di Prüm nel tessuto connettivo dell'UE, con la conseguente transustanziazione di un accordo internazionale multilaterale in matrice di una fonte di diritto primario UE[134].

In questa sede[135], basterà ricordare l'obbligo, gravante su ciascuno Stato, di creare e mantenere tre archivi nazionali centralizzati, contenenti, il primo, i profili DNA archiviati nel territorio nazionale, il secondo, le impronte digitali catalogate, l'ultimo, le informazioni relative ai veicoli immatricolati[136]. L'*information sharing* viene realizzata, o mediante l'accesso automatizzato a certe categorie di informazioni disponibili on-line (in genere, i soli dati di indice), o mediante il trasferimento delle informazioni richieste, a seguito di una specifica domanda che un'autorità di contrasto rivolge al proprio omologo d'oltre confine. Trattasi di operazioni che si integrano vicendevolmente, posto che la seconda è diretta ad acquisire tutte le informazioni che non sono direttamente accessibili on-line[137].

Paese è stata formalmente enunciata dal Ministro dell'Interno il 4 luglio 2006, a Berlino; di recente il tema è tornato di grande attualità, alla luce del c.d. pacchetto sicurezza, varato dal Consiglio dei ministri il 21 maggio 2008 (*amplius*, sul punto, A. Marandola, "*Information sharing* nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione").

134 Cfr. *infra* nel testo.

135 Per una più completa disamina degli accordi di Prüm, anche sul fronte dell'*information sharing*, vedasi *infra* A. Marandola, *op. cit*.

136 A rigore, l'obbligo di istituzione va riferito alla sola banca dati DNA (in argomento, cfr. C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un "diritto comune" europeo*, in "Diritto penale e processo", 2007, p. 385), posto che gli Stati di norma già dispongono, a livello centralizzato, di archivi dattiloscopici (AFIS: *automated fingerprint information system*) e di pubblici registri automobilistici. Se gli Stati sono tenuti a istituire e mantenere le banche dati in commento, nulla è detto (salva la peculiare ipotesi di cui all'art. 7) circa eventuali obblighi di costante alimentazione.

137 Per completezza, va detto che il modello appena delineato (e che verrà approfondito *infra*, nel testo), se rappresenta lo strumento di maggiore impatto sul piano dell'*information sharing* concepita a Prüm, non esaurisce tuttavia il panorama dei meccanismi imperniati sullo scambio di informazioni. Vale, ad esempio, la pena di richiamare gli artt. da 13 a 15 del Trattato, riservati alla trasmissione di dati in occasione dei c.d. grandi eventi, e l'art. 16, dedicato allo scambio di dati in funzione di contrasto al terrorismo. Attualmente, vedansi i medesimi articoli in seno alla decisione 2008/615/GAI. Sul punto si sofferma, *infra*, A. Marandola, *op. cit*.

Sul piano operativo, si vede che gli scambi avvengono per mezzo di una rete di punti di contatto nazionali: per ciascuna categoria d'informazioni (DNA, *fingerprints*, veicoli) è prevista la designazione, Stato per Stato, di un punto di contatto nazionale *ad hoc*, incaricato sia delle procedure passive (quando ad attivarsi è un'autorità straniera), sia delle procedure attive (innescate da un'autorità di *law enforcement* nazionale). Il Trattato di Prüm non chiarisce se le richieste, indirizzate ai punti di contatto, possano provenire solo dall'autorità di polizia, ovvero anche dall'autorità giudiziaria, il che lascia presumere (ove ci si collochi nella fase delle indagini preliminari, non nel quadro delle attività di prevenzione) che la legittimazione spetti a entrambe[138]. In questo senso, sembra deporre anche l'individuazione della base giuridica della decisione del Consiglio 2008/615/GAI, dato che ivi compaiono gli artt. 30, 31, 32 e 34 TUE[139].

Quanto alla banca dati DNA, gli indici di consultazione (compulsabili on-line dai punti di contatto nazionali) contengono profili ottenuti dalla parte non codificante del campione (c.d. *junk DNA*)[140], cosicché da essi non è possibile risalire alla caratteristiche fisiche o psicologiche dell'interessato. La banca dati raccoglie anche *open records*, cioè profili DNA che non sono riconducibili a soggetti identificati; cosa che accade di frequente, quando si raccolgono campioni biologici sulla scena del crimine, senza riuscire successivamente a ricondurli ad un soggetto determinato. L'indice associa al profilo DNA oggetto della ricerca un numero di riferimento, utilizzabile per accedere alle ulteriori informazioni archiviate. Degno di menzione il fatto che, a differenza delle altre due banche dati, accessibili anche per finalità preventive, la banca dati DNA è utilizzabile solo per finalità di perseguimento di reati, *id est* quando si lavora sulla base di una *notitia criminis*.

L'accesso on-line alla banca dati DNA avviene secondo due modalità alternative, consultazione («searching») o comparazione («comparison»). Di "consultazione" si parla quando il profilo di cui il richiedente dispone è già di per sé riferibile a persona identificata. Lo scopo è, quindi, quello di cercare oltre confine ulteriori informazioni sulla persona, già nota, cui si riferisce il profilo DNA: il punto di contatto instante riceverà una risposta automatizzata, di segno affermativo o negativo, a seconda che nell'altro Stato, coinvolto dalla richiesta, quel profilo DNA risulti o meno archiviato. L'autorità richiedente può effettuare, in-

---

138 Polarizza invece l'attenzione sulle sole autorità di polizia F. Gandini, *op. cit.*, p. 67.

139 V. *infra*, nel testo.

140 L'accordo non si sofferma sulle modalità di raccolta ed estrazione dei profili DNA dai campioni di materiale biologico. Se maggiori indicazioni si possono ricavare dall'*Administrative and technical implementing Agreement to the Prüm Convention*, del 5 dicembre 2006 (<http://www.statewatch.org/news/2007/jan/prum-implementing-agreement.pdf>), merita comunque un cenno *in parte qua* la già menzionata (*supra*, § 4) risoluzione del Consiglio UE del 25 giugno 2001, che detta disposizioni in materia di standard per le tecniche di analisi forense in materia di DNA e di scambio dei risultati delle analisi, stabilendo la serie europea standard (ESS) dei marcatori del DNA.

vece, una "comparazione" – si badi, peculiare delle banche dati DNA, non essendo prevista per quelle concernenti impronte digitali e veicoli – quando dispone solamente di un *open record*, cioè lavora con un profilo DNA che non è attributo ad alcuna persona determinata. La comparazione coinvolge tutti i profili DNA registrati nelle altre banche dati straniere, siano o meno attribuibili a persone determinate.

A prescindere dalla modalità di accesso praticata, in caso di esito positivo, la parte richiedente si vede comunicare un indice del profilo del DNA, corrispondente a quello trasmesso, che è rigorosamente anonimo. Eventuali ulteriori informazioni di carattere personale non sono accessibili on-line (si parla di "doppio binario" tra indici di consultazione e dati personali) e la loro trasmissione avverrà, su domanda dell'autorità interessata (che seguirà le indicazioni allegate al dato di indice per identificare l'omologa cui rivolgersi), nel rispetto delle singole legislazioni nazionali. E poiché il Trattato di Prüm, pedissequamente ripreso *in parte qua* dalla decisione 2008/615/GAI[141], non impartisce direttive a quest'ultimo riguardo (ben diversamente dalle proposte di decisione quadro della Commissione e del Regno di Svezia che, lo si ricorderà, si soffermano sulle possibili ragioni di un rifiuto di ostensione, enunciandole tassativamente), sono preconizzabili soluzioni interne potenzialmente divergenti, in quanto tali idonee a ostacolare o rallentare il funzionamento dell'apparato circolatorio in esame[142].

Rispetto all'AFIS (*Automated Fingerprint Information System*), valgono pressoché le stesse regole disciplinanti gli archivi DNA. Sono tuttavia meno stringenti le ragioni dell'accesso, poiché, oltre alle finalità repressive, entra in gioco la prevenzione dei reati; terreno, quest'ultimo, di tipica competenza dell'autorità di polizia. Quanto alle banche dati "automobilistiche", esse annoverano, in ulteriore aggiunta, la prevenzione di minacce alla sicurezza e all'ordine pubblico. Inoltre, qui non vale il principio del "doppio binario": è necessario disporre del numero (completo) d'immatricolazione o di telaio del veicolo e, se l'esito è fruttuoso, si accede immediatamente alle generalità di proprietario e utilizzatore, oltre che a tutte le altre informazioni concernenti questi ultimi e il veicolo. Il *tertium genus* di archivi, quindi, è strutturato in modo che di "disponibilità" si possa parlare, non solo con riguardo ai dati di indice (targa o telaio), ma anche rispetto a tutte le informazioni correlate, disponibili nello Stato richiesto e inserite nell'archivio informatico.

Sintetizzando, il Capitolo II del Trattato di Prüm e, attualmente, il Capo 2 della decisione 2008/615/GAI concepiscono il principio di disponibilità in maniera

---

141 Cfr. agli artt. 5 e 10.

142 Su questo fronte, si candidano a esercitare una certa influenza la Convenzione europea di Strasburgo del 20 aprile 1959 (resa esecutiva nel nostro Paese con l. 23 febbraio 1961, n. 215) e la Convenzione sull'assistenza giudiziaria, adottata dal Consiglio dell'Unione europea il 29 maggio 2000 (anche se, rispetto a quest'ultima, non possono certo trascurarsi i problemi in punto "ratifica", come dimostra l'esperienza italiana).

molto calibrata, limitandolo a categorie rigorosamente determinate di dati, quali sono i profili DNA, le impronte digitali e le informazioni concernenti i veicoli immatricolati: questi sono gli unici dati di cui è prevista una disponibilità *tout court*, in forza dell'inserimento nelle relative banche dati centralizzate, accessibili direttamente on-line ad opera dei punti di contatto degli altri Stati-parte. Quanto alla massa di informazioni che gravita intorno ai profili DNA e alle impronte digitali, invece, Trattato e decisione rimandano al diritto nazionale dello Stato richiesto, senza apportare modifiche alle condizioni dell'*information sharing*: in questo modo, non rendono *ex se* disponibili le informazioni *de quibus*, limitandosi a creare le condizioni affinché la circolazione avvenga (ovviamente, in materia potranno supplire altre fonti internazionali, concernenti la cooperazione di polizia e giudiziaria). Questa strategia operativa si ritrova nella proposta di decisione quadro della Commissione n. 490 del 2005, la quale, tuttavia, si distingue per almeno due ordini di motivi. *In primis*, perché contempla, in aggiunta, dati balistici, numeri di telefono e altri dati relativi al contenuto "esterno" delle comunicazioni, nonché i dati minimi per la identificazione delle persone, ricavabili dai registri anagrafici. *In secundis*, perché concepisce, sì, i due strumenti complementari dell'accesso immediato on-line e dello scambio di informazioni su richiesta, ma non pone limiti alla quantità e alla qualità dei dati direttamente compulsabili per via telematica (purché si rientri nelle *species* di cui all'Allegato II), mentre circoscrive a ipotesi tassative i casi in cui una richiesta di ulteriori informazioni può essere disattesa.

La centralità rivestita dallo scambio di dati e di informazioni di *law enforcement* giustifica, in seno agli accordi di Prüm e alla decisione n. 615 del 2008, la particolare attenzione riservata alla tematica della protezione dei dati, cui è dedicato un intero capitolo[143].

Anzitutto, gli Stati sono vincolati ad assicurare, tramite la legislazione interna, un livello di protezione almeno equivalente a quello della Convenzione del Consiglio d'Europa n. 108 del 28 gennaio 1981, del relativo protocollo addizionale dell'8 novembre 2001 e della raccomandazione R (87) 15 del Comitato dei ministri del Consiglio d'Europa sull'uso dei dati personali da parte delle forze di polizia. Oltre allo strumento del rinvio ad altre fonti, l'accordo e la decisione contengono alcune regole specifiche, che spaziano dalle garanzie assicurate all'interessato, ai doveri di aggiornamento e correzione; dalle misure di sicurezza per evitare indebite intrusioni o adulterazioni, ai limiti di utilizzabilità delle informazioni archiviate[144]. Com'è agevole comprendere, l'innesto di uno statuto dell'autodeterminazione informativa in seno allo stesso accordo che contempla una forma di disponibilità delle informazioni si rivela una scelta efficace, soprattutto alla luce

143 Il Capitolo VII del Trattato; il Capo 6 della decisione del Consiglio.

144 Sul tema vedasi, per maggiori dettagli, *infra*, A. Marandola, *op. cit.*, § 5.

della clausola[145] secondo cui lo scambio di informazioni ai sensi del Trattato di Prüm o della decisione 2008/615/GAI potrà avvenire solo tra quei Paesi che abbiano implementato nella propria legislazione nazionale tutte le disposizioni di tutela contenute nel Capitolo VII del primo o nel Capo 6 della seconda.

In conclusione, preme soffermarsi brevemente sull'art. 1, par. 4, del Trattato, che, già dalla primavera del 2005, preannuncia iniziative intese alla «trascrizione» delle disposizioni del Trattato di Prüm «nel quadro giuridico dell'Unione europea, sulla base di una valutazione dell'esperienza acquisita grazie all'attuazione del Trattato stesso». Ebbene, va detto che la Presidenza (tedesca) dell'Unione europea ha avviato un intenso dibattito sul punto nel gennaio 2007, raccogliendo ampi consensi circa la possibilità della ricezione dell'*acquis* di Prüm nel "terzo pilastro" dell'UE[146]. In questo clima favorevole, tredici Stati membri hanno avanzato (il 6 febbraio 2007) un'iniziativa formale, sottoscrivendo una bozza di decisione del Consiglio GAI, volta all'integrazione nel "terzo pilastro" delle «non-Schengen-relevant provisions of the Prüm Treaty», cui ne succederà una seconda, pressoché pedissequa nei contenuti, ma sottoscritta da quindici Stati membri[147]. Così, in linea con le determinazioni del Comitato di coordinamento e con le suddette iniziative legislative, la Presidenza ha invitato formalmente il Consiglio a raggiungere un'intesa politica[148], affinché le «non-Schengen-relevant provisions of the Prüm Treaty» siano integrate nel *legal framework* del "terzo pilastro" dell'Unione europea[149]. La Presidenza si è rivolta anche al Parlamento, in-

---

145 Contenuta nell'art. 34, par. 2, del Trattato e nell'art. 25, par. 2, della decisione.

146 Nella «Relazione sull'attuazione del programma dell'Aia per il 2006» (COM (2007) 373 def., 3 luglio 2007, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0373:FIN:IT:PDF>), la Commissione afferma che l'iniziativa tedesca in parola potrebbe essere considerata un'applicazione parziale del principio di disponibilità. Analogamente, l'accesso al VIS da parte delle autorità di polizia rappresenterebbe, secondo la Commissione, un passo avanti verso l'applicazione di tale principio (in argomento, cfr. la proposta di decisione quadro della Commissione, COM (2005) 600 def., 24 novembre 2005). F. Gandini, *op. cit.*, p. 57, premesso che il trattato dedica la massima attenzione alla prevenzione delle minacce all'ordine e alla sicurezza pubblica e alla prevenzione di talune condotte criminali, tra cui spicca il terrorismo, afferma che, mentre la prevenzione delle seconde rientra a pieno titolo tra i compiti dell'Unione (art. 29, par. 2, TUE), così non è per la prevenzione delle minacce all'ordine e alla sicurezza pubblica. Sicché, quest'ultimo tema potrebbe risultare critico nella prospettiva del recepimento nell'UE.

147 Sempre del febbraio 2007 (in *GUUE*, C 71, 28 marzo 2007, p. 35). Merita segnalarsi che, rispetto al trattato originario, le bozze di decisione del Consiglio accantonano la figura degli *air marshals* (artt. 17 sg.), le misure relative alla lotta contro la migrazione illegale (artt. 20 sgg.) e le regole circa la cooperazione su richiesta (art. 27); quanto alle «misure in caso di pericolo imminente» (art. 25), va detto che queste, contemplate nella "bozza dei tredici", scompaiono nella proposta a quindici teste.

148 *Documento del Consiglio n. 6220/07*, 9 febbraio 2007, <http://register.consilium.europa.eu/pdf/it/07/st06/st06220.it07.pdf>.

149 Degne di attenzione *in parte qua*, se non altro per la particolare carica politica, anche le conclusioni del Consiglio europeo di Bruxelles del giugno 2007 (in <http://www.consilium.europa.eu/ueDocs/cms__Data/docs/pressData/it/ec/94947.pdf>): «Si dovrà continuare a

vitandolo a sottoscrivere un parere circa le bozze di decisione in commento; ciò che è avvenuto nel giugno 2007[150], a mezzo di una risoluzione legislativa sostanzialmente adesiva nei confronti delle iniziative statuali, sia pure contemplando taluni emendamenti[151].

Prodromo della recente adozione, un documento del Consiglio che incorpora una bozza di decisione, la cui matrice è rappresentata, essenzialmente, dall'articolato proposto, nel febbraio 2007, dai quindici Stati membri[152]. Da qui, l'ultimo *step*, e cioè l'approvazione della più volte menzionata decisione 2008/615/GAI[153]. Al qual riguardo, vale la pena di osservare che la scelta di fondare l'incorporazione delle regole di Prüm su una decisione, anziché su una decisione quadro, potrebbe trovare giustificazione nella possibilità che solo la prima offre (a mente dell'art. 34, par. 2, lett. *c*) TUE) di adottare le misure necessarie per l'attuazione anche a maggioranza qualificata[154].

9. La decisione quadro sul principio di disponibilità delle informazioni in "terzo pilastro" (2006/960/GAI)

La prospettiva, tracciata dal Programma dell'Aia, della circolazione capillare delle informazioni fra autorità di *law enforcement* ha rappresentato un difficile banco di prova per le istituzioni europee. In particolare, il Consiglio si è trovato, col passare del tempo, al cospetto di uno scenario sempre più intricato: sul fronte della tutela del dato personale in "terzo pilastro", una proposta di decisione quadro che ha da subito catalizzato perplessità, obiezioni e solo tiepidi consensi (tanto che un dibattito, protrattosi per oltre tre anni, non è comunque valso ad approdare una soluzione condivisa); nell'ottica del principio di disponibilità, una progressiva sedimentazione di iniziative, dato che alla più risalente proposta svedese e a

---

compiere sforzi particolari per rafforzare la cooperazione di polizia e giudiziaria e la lotta contro il terrorismo. I cittadini europei si aspettano che l'UE ed i suoi Stati membri agiscano in modo deciso per preservare la loro libertà e sicurezza, in particolare nella lotta contro il terrorismo e la criminalità organizzata. La recente decisione di integrare le disposizioni fondamentali del trattato di Prüm nel quadro giuridico dell'Unione europea aiuterà ad intensificare la cooperazione transfrontaliera di polizia».

150 *Documento n. P6__TA(2007)0228*, 7 giugno 2007, in <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2007-0228+0+DOC+WORD+V0//IT>.

151 Sul percorso di avvicinamento dell'Unione europea all'*acquis* di Prüm, v. *infra*, A. Marandola, *op. cit.*, § 1 .

152 *Documento del Consiglio n. 11896/07*, 17 settembre 2007, in <http://register.consilium.europa.eu/pdf/it/07/st11/st11896.it07.pdf>.

153 In *GUUE*, L 210, 6 agosto 2008, p. 1. La decisione è entrata in vigore il 26 agosto 2008.

154 L'opzione ha costituito oggetto di critiche da parte del Parlamento europeo, che nella risoluzione legislativa citata *supra*, nel testo, ha proposto un emendamento inteso a riqualificare la fonte come decisione quadro.

quella della Commissione, devono affiancarsi, per ragioni di affinità contenutistica, gli accordi di Prüm e altri strumenti giuridici, quali ad esempio la decisione relativa allo scambio d'informazioni estratte dal casellario giudiziale[155].

Ad ogni modo, la decisione quadro sul principio di disponibilità è venuta alla luce nel dicembre 2006[156], a testimonianza che, su certi temi, il consesso degli esecutivi nazionali fatica meno che altrove a raggiungere un accordo unanime. Non vanno comunque dimenticate le contingenze storiche che, con ogni probabilità, hanno accelerato la formazione di tale consenso: si allude, in particolare, agli attentati terroristici del settembre 2001 negli Stati Uniti d'America, del marzo 2004 in Spagna e del luglio 2005 nel Regno Unito. Che non si tratti di deboli spinte motivazionali lo suggerisce il fatto che viene qui in gioco un settore, quello dell'attività di polizia e giudiziaria in materia penale, in cui è tradizionalmente molto radicato il sentimento di "gelosia" dei Paesi membri – se non addirittura delle singole autorità di *law enforcement* – nei confronti dei risultati ottenuti e degli obiettivi raggiunti "sul campo". Ne discende, sovente, una certa ostilità verso forme di collaborazione intense e prolungate nel tempo: si è fatto giustamente notare che, in quest'ambito, i governi nazionali tendono ad «accordare preferenza o manifestare minori resistenze nei confronti di iniziative puntuali […], piuttosto che nei confronti di un disegno organico, di ampio respiro e di lunga durata, svincolato dalla contingenza e dalle emergenze quotidiane»[157]. Ciò che spiega come non si potesse dare per scontata la tempestiva approvazione di una disciplina generale *in subiecta materia*.

L'*incipit* della decisione quadro n. 960 del 2006 ribadisce un concetto ormai sedimentato: l'obiettivo di assicurare ai cittadini dell'Unione un livello elevato di sicurezza richiede una più stretta cooperazione fra «le autorità degli Stati membri incaricate dell'applicazione della legge» e la base di partenza per tale cooperazione non può che essere lo scambio di informazioni e *intelligence*. In uno spazio in cui sono stati aboliti i controlli alle frontiere interne, si reputa cioè irrinuncia-

---

155 V. *amplius*, *infra*, M. Gialuz, "Il casellario giudiziario europeo: una frontiera dell'integrazione in materia penale".

156 La decisione quadro (in *GUUE*, L 386, 29 dicembre 2006, p. 89) è entrata in vigore il 30 dicembre 2006 (vi dedica brevi cenni B. Piattoli, *Diritti fondamentali: obiettivi e programmi dell'Unione europea in materia di giustizia penale*, in "Diritto penale e processo", 2007, p. 549). In tema, merita di essere ricordato il parere reso dal Garante europeo per la protezione dei dati nel febbraio 2006 (in *GUUE*, C 116, 17 maggio 2006, p. 8). Chiamato a esprimersi sulla proposta di decisione quadro n. 490 del 2005, il Garante esordiva spiegando che la molteplicità di iniziative appena ricordate nel testo sconsigliava di esaminare la proposta della Commissione in modo isolato, dovendosi piuttosto tener conto dell'esistenza di altre strategie di avvicinamento al tema dello scambio di informazioni di *law enforcement* e, soprattutto, non potendosi trascurare la tendenza, già emersa in seno al Consiglio, a preferire queste ultime rispetto all'approccio generale sposato dalla Commissione. Su queste basi, il GEPD vaticinava, correttamente, che la proposta della Commissione avrebbe potuto non essere nemmeno discussa in seno al Consiglio.

157 Testualmente, L. Salazar, *La lotta alla criminalità nell'Unione*, cit., p. 3527.

bile uno sforzo inteso a semplificare e favorire il tempestivo accesso a informazioni accurate e aggiornate, affinché le autorità competenti siano effettivamente messe in condizione di individuare, prevenire e indagare su attività criminali[158].

Da questi passaggi di esordio[159] si evince che il Consiglio concepisce il principio di disponibilità come uno strumento utile, sia sul piano della prevenzione dei reati, cioè quello che coinvolge in modo pressoché esclusivo le autorità di polizia, sia su quello della repressione, in cui giocano un ruolo solidale le autorità di polizia e quelle giudiziarie. E, coerentemente, l'art. 2 stila precise definizioni *in parte qua*: per «operazione di intelligence criminale», si intende la fase nella quale un'autorità competente incaricata dell'applicazione della legge ha facoltà di raccogliere, elaborare e analizzare informazioni su reati o attività criminali, al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti; si parla, invece, di «indagine penale» rispetto a una fase procedurale nella quale le autorità incaricate dell'applicazione della legge o le autorità giudiziarie competenti adottano misure per individuare e accertare i fatti, le persone sospette e le circostanze in ordine a uno o più atti criminali accertati, *id est* in ordine a una o più notizie di reato.

Sennonché, a polarizzare gli effetti del principio di disponibilità, anche nel momento repressivo (quello dell'indagine penale), sulle sole autorità di polizia è un duplice ordine di fattori. In primo luogo, l'individuazione della base giuridica dell'atto, ove compare l'art. 30, non l'art. 31 TUE: il Consiglio dimostra, così, di occuparsi della cooperazione di polizia, non di quella *stricto sensu* giudiziaria[160]. In secondo luogo, un accostamento testuale, in seno al "considerando" n. 5 e al succitato art. 2, tra i *nomina iuris* «autorità incaricate dell'applicazione della legge» («law enforcement authorities») e «autorità giudiziarie» («judicial authorities»), a suggerire che le seconde non rientrano, per il Consiglio, nella vaga

---

158 In materia, vedasi anche la decisione 2005/671/GAI, del 20 settembre 2005 (in *GUUE*, L 253, 29 settembre 2005, p. 22) sullo scambio di informazioni e sulla cooperazione concernente i reati di terrorismo, la quale prevede specifiche modalità di trasmissione di informazioni relative ai reati terroristici attraverso il coinvolgimento di Europol ed Eurojust. Quanto alle informazioni concernenti le armi da fuoco, cfr. il Protocollo sul traffico di tali armi, correlato alla c.d. Convenzione di Palermo; in argomento, F. Spiezia, "Il Protocollo sul traffico di armi da fuoco", in *Criminalità organizzata transnazionale*, cit., pp. 478 sgg. Infine, è del 6 novembre 2007 una proposta di decisione quadro, avanzata dalla Commissione (COM (2007) 654 def., <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:IT:PDF>), relativa all'utilizzo dei dati del codice di prenotazione (Passenger Name Record, PNR) per finalità di prevenzione e repressione dei reati. In materia, cfr. *supra*, M. Gialuz, "La cooperazione informativa quale motore del sistema europeo di sicurezza", § 4.

159 Ma si veda anche il "considerando" n. 7, che *claris verbis* allude alla possibilità di chiedere ed ottenere informazioni e *intelligence* da altri Stati membri in vari stadi delle operazioni di *law enforcement*, dalla fase di raccolta di *intelligence* criminale alla fase d'indagine penale.

160 Certo, non va dimenticato che le attività repressive si svolgono, normalmente, sotto la direzione di un magistrato inquirente. È lecito, perciò, attendersi che quest'ultimo possa ampiamente beneficiare, seppure in via mediata, dei nuovi canali aperti per le forze di polizia.

nozione di *law enforcement authorities*. Meno perspicuo, viceversa, l'art. 2 lett. *a*), il quale, sebbene fornisca un'interpretazione "autentica" di quest'ultimo concetto, risulta ambiguo, dato che si riferisce non solo alla polizia e ai servizi doganali, ma anche ad altre autorità nazionali che, in forza della legislazione interna, sono competenti a individuare, prevenire e indagare su reati o attività criminali, esercitare l'autorità e adottare misure coercitive nell'ambito di tali funzioni: una definizione tanto generica da non risultare idonea, di per sé sola, a sceverare le autorità di polizia da quelle giudiziarie. Piuttosto, la norma in commento gioca un ruolo-chiave in senso negativo, quando esclude *claris verbis* «i servizi o le unità che si occupano specificamente di questioni connesse alla sicurezza nazionale» («agencies or units dealing expecially with national security issues»), in tal modo prendendo posizione su un tema che aveva suscitato più di una perplessità a fronte della proposta svedese e di quella della Commissione, reticenti al riguardo.

Dunque, nonostante sia l'iniziativa svedese il referente principe della decisione quadro in commento (è inequivocabile il riferimento ad essa contenuto nell'*incipit*), in punto "*law enforcement authorities*" l'opzione estensiva del Regno di Svezia non viene pienamente accolta: se quest'ultima includeva, sia pure condizionatamente, anche le autorità giudiziarie, il consesso degli esecutivi nazionali limita la sfera applicativa del principio di disponibilità ai rapporti fra le autorità di polizia, allineandosi, sotto questo prospetto, alla proposta della Commissione. Inoltre, sancisce in termini univoci che restano esclusi dall'area d'impatto del principio in parola i c.d. servizi segreti.

Sul piano funzionale, come già anticipato, vengono in gioco sia il momento della prevenzione dei reati e dell'individuazione di *notitiae criminis*, sia quello dell'eventuale repressione; con una precisazione che è d'uopo su quest'ultimo fronte. La decisione quadro non impone, infatti, alcun obbligo per gli Stati membri di fornire informazioni e *intelligence* da utilizzare «come prove dinanzi ad un'autorità giudiziaria» («as evidence before a judicial authority»), né di conferire il diritto a utilizzarle a tal fine. Perciò, le informazioni, ottenute in virtù del principio di disponibilità, potranno essere sfruttate per attività d'*intelligence* o nel corso delle indagini preliminari, mentre, per utilizzarle come prove nel corso di un processo *stricto sensu*, s'imporrà il ricorso agli ordinari strumenti di cooperazione giudiziaria, se del caso chiedendo il consenso dello Stato d'origine[161]. Sul punto, il Consiglio non si discosta né dall'iniziativa svedese né da quella della Commissione, forgiando una possibile causa d'inutilizzabilità "funzionale" o "fisiologica", concernente le informazioni di *law enforcement* ottenute da oltre confine.

Su queste basi è quindi possibile fissare qualche punto fermo, rimarcando che la decisione quadro n. 960 del 2006: *a*) si riferisce alle sole autorità di polizia (con esclusione dei servizi segreti), non all'autorità giudiziaria; *b*) concerne

161 Tale consenso non sarà necessario solamente qualora lo Stato membro richiesto abbia già dato, al momento della trasmissione originaria, la propria autorizzazione a utilizzarle a tale scopo.

le operazioni di *intelligence* criminale oltreché la fase, immediatamente successiva all'eventuale acquisizione di una *notitia criminis*, delle indagini preliminari; *c*) non pervade il momento *stricto sensu* processuale, cioè quello che presuppone un'accusa formalmente elevata e un'attività di istruzione probatoria che la riguarda; ivi, la decisione quadro non produce effetti, sicché i meccanismi di circolazione transfrontaliera delle prove restano regolati dagli ordinari strumenti di cooperazione internazionale o da altre fonti europee[162].

Conformemente all'iniziativa del Regno di Svezia e differenziandosi da quella della Commissione, la decisione quadro, parlando di informazioni e *intelligence*, allude a concetti amplissimi: vi rientra, non solo qualsiasi tipo di informazioni o dati detenuti dalle stesse autorità di *law enforcement*, ma anche qualsiasi genere di informazioni o dati detenuti da autorità pubbliche o da enti privati che siano accessibili alle autorità incaricate dell'applicazione della legge senza il ricorso a mezzi coercitivi. Seguendo queste direttive, nell'ottobre 2008, la Presidenza del Consiglio UE ha diramato un compendio di «Draft Guidelines on the implementation of the 'Swedish Framework Decision'»[163], il cui Allegato III distingue: *I*) «information/databases managed and directly accessible by law enforcement authorities»; *II*) «information/databases directly accessible by law enforcement authorities but managed by other authorities»; *III*) «information/databases accessible by law enforcement authorities but managed by private entities»; *IV*) «information/databases that always require a judicial authorisation to be accessed by law enforcement authorities». Una quadripartizione, questa, che mette bene in chiaro il grado di pervasività del principio di disponibilità, in sostanza afferente a tutte le categorie di informazioni cui, in un modo o nell'altro (direttamente, previa richiesta motivata, in base ad autorizzazione giudiziale), le autorità di polizia nazionali possono accedere senza ricorrere all'uso di mezzi coercitivi.

La decisione quadro non impone, invece, alcun obbligo agli Stati membri di raccogliere e conservare informazioni e *intelligence* al precipuo scopo di fornirle alle autorità competenti di altri Stati membri, né impone di ottenere informazioni che siano state richieste, ove non fossero *ab ovo* disponibili.

Ne discende un duplice corollario: quanto alle informazioni di *law enforcement* già archiviate all'interno dei confini nazionali, il principio di disponibilità rivela un'efficacia sostanzialmente onnipervasiva; viceversa, esso non innesca obblighi di raccolta e collezione al solo fine della successiva condivisione. La decisione quadro n. 960, in altri termini, impone di condividere ciò di cui si dispone, non di raccogliere e archiviare allo scopo di condividere.

---

162 Il tema è approfondito *infra* da M. Gialuz, "Banche dati europee e procedimento penale italiano", § 3.

163 *Documento del Consiglio n. 13942/08*, 10 ottobre 2006, <http://www.statewatch.org/news/2008/oct/eu-exchange-of-crim-data-swedish-13942-08.pa.pdf>.

Per il Consiglio UE, "principio di disponibilità" significa che gli Stati membri dovranno provvedere affinché la comunicazione di informazioni e *intelligence* alle autorità competenti di altri Stati membri non sia soggetta a condizioni più rigorose di quelle applicabili a livello nazionale. Perciò, se all'interno di uno Stato membro le autorità di *law enforcement* possono accedere a certe categorie di informazioni o *intelligence* senza bisogno di autorizzazioni da parte di autorità terze (in particolare, dell'autorità giudiziaria), allora lo Stato non subordinerà ad alcuna autorizzazione l'accesso alle stesse categorie d'informazioni ad opera delle autorità di polizia straniere. Se, invece, la legislazione nazionale dello Stato membro richiesto consente alle proprie autorità di *law enforcement* di accedere solo previa autorizzazione da parte dell'autorità giudiziaria, tale autorizzazione dovrà rilasciarsi anche in favore della polizia straniera. In concreto, sarà l'autorità (nazionale) di *law enforcement* interpellata a fare da intermediario, chiedendo all'autorità giudiziaria competente l'autorizzazione ad accedere e a scambiare le informazioni richieste dall'estero: per l'adozione della propria decisione, l'autorità giudiziaria applicherà le stesse regole valide per i casi meramente interni[164].

Questa *par condicio* fra autorità di polizia nazionali e straniere non risulta condizionata dall'esistenza di una "omogeneità funzionale" tra le autorità di *law enforcement* coinvolte. Stando alla decisione quadro in commento, gli Stati comunicheranno, sì, l'elenco delle proprie autorità di *law enforcement* (al proposito, le summenzionate *Draft Guidelines* del 10 ottobre 2008 contengono un apposito Allegato IV, funzionale alla descrizione, ad opera dei singoli Paesi, delle *competent authorities*), ma alla redazione di tale "inventario" non seguirà l'elaborazione di una "tavola di corrispondenza" su scala europea. La decisione quadro non segue, in altre parole, l'iniziativa della Commissione[165] nel pretendere che i singoli Stati UE comunichino ad un organismo *ad hoc* l'elenco delle proprie autorità di polizia, precisandone compiti e funzioni, affinché risulti possibile identificare, per ogni autorità nazionale, l'omologa d'oltre confine (polizia dello Stato A-polizia dello Stato B, guardia di finanza dello Stato C-guardia di finanza dello Stato D), allo scopo di parametrare le possibilità di accesso ai dati. Nella decisione quadro del Consiglio, il riferimento è fatto, genericamente, alle autorità incaricate dell'applicazione della legge. Tanto è vero che, in modo piuttosto eloquente, il "considerando" n. 5, riproducendo il quinto "considerando" svedese, definisce «importante che le possibilità» per tali autorità di ottenere informazioni e *intelligence* da altri Stati membri «siano viste orizzontalmente e non in termini di differenze in ordine al tipo di reato o alla suddivisione delle competenze tra autorità incaricate dell'applicazione della legge o autorità giudiziarie». Questo significa che un'au-

164 Se il dato, cui si riferisce la richiesta straniera, era già stato oggetto di un *cross border exchange*, sarà necessario che l'autorità interpellata ottenga il consenso all'ulteriore trasmissione transfrontaliera da parte dello Stato d'origine.

165 V. *supra*, § 4.

torità di *law enforcement* non dovrà necessariamente misurarsi con le funzioni e i compiti del suo *alter ego* straniero.

Onde evitare un utilizzo indiscriminato dell'apparato circolatorio, la decisione quadro fa leva sullo strumento della richiesta motivata: le informazioni e l'*intelligence* possono essere richieste da un'autorità di *law enforcement*, laddove vi sia «motivo di fatto di ritenere» («factual reasons to believe») che informazioni e *intelligence* pertinenti siano disponibili in un altro Stato membro. A mente dell'art. 5 (esplicato dall'Allegato B, contemplante un formulario che deve essere utilizzato dalla parte instante), la richiesta specificherà i motivi che la sorreggono e illustrerà quali finalità le informazioni e l'*intelligence* (eventualmente) trasmesse siano destinate ad assolvere, chiarendo il nesso tra le finalità in parola e la persona cui le informazioni si riferiscono.

Quanto alle modalità dello scambio, l'art. 6, par. 1 dispone, in maniera alquanto sibillina, che esso può aver luogo tramite «qualsiasi canale esistente ai fini della cooperazione internazionale in materia di applicazione della legge» («via any existing channels for international law enforcement cooperation»), avendo cura di coinvolgere anche Europol (in conformità alla relativa convenzione) ed Eurojust (in conformità alla rispettiva decisione), ogniqualvolta lo scambio riguardi un reato o un'attività criminale di loro competenza[166]. Sono ancora le *Draft Guidelines* presidenziali dell'ottobre 2008 a fornire utili chiarimenti. Segnatamente, vengono presi a riferimento e *claris verbis* menzionati quelli che, ad oggi, sono considerati i canali più importanti ai fini della *law enforcement cooperation* («SIRENE; ENU/EUROPOL Liaison Officer; INTERPOL NCB; Liaison officers; mutual administrative international customs assistence ("Naples II Convention"); bilateral cooperation channels») e si precisa che, in via di regola, lo Stato richiesto risponderà utilizzando il medesimo canale prescelto dall'autorità instante, avendo cura di avvertire tempestivamente quest'ultima ove, per giustificati motivi, debba ricorrere ad uno strumento cooperativo diverso. Non manca, poi, l'elencazione di una serie di criteri che devono essere seguiti al momento della scelta del canale da utilizzarsi.

Ebbene, è facile notare come, sui versanti da ultimo esplorati, la decisione quadro si riveli estremamente cauta, se non rinunciataria: da un lato, fa leva sul meccanismo della domanda-risposta[167]; dall'altro, ricorre, per far circolare i dati

166 Lo scambio, in realtà, può anche avvenire spontaneamente: fatto salvo l'art. 10, l'art. 7 afferma che le autorità competenti incaricate dell'applicazione della legge, senza che sia necessaria alcuna richiesta preventiva, forniscono alle autorità competenti per l'applicazione della legge di altri Stati membri interessati le informazioni e l'*intelligence* pertinenti, qualora sussistano ragioni di fatto per ritenere che dette informazioni e *intelligence* possano contribuire all'individuazione, alla prevenzione o all'indagine riguardanti i reati di cui all'art. 2, par. 2, della decisione quadro 2002/584/GAI. La determinazione delle modalità di questo scambio spontaneo è affidata alla legislazione nazionale dello Stato membro che fornisce le informazioni.

167 Gli Allegati B ed A, rispettivamente, contemplano i formulari che devono essere utilizzati per chiedere e rispondere.

in virtù del principio di disponibilità, ai "canali" di comunicazione già esistenti. In tal modo, il Consiglio si pone agli antipodi rispetto alla Commissione che, nella propria iniziativa dell'ottobre 2005, delineava scenari innovativi, con archivi di informazioni o di dati di indice, compulsabili direttamente on-line. Ma nemmeno recepisce *in toto* il modello svedese che, se a tutte lettere coinvolgeva il SIS, il SID ed Europol ("funzionalizzandoli" anche alla circolazione dei dati giusta il principio di disponibilità), concepiva delle alternative, come lo scambio diretto tra «le autorità centrali o locali incaricate dell'applicazione della legge»[168]. *In parte qua*, la decisione quadro del Consiglio opta invece per l'astensione: descritta per sommi capi la quintessenza del principio di disponibilità, non si addentra nel tema relativo alle modalità di circolazione del dato, rifacendosi a canali creati *aliunde*.

Questa politica di "canalizzazione", incentrata sul meccanismo della domanda-risposta (non dell'accesso diretto on-line) e sul ricorso ai sistemi informativi esistenti (da utilizzarsi come cinghie di trasmissione), non traduce in atto i profili di maggiore originalità insiti nel Programma dell'Aia che, gioverà ricordarlo, nel delineare un «approccio innovativo nei confronti dello scambio transfrontaliero di informazioni», pone alla ribalta «l'accesso reciproco o l'interoperabilità [tra le] basi di dati nazionali». Non è da escludere che la scelta del Consiglio UE sia stata dettata (anche) da una volontà di semplificazione e di risparmio in termini economici, dato che lo schema domanda-risposta e il ricorso a SIS, SID, Europol, Interpol come veicoli delle stesse, evita agli Stati l'ingente sforzo di istituire archivi di dati di indice o di assicurare alle autorità di tutti i Paesi europei l'accesso diretto on-line ai propri database nazionali, secondo il modello prospettato dalla Commissione nell'ottobre 2005. Né deve sfuggire che "accesso diretto on-line" è sinonimo di "disponibilità pura", perché consente all'autorità straniera di compulsare un archivio, prescindendo da qualsiasi collaborazione con le autorità dello Stato d'origine: il sentimento di "gelosia" cui si è fatto cenno in apertura di paragrafo potrebbe allora mettere in luce un'ulteriore spinta motivazionale contraria al recepimento delle scelte più coraggiose, propugnate dalla Commissione nell'autunno 2005.

La decisione quadro in commento non manca di definire, sia i termini entro cui lo scambio deve avvenire, sia le possibili ragioni di un rifiuto della trasmissione.

Sul primo fronte, l'art. 4 scandisce ritmi molto diversificati, con oscillazioni che vanno dai quattordici giorni, previsti in via di regola, alle otto ore, in riferimento alle richieste urgenti relative a specifiche categorie di reati. Più precisamente, viene tracciata una linea di demarcazione a seconda che le informazioni e l'*intelligence* riguardino o meno i reati di cui all'art. 2, par. 2, della decisione quadro 2002/584/GAI[169]. Se le informazioni rientrano nel suddetto *genus*, trattasi

---

168 Cfr. l'art. 7, par. 2, della proposta svedese.

169 La decisione quadro, risalente al 13 giugno 2002 (in *GUCE*, L 190, 18 luglio 2002, p. 1) e relativa al mandato di arresto europeo, contempla un'ampia schiera di illeciti, identificati con un più o meno generico riferimento alla tipologia della condotta criminale (terrorismo, tratta

di distinguere le richieste qualificate come urgenti nella rispettiva domanda e quelle non indicate come tali: nel primo caso, gli Stati membri sono chiamati ad assicurare l'apprestamento di procedure che consentano di rispondere entro otto ore dalla ricezione della domanda, sempre che le informazioni o l'*intelligence* siano conservate in una banca dati alla quale l'autorità richiesta può accedere direttamente[170]; nella seconda ipotesi (richiesta non urgente), lo *spatium temporis* si dilata a una settimana. Tutti gli altri casi soggiaciono a una disciplina uniforme: gli Stati membri provvedono a che le informazioni richieste siano comunicate entro quattordici giorni; se non saranno in grado di rispondere per tempo, le autorità interpellate informeranno del ritardo chi ha inoltrato la richiesta.

Sul secondo versante si colloca l'art. 10, par. 1, perentorio nello stabilire che l'autorità competente incaricata dell'applicazione della legge può rifiutare la trasmissione soltanto nell'ipotesi in cui sussistano «ragioni di fatto» per ritenere che la comunicazione: *a*) pregiudichi interessi fondamentali della sicurezza nazionale del proprio Stato, oppure *b*) metta a repentaglio il buon esito di un'indagine o di un'operazione di *intelligence* criminale in corso o la sicurezza di persone, ovvero *c*) sia palesemente sproporzionata o irrilevante per lo scopo per cui è stata richiesta. Peculiare, infine, il caso contemplato dal par. 2: la trasmissione diviene comunque facoltativa se riguarda un fatto che, nello Stato richiesto, è passibile di una pena privativa della libertà personale che non supera l'anno. In questo modo, si introduce una sorta di clausola di proporzionalità, sancendo che, se lo scambio non è immediatamente riconducibile alla prevenzione o al perseguimento di un reato di una certa gravità, all'obbligo di trasmettere (salvo tassative eccezioni) subentra la decisione adottata in base alle peculiarità del caso concreto.

Avvenuto l'attraversamento del confine, il trattamento delle informazioni sarà regolato dalle disposizioni in materia di protezione dei dati dello Stato membro ricevente: in quest'ultimo, le informazioni e l'*intelligence*, ottenute dall'estero, saranno considerate come *ab ovo* raccolte entro il perimetro nazionale. È difficile sottacere una notazione critica su questa soluzione adottata dalla decisione quadro n. 960. Infatti, in assenza di una decisione quadro concernente la tutela del dato personale nel "terzo pilastro" UE (*rectius*, concernente la tutela delle informazioni trattate per finalità di *law enforcement*, anche all'interno dei confini nazionali), quello appena descritto si risolve in un riferimento "in bianco", *id est* in un rinvio a discipline nazionali che, di fatto, potrebbero non esistere punto, ovvero che potrebbero rivelare marcate disomogeneità. Rimossa la patina superficiale, si coglie agevolmente la reale portata della clausola *de qua*, formalisticamente posta

---

di esseri umani, sfruttamento sessuale dei bambini e pornografia infantile, traffico illecito di stupefacenti e sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, corruzione, frode, *et cetera*).

170 Se l'autorità non è in grado di rispondere entro le summenzionate otto ore, dovrà fornire adeguata e tempestiva motivazione all'autorità instante, impegnandosi a comunicare le informazioni o l'*intelligence* nel più breve tempo possibile e, in ogni caso, entro tre giorni.

a salvaguardia dell'informazione trasmessa: trattasi di una scatola vuota, poiché, a livello europeo, non esisteva (fino all'inverno 2008) una fonte di riferimento che assicurasse uno standard di protezione generalizzato per l'informazione utilizzata all'interno dei confini nazionali nel quadro della lotta al crimine.

Diverso, invece, il discorso relativo al principio di "finalità limitata", connotato da una certa chiarezza d'intendimenti. Per il Consiglio, le autorità competenti dello Stato ricevente potranno utilizzare le informazioni e l'*intelligence* soltanto per gli scopi per i quali sono state fornite. Questa la regola, cui si affiancano due eccezioni. La prima concerne la prevenzione di un pericolo grave e immediato per la sicurezza pubblica, rispetto alla quale l'utilizzo *extra ordinem* è consentito in via generalizzata. La seconda fa perno su un'autorizzazione *ad hoc* rilasciata dello Stato membro che ha trasmesso i dati, il quale vi provvederà in ossequio alla propria legislazione nazionale.

Infine, meritano un cenno le esigenze correlate al tema della «riservatezza» («confidentiality»). Secondo l'art. 9, in ogni caso specifico di scambio di informazioni e *intelligence*, le autorità competenti incaricate dell'applicazione della legge tengono nel debito conto i requisiti di segretezza delle indagini. A tal fine, le autorità coinvolte, conformemente alle rispettive legislazioni nazionali, assicurano la riservatezza di tutte le informazioni e l'*intelligence* fornite, cui sia stato attribuito tale carattere.

10. Riflessioni conclusive

Non v'è dubbio che la libera circolazione di persone, merci e capitali nel territorio dell'Unione europea richieda l'apprestamento di adeguate misure di compensazione sul fronte della prevenzione e della repressione della criminalità. Lo stesso Trattato sull'Unione europea menziona a più riprese uno Spazio connotato da un trittico di paradigmi, in cui alla Libertà, si affiancano la Sicurezza e la Giustizia; concetti, questi ultimi, che evocano rispettivamente l'idea della prevenzione e della repressione dei reati. Perciò, non si può che accogliere con favore l'approvazione di una decisione quadro sul principio di disponibilità delle informazioni di *law enforcement*. Viceversa, la prolungata assenza di una disciplina generale concernente la protezione del dato personale ha creato uno squilibrio nell'assetto normativo del c.d. terzo pilastro dell'Unione europea cui solo con grave ritardo si è posto rimedio.

Lo pretendeva, innanzitutto, il rispetto per il diritto alla privacy e all'autodeterminazione informativa. Notazione, questa, valida a due livelli.

Statale *in primis*: perché i Paesi membri dell'Unione europea tendono oramai ad ascrivere a tali diritti un rango *meta*-legislativo, costituzionale, degno di considerazione anche quando ci si trovi al cospetto di esigenze di contrasto alla criminalità. Sicché appariva davvero poco responsabile l'atteggiamento dei rappresentanti dei governi che, in seno al Consiglio dell'UE, esprimevano il proprio voto

favorevole all'adozione di provvedimenti sulla cui ortodossia (vista l'unidirezionalità nel senso dello scambio delle informazioni) non era dato scommettere, ragionando secondo i canoni *meta*-primari interni ai rispettivi confini nazionali. Ciò che esponeva le scelte dei governi a un'ulteriore critica. Non va dimenticato, infatti, che, a livello statuale, la funzione legislativa compete ad organi istituzionali diversi, come i parlamenti. Donde la possibilità che questi ultimi, tenendo nel dovuto conto alcuni profili del diritto all'autodeterminazione informativa e in assenza di una disciplina europea di riferimento sul versante della tutela del dato, potessero in via di fatto vanificare il concetto di disponibilità, attuando la decisione quadro in materia con leggi diversificate e disomogenee.

Europeo *in secundis*: perché, nonostante i dubbi sulla valenza prescrittiva della c.d. Carta di Nizza e la non ancora avvenuta adesione dell'Unione europea alla CEDU, anche nel territorio dell'Unione l'autodeterminazione informativa è considerata un valore fondamentale. Perciò, le istituzioni europee (e, segnatamente, il Consiglio) rivelavano una certa incoerenza quando affiancavano a ispirate declamazioni di principio opzioni normative unilaterali sul fronte dell'*information sharing*.

Scarsa attenzione per la "tutela del dato", comunque, non significa soltanto oblio dell'interesse del singolo al riconoscimento di alcune garanzie di base, relative al trattamento dei dati che lo riguardano. All'assenza di una compiuta disciplina di riferimento *in parte qua* si associa anche la mancanza di garanzie concernenti le modalità di raccolta delle informazioni, la completezza degli archivi, il loro costante aggiornamento. Sfuma, cioè, quella dimensione "pubblicistica" della tutela dei dati personali che, affiancando la componente propriamente "soggettiva", contribuisce a ridurre il rischio che la cooperazione informativa si traduca in un fenomeno degenerativo. L'accelerazione sul solo binario della "disponibilità" delle informazioni rischiava di decretare un parziale fallimento di questa forma di cooperazione transfrontaliera: se la circolazione capillare di *law enforcement information* risulta inquinata da una congerie di dati scorretti o inattuali, irreparabilmente commisti agli altri, corretti e aggiornati, anche l'utilità dei secondi finisce per essere compromessa, e le attività preventive o repressive, oltre che coadiuvate, possono essere rallentate o addirittura fuorviate da un'ingovernabile massa spuria, in cui ciò che è preciso e attuale risulta difficilmente distinguibile da ciò che è approssimativo e superato.

Queste notazioni hanno, quale referente immediato, la sorte, uguale e contraria, che, nel biennio dicembre 2006-dicembre 2008, le proposte di decisione quadro hanno avuto, a seconda che si occupassero di disponibilità informativa o di protezione dei dati personali. Non può, allora, nascondersi che, dal giugno 2008, l'Unione europea ha dato vita a un'ulteriore complicazione dello scenario complessivo. Il recepimento degli accordi di Prüm nel *legal framework* del "terzo pilastro", infatti, prelude ad un potenziamento delle strategie cooperative in termini di *information sharing*, i cui effetti è arduo calcolare con esattezza.

In particolare, si delinea una sorta di effetto moltiplicatore per il principio di disponibilità. Da un lato, con l'istituzione di un *network* tra le banche dati cen-

tralizzate DNA, *fingerprints* e veicoli in tutti gli Stati membri, verranno posti finalmente in essere dei "motori di ricerca" preziosissimi per individuare, oltre confine, l'esistenza di informazioni utili sul versante della prevenzione e della repressione dei reati. In questo modo, l'*acquis* di Prüm colmerà (almeno per le tre summenzionate categorie di dati) un'evidente lacuna della decisione quadro n. 960 del 2006, la quale si limita a richiamare i canali di comunicazione già esistenti e a fare perno sul principio della domanda-risposta. D'altro canto, però, la stessa decisione quadro n. 960, introducendo la regola generale della disponibilità informativa, insisterà sulla seconda movenza dell'*information sharing* concepita a Prüm, *id est* quella che, come gli originari sette firmatari, la decisione 2008/615/GAI affida alla «legislazione nazionale dello Stato membro richiesto, comprese le disposizioni relative all'assistenza giudiziaria». In virtù della decisione quadro 2006/960/GAI, sarà proprio il diritto nazionale dei singoli Stati membri a doversi conformare al principio di disponibilità. Sicché, il fronte più debole degli accordi di Prüm potrebbe venire decisamente rinforzato dalle leggi attuative della disciplina approvata dal Consiglio UE nel dicembre 2006.

Per completezza, e tornando al tema della privacy, va comunque ribadito che sarebbe riduttivo imputare il ritardo nell'approvazione di una decisione quadro sulla tutela del dato in "terzo pilastro" alla sola strategia dei governi nazionali, propensi a non forgiare condizionamenti e vincoli per lo scambio di *law enforcement information*. Con tale (vera o presunta) volontà politica, si coniugano le effettive ambiguità e cedevolezze che inficiavano il testo elaborato *illo tempore* dalla Commissione. Ma, se questo è vero, suscita più di una perplessità il fatto che i ferventi lavori, protrattisi per oltre un triennio *in subiecta materia*, anziché aver condotto a un miglioramento della proposta originaria, sembrano aver seguito una parabola discendente, finendo per approdare a un articolato normativo rinunciatario, che premia opzioni minimaliste. Opinabile appare, soprattutto, la scelta di varare una decisione quadro dalla cui area d'impatto esula il trattamento *purely domestic* delle informazioni e dell'*intelligence* criminale: sul punto, è difficile dissentire dalle opinioni insistentemente espresse dal Garante europeo della protezione dei dati personali e dal Parlamento europeo.

Infine, un appunto di natura processuale. La forza d'urto e il grado di pervasività del principio di disponibilità, quando si discute di attività repressive (cioè incentrate su una *notitia criminis* rispetto alla quale le autorità di polizia e giudiziarie indagano), pongono un problema in termini di parità fra le parti del procedimento penale: tanto più fluente è la circolazione transfrontaliera di informazioni tra le autorità inquirenti, tanto più si acuisce il divario con la difesa dell'indagato, aggiungendo un nuovo capitolo al già scottante tema dei rapporti tra una difesa che (quanto alla dotazione di strumenti tecnico-giuridici) rimane "domestica" e un pubblico ministero e una polizia giudiziaria sempre più "europei". Né il punto dolente si esaurisce nella fase di ricerca e raccolta *cross-border* delle informazioni; ulteriore problema è quello della difesa "dalle" informazioni, una volta che gli inquirenti le abbiano raccolte oltre confine. Sotto questo pro-

spetto, la tempestiva e compiuta attuazione della neonata decisione quadro n. 977 rappresenterà un momento nevralgico, in quanto strumento-cardine per scongiurare (*ex ante*) la circolazione di informazioni scorrette o non aggiornate e per fornire (*ex post*) eventuali strumenti di reazione di cui possa beneficiare l'interessato, risalendo alla fonte originaria delle informazioni, accertando quali autorità in Europa ne abbiano fruito e a che scopi, coinvolgendo se del caso un'autorità garante o l'autorità giudiziaria.

Sempre sul piano del procedimento penale, merita un cenno la polarizzazione, *ex* decisione quadro 2006/960/GAI, del principio di disponibilità sulle sole autorità di polizia, con esclusione di un diretto coinvolgimento delle autorità giudiziarie (la proposta svedese deponeva in senso diverso ma, *in parte qua*, non è stata accolta dal Consiglio). Ne consegue un potenziale, leggero slittamento del baricentro delle indagini preliminari verso la polizia giudiziaria, a "discapito" del pubblico ministero che, stando alla decisione quadro n. 960 (non così, invece, la decisione 2008/615/GAI), in punto "ricerca e condivisione transfrontaliera di informazioni" dovrà fare leva sulle potenziate capacità investigative dei soggetti che coordina e dirige, non potendo procedere autonomamente (se non ricorrendo ad altri strumenti cooperativi).

Si può, quindi, concludere che, all'apprezzamento per i sensibili progressi compiuti in Europa sul piano della cooperazione di polizia e giudiziaria in materia penale nelle forme dell'*information sharing*, si affiancano alcune perplessità relative al tema dell'autodeterminazione informativa. Una disciplina generale della tutela del dato personale scambiato fra le autorità di *law enforcement* è necessaria, sia in una prospettiva "pubblicistica" (attenta quindi alla qualità e non solo alla quantità dei dati condivisi, in vista di un effettivo potenziamento della *law enforcement cooperation*), sia "soggettiva" (cioè concentrata sul soggetto cui le informazioni si riferiscono), declinabile quest'ultima, nel sistema del processo penale, in termini di rispetto del principio di parità tra le parti e di inviolabilità del diritto di difesa. L'adozione della decisione quadro sulla tutela del dato (2008/977/GAI) impone di attendere le scelte che, a livello nazionale, i singoli Paesi compiranno in chiave attuativa. Di certo, il turbolento e ondivago itinerario che ha preceduto l'approvazione del nuovo testo mette in chiara luce alcuni punti deboli della nuova disciplina. Fra tutti, spicca la scelta di non includere nell'area d'impatto della decisione quadro il trattamento "*purely domestic*", così da imporre una rigida limitazione degli standard europei alle informazioni che valicano i confini: la sensazione è che il fenomeno della protezione del dato non si presti a un tal genere di astrattismi.

Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia

FEDERICO DECLI
Avvocato in Trieste
(paragrafi 3, 4, 6)

GABRIELLA MARANDO
Dottoranda di ricerca in Scienze penalistiche
Università di Trieste
(paragrafi 1, 2, 5)

1. Le banche dati dell'Unione europea quale strumento fondamentale della cooperazione informativa.

Nel quadro degli strumenti vòlti alla realizzazione di uno spazio di libertà, sicurezza e giustizia nell'ambito dell'Unione europea[1], la cooperazione è delineata dal legislatore europeo nella duplice dimensione afferente, l'una, al settore della prevenzione del crimine (art. 30 TUE) e, l'altra, alla fase di accertamento e repressione dei reati (art. 31 TUE). Punto di convergenza di entrambe le prospettive è rappresentato dalla necessaria predisposizione di strumenti e canali di scambio di dati e informazioni tra le competenti autorità statuali ed europee, al fine di consentire la formazione di un quadro conoscitivo comune funzionale alla predisposizione di una strategia investigativa e alla successiva attività di formazione della prova, in vista della realizzazione del principio del mutuo riconoscimento delle decisioni giudiziali.

Il paradigma della cooperazione informativa si realizza secondo differenti moduli operativi.

Sotto un primo profilo, attinente alla cooperazione cd. orizzontale tra le competenti autorità degli Stati membri, una linea di demarcazione separa le strutture operative di matrice tradizionale che prefigurano, sulla scorta del modello delineato dalla Convenzione Schengen, uno scambio di informazioni "mediato" dall'intervento di un'autorità centrale europea, dagli strumenti di più recente introduzione che, in attuazione del principio di disponibilità coniato dal Programma dell'Aia del 2004[2], consentono una trasmissione di dati immediata e diretta tra le autorità dei singoli Stati[3].

Pur innovando il panorama della cooperazione informativa nella direzione dello scambio diretto tra gli Stati, il Programma dell'Aia non oblitera gli altri canali informativi mediati esistenti in tale settore, ponendo, al contrario, le

---

1 Nel percorso che porta all'edificazione di uno spazio giudiziario europeo vengono generalmente individuate le due direttrici della cooperazione e della armonizzazione dei sistemi normativi: si leggano, *ex multis*, E. Aprile, *Diritto processuale penale europeo e internazionale*, Padova, Cedam, 2007, p. 25; A. Bernardi, *Strategie per l'armonizzazione dei sistemi penali europei*, in "Rivista trimestrale di diritto penale dell'economia", 2002, p. 789; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale. Verso un sistema integrato di forme e strumenti di collaborazione*, Milano, Giuffrè, 2007, p. 296; L. Salazar, *La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il Programma dell'Aia*, in "Cassazione penale", 2004, p. 3510.

2 Sul principio di disponibilità, si veda, *amplius*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea".

3 Tra gli strumenti normativi che danno attuazione al principio di disponibilità enunciato dal Programma dell'Aia, ponendo le basi per una cooperazione diretta tra le autorità degli Stati membri, si rinvengono la decisione quadro n. 960 del 2006 (sulla quale, si veda *supra*, S. Ciampi, *op. cit.*, § 9), e la decisione quadro 2008/615/GAI, che recepisce il Trattato di Prüm (sulla quale, si rinvia ad A. Marandola, "*Information sharing* nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione").

premesse per una sinergia tra questi ed il principio di disponibilità. All'uopo, il punto 2.1 prevede che «lo scambio di informazioni dovrebbe sfruttare appieno le nuove tecnologie e i metodi utilizzati dovrebbero essere adeguati ai diversi tipi di informazioni, se del caso attraverso [...] l'accesso diretto (on-line), anche per l'Europol, alle basi di dati centrali dell'UE già esistenti» e che «nuove basi di dati centralizzate a livello europeo dovrebbero essere create soltanto sulla base di studi che ne dimostrino il valore aggiunto»[4].

Il riferimento alle «basi di dati centrali dell'UE già esistenti» va inteso, principalmente, al Sistema Informativo Schengen (SIS)[5], pervenuto alla seconda generazione (SIS II), e al Sistema Informativo Doganale (SID)[6]. Questi due strumenti catalizzano le informazioni provenienti dagli Stati membri convogliandole all'interno di una banca dati centrale che può essere compulsata, a richiesta, dalle autorità competenti dei singoli Stati. Il meccanismo operativo è caratterizzato da un sistema "a stella": il dato viene immesso da parte di un'autorità nazionale e, transitando per mezzo di una unità centrale di supporto tecnico, viene reso disponibile alle autorità degli altri Paesi. L'unità centrale non rielabora il dato, ma si limita a renderlo identico, e, dunque, disponibile per tutti gli utenti del sistema realizzando, per tale via, una forma di cooperazione "orizzontale" mediata.

Sotto un secondo e diverso profilo, la comparsa sulla scena europea di nuove istituzioni (quali OLAF, la Rete giudiziaria europea, i Magistrati di collegamento, e, soprattutto, Europol ed Eurojust), cui viene demandata una funzione di coordinamento nei rapporti tra le autorità di polizia e giudiziarie dei Paesi membri, ha favorito un processo di verticalizzazione della cooperazione[7], che attribuisce un ruolo di primo piano agli organismi di matrice europea. Questo rinnovato assetto istituzionale si riflette anche sul piano della cooperazione informativa mediante la creazione di strutture centralizzate di raccolta e scambio di dati che abbandonano la veste di meri collettori di informazioni per assumere il ruolo attivo di organismi di analisi e rielaborazione di dati e notizie di cui, oltre a disporne la trasmissione all'autorità richiedente, potranno autonomamente avvalersi nell'esercizio delle loro funzioni. Esemplificative, al riguardo, le basi di dati TECS di Europol[8] ed EPOC III di Eurojust[9]. Il cuore pulsante di entrambe le strutture è

---

4 Così, *Programma dell'Aia. Rafforzamento della libertà, della sicurezza e della giustizia nell'Unione Europea*, in *GUUE*, C 53, 3 marzo 2005, p. 7.

5 Cfr. *infra*, § 2.

6 V. *infra*, § 3.

7 Distingue tra una forma di cooperazione orizzontale e una verticale, con riferimento, per quest'ultima, all'istituzione di OLAF ed Eurojust, G. De Amicis, *op. cit.*, p. 289; M. Delmas-Marty, *Il* Corpus Juris *delle norme penali per la protezione degli interessi finanziari dell'Unione Europea*, in "Questione giustizia", 2000, p. 164.

8 Cfr. *infra*, § 4.

9 V. *infra*, § 6.

costituito da un'unità centrale di raccolta di dati alimentati dalle competenti autorità dei singoli Stati, in modo non dissimile da quanto avviene nei sistemi SIS e SID. Ma, a differenza di questi ultimi, le informazioni ivi contenute non transitano *sic et simpliciter* da uno Stato all'altro, ma vengono conservate nel database di tali enti, che si occupano di rielaborarla, modificarla e perfezionarla, secondo quanto ritenuto opportuno, prima di ritrasmetterle all'Autorità nazionale.

La creazione, a livello europeo, di una rete di archivi idonei a consentire la raccolta, l'elaborazione e la creazione di canali di scambio e di collegamento tra le informazioni richiede che una particolare attenzione venga tributata al tema della tutela dei dati ivi contenuti[10].

L'esigenza di predisporre una normativa uniforme di tutela dei dati personali, già avvertita in relazione alle strutture tradizionali di memorizzazione ai fini di scambio delle informazioni, si acutizza con la creazione delle banche dati di seconda generazione che consentono l'elaborazione di una piattaforma ampliata di dati e la creazione di canali di collegamento delle notizie raccolte.

Tali strumenti, agevolando l'incrocio dei flussi informativi, accentuano la necessità di predisporre una disciplina unitaria di protezione del dato sotto il duplice aspetto della sicurezza e della protezione dell'informazione, quali corollari del diritto soggettivo alla riservatezza del soggetto cui la notizia si riferisce[11]. Il primo aspetto (c.d. sicurezza del dato o *Datensicherung*) involge la tutela del dato da quei fattori esterni che possono pregiudicarne l'integrità e, dunque, l'attendibilità. Il secondo aspetto (cd. protezione del dato o *Datenschutz*) attiene al catalogo di situazioni soggettive riconosciute al soggetto interessato, il quale deve essere posto in grado di controllare l'*iter* di circolazione del dato, di richiederne, eventualmente, l'aggiornamento o la rettifica qualora esso si riveli non più adeguato o erroneo, e, infine, di ottenerne la cancellazione dal sistema.

---

10 In argomento, con particolare riguardo al delicato equilibrio che si instaura tra il diritto alla riservatezza e le esigenze di accertamento penale nel quadro della cooperazione di polizia e giudiziaria in Europa, si vedano: S. Allegrezza, "Giustizia penale e diritto all'autodeterminazione dei dati nella regione Europa", in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. Negri, Roma, Aracne, 2007, p. 59; M. Bonetti, *Riservatezza e processo penale*, Milano, Giuffrè, 2003, p. 64; D. Negri, "La circolazione del '*curriculum criminale*' tra i procedimenti penali", in *Contrasto al terrorismo interno e internazionale*, a cura di R.E. Kostoris e R. Orlandi, Torino, Giappichelli, 2006, p. 307.

11 La dicotomia protezione del dato (*Datenschutz*) – sicurezza del dato medesimo (*Datensicherung*) si deve ad alcuni esponenti della dottrina tedesca che, negli anni '70 del secolo scorso, per primi si sono preoccupati di individuare talune categorie giuridiche per meglio definire la problematica in esame: L. Bergmann-R. Möhrle, *Datenschutzrecht*, Stuttgart-München-Hannover, 1979, pp. 9 sgg.; S. Simitis, *Chanchen und Gefahren der elektronischen Datenverarbeitung*, in "Neue juristische Wochenschrift", 1971, pp. 673 sgg. Nella dottrina italiana, il diverso distinguo tra diritto negativo del singolo di escludere i terzi dalla propria sfera personale e diritto positivo di affermare il proprio controllo sui propri dati risale a S. Rodotà, *La* "privacy" *tra individuo e collettività*, in "Politica del diritto", 1974, p. 545. Sul punto, si veda S. Carnevale, "Autodeterminazione informativa e processo penale: le coordinate costituzionali", in *Protezione dei dati personali e accertamento penale*, cit., p. 7.

Le sopraccennate istanze hanno trovato sbocco, da ultimo, nell'approvazione da parte del Consiglio della decisione quadro 2008/977/GAI del 27 novembre 2008, recante una disciplina uniforme di tutela dei dati personali trattati nell'ambito del "terzo pilastro"[12].

Nel definire i rapporti con le fonti normative previgenti nel settore della cooperazione informativa, la decisione opera un distinguo tra gli atti che contengono una disciplina organica e completa in materia di protezione del dato, i quali non ricevono alcun pregiudizio dalla sua approvazione (considerando n. 39 della decisione quadro 2008/977/GAI), e gli strumenti giuridici che ne vengono intaccati, in quanto dedicano alla tutela dei dati un'attenzione solo parziale o residuale. Le basi giuridiche dei sistemi informativi SIS, SID e delle banche dati di Europol ed Eurojust rimangono impregiudicate dall'adozione della nuova disciplina, in quanto la medesima decisione ne ha decretato esplicitamente la sussunzione nella prima categoria di atti, caratterizzati dalla predisposizione di una cornice normativa esauriente in materia di tutela del dato[13].

Per altro verso, la decisione quadro succede alla Convenzione n. 108 del Consiglio d'Europa e alla Raccomandazione R (87) 15 nel ruolo di denominatore comune minimo di garanzia in materia di protezione delle informazioni nel settore della cooperazione penale. Pertanto, i richiami operati dalle basi giuridiche degli archivi in commento a tali fonti potrebbero intendersi riferiti alle nuove norme comuni in tema di tutela del dato ogni qualvolta queste pongano condizioni più restrittive all'accesso del dato rispetto alle corrispondenti norme convenzionali[14].

Rimane parimenti irrilevante, non applicandosi al settore della cooperazione di polizia e giudiziaria in materia penale, l'articolata disciplina contenuta nella direttiva 95/46/CE, la cui vigenza è limitata alle banche dati rientranti nel "primo pilastro"[15], quali il sistema di informazione visti (VIS), la banca dati dell'OLAF ed Eurodac[16].

---

12 Il testo della decisione è pubblicato in *GUUE*, L 350, 30 dicembre 2008, p. 60. Per un'analisi di tale strumento normativo, si veda, *amplius*, S. Ciampi, *op. cit.*, § 5.

13 V., ancora, il considerando n. 39 della decisione quadro 2008/977/GAI, il quale prevede che lo strumento normativo «dovrebbe lasciare impregiudicata la pertinente serie di disposizioni sulla protezione dei dati di detti atti e, segnatamente, quelle che disciplinano il funzionamento dell'Europol, di Eurojust, del sistema d'informazione Schengen (SIS) e del sistema informativo doganale (SID) e quelle che introducono l'accesso diretto delle autorità degli Stati membri a taluni sistemi di dati di altri Stati membri».

14 Così, opinando sulla base di quanto disposto dal considerando n. 40 della decisione quadro 2008/977/GAI.

15 La trattazione delle banche dati rientranti nel "primo pilastro" esula, in ragione della loro appartenenza al settore comunitario, dall'ambito della presente trattazione, che deve intendersi limitata agli archivi, aventi finalità di cooperazione giudiziaria e di polizia, operanti nel "terzo pilastro".

16 Per qualche cenno riguardo a Eurodac, cfr. *infra*, M. Gialuz, "Principio di accessibilità e banche dati di 'primo pilastro'".

Entro tale cornice deve essere inteso, pertanto, il richiamo a tale fonte comunitaria inserito nel Regolamento istitutivo del SIS II. Conseguentemente, la direttiva potrà trovare applicazione solo con riferimento alle materie del SIS II che si collocano nel settore comunitario.

2. Il sistema di informazione Schengen: dal SIS al Sistema informativo di seconda generazione (SIS II)

L'obiettivo, perseguito dagli Accordi di Schengen, della creazione di uno spazio comune europeo privo di frontiere interne in cui fosse assicurata la libera circolazione di persone, merci, servizi e capitali ha imposto l'introduzione di diverse e più stringenti regole di cooperazione giudiziaria e di polizia.

In un contesto normativo segnato dall'integrazione dell'*aquis* di Schengen nell'ordinamento dell'Unione, il rafforzamento della cooperazione tra le autorità di *intelligence* degli Stati membri risponde alla duplice esigenza di garantire una gestione comune dei controlli delle frontiere esterne a fronte della soppressione di quelle interne[17], da un lato, e di contrastare efficacemente le potenzialità offensive del crimine transnazionale[18], alimentate anche dal suddetto abbattimento delle frontiere nazionali, dall'altro lato.

Al fine di soddisfare tali esigenze, la Convenzione di Applicazione dell'accordo di Schengen[19] (d'ora innanzi CAAS) ha istituito un apposito sistema informatizzato per la gestione e lo scambio di dati tra i Paesi aderenti alla Convenzione (cd. SIS I): esso, infatti, era vòlto a consentire i necessari accertamenti, sia in sede di controlli alle frontiere, sia in occasione di interventi di polizia effettuati all'interno di ciascun Paese.

Se, in prima battuta, la base giuridica del sistema appariva fondata su una fonte di diritto internazionale *tout court* – per l'appunto, la Convenzione, ratificata dall'Italia con la l. 30 settembre 1993, n. 388 –, in seguito all'integrazione dell'*aquis* di Schengen in ambito UE le disposizioni relative al SIS sono divenute parte integrante del quadro giuridico dell'Unione, la cui base viene individuata nel "terzo pilastro"[20].

---

17 In questa prospettiva, C. Favilli, *Un'armonizzazione delle procedure «appesa» all'*iter *delle adesioni,* in "Guida al diritto. Diritto comunitario e internazionale", 2006, p. 39.

18 Per un approfondimento, si veda G. De Amicis, *op. cit.*, p. 283; A. Laudati, "Il coordinamento delle indagini nel crimine organizzato transnazionale. Il ruolo della Direzione nazionale antimafia alla luce dei coordinamenti in sede europea", in *Criminalità organizzata transnazionale e sistema penale italiano. La Convenzione O.N.U. di Palermo*, a cura di E. Rosi, Milano, Ipsoa, 2007, p. 377.

19 In *GUCE*, L 239, 22 settembre 2000, p. 19.

20 In mancanza di una diversa ripartizione degli elementi dell'*aquis* di Schengen tra il primo e il "terzo pilastro", che doveva essere stabilita dal Consiglio con la decisione 1999/435/CE, le disposizioni relative al SIS sono considerate atti fondati sul Titolo VI del Trattato UE, ai sensi dell'art. 2, par. 1, del Protocollo Schengen.

Nell'assetto disciplinato dalla Convenzione, il Sistema di informazione Schengen è formato da una banca dati nazionale (unità N-SIS) ubicata presso ciascuno Stato membro e da un servizio centrale (C-SIS) avente sede a Strasburgo e collegato a ciascuna unità nazionale. La sezione N-SIS accoglie, al suo interno, la base informativa e un ufficio operativo (SIRENE, acronimo di *Supplementary Information Request at the National Entry*), che svolge la funzione di fornire le informazioni non ricavabili dalla banca dati nazionale N-SIS.

L'architettura "a stella" consente alle autorità competenti dei singoli Stati di inoltrare le richieste di segnalazione alla base centrale, la quale, previo controllo formale della richiesta, modifica il proprio *database* e diffonde la segnalazione alle altre unità N-SIS, garantendo, per tale via, il costante aggiornamento dell'archivio centrale e l'uniformità di contenuto con gli archivi periferici.

La procedura di interrogazione automatica è fondata su un sistema *hit/no hit*, in virtù del quale, una volta accertata la presenza del dato nel sistema, ulteriori informazioni possono essere fornite dai competenti uffici nazionali SIRENE.

Il duplice profilo inerente all'individuazione delle categorie delle segnalazioni conservate negli archivi e delle autorità legittimate ad accedervi è stato oggetto di modifica ad opera del regolamento (CE) n. 871/2004[21] e della decisione 2005/211/GAI[22], volti al potenziamento della banca dati nella prospettiva del graduale superamento del sistema delineato dalla Convenzione Schengen mediante l'adozione di uno strumento di seconda generazione.

Sotto il primo profilo, la piattaforma di dati delimitata dagli artt. 95 sgg. della Convenzione comprende due categorie di informazioni, soggettive e oggettive.

Quanto alla prima categoria, rimane inalterato l'assetto delineato dagli artt. 95, 97 e 98 CAAS, che comprende i dati personali[23], ad esclusione di quelli sensibili[24], inerenti alle persone ricercate per l'arresto ai fini di estradizione, agli stranieri segnalati ai fini della non ammissione, alle persone scomparse, da tutelare o da porre sotto protezione e, *last but non least*, ai testimoni nell'ambito di un procedimento penale e ai destinatari di citazioni a comparire dinnanzi all'autorità

---

21 In *GUUE*, L 162, 30 aprile 2004, p. 29.

22 In *GUUE*, L 68, 15 marzo 2005, p. 44. La decisione 2005/211/GAI introduce nuove funzioni nel sistema di informazione Schengen nel quadro della lotta contro il terrorismo. Sul punto, si veda il commento di S. Dambruoso, *Più facile la verifica dei documenti e il controllo degli ingressi irregolari*, in "Guida al diritto. Diritto comunitario e internazionale", 2005, n. 3, p. 49.

23 I dati personali che, a mente dell'art. 94 CAAS, potevano essere inclusi nel SIS erano esclusivamente quelli concernenti: cognome, nome, prima lettera del secondo nome, soprannome, segni fisici particolari, luogo e data di nascita, sesso, cittadinanza, uso di violenza o di armi. A seguito delle modifiche apportate dal regolamento n. 871 del 2004 e dalla decisione n. 211 del 2005, sono inclusi nel *database* anche l'eventuale *status* di evaso e, per gli estradandi, il tipo di reato commesso.

24 La categoria dei dati sensibili è oggetto di un espresso divieto di conservazione ai sensi dell'art. 94, par. 3, CAAS.

giudiziaria, di notifiche di sentenze e di ordini di esecuzione di pene privative della libertà personale.

Quanto alla seconda categoria, inerente agli oggetti ricercati a scopo di sequestro o di prova in un procedimento penale, quali veicoli e armi da fuoco, l'art. 100 CAAS, modificato dalla decisione 2005/211/GAI, contempla, ulteriormente, l'immissione nel sistema di ulteriori dati, quali quelli relativi ai permessi di soggiorno e ai documenti di viaggio, al fine di agevolare il controllo alle frontiere. In aggiunta alle finalità sopra riportate, i dati soggettivi e oggettivi possono essere inseriti nel sistema allo scopo di consentire una sorveglianza discreta o un controllo specifico[25].

La novità più significativa introdotta dal regolamento e dalla decisione attiene al secondo profilo e riguarda specificamente le autorità legittimate ad accedere all'archivio[26]. Il diritto di consultare la banca dati, in origine circoscritto alle autorità competenti in materia di controlli alle frontiere e di rilascio visti, viene esteso anche alle autorità giudiziarie nazionali, a Europol, ai membri nazionali di Eurojust e ai loro assistenti. Tuttavia, con riferimento agli organismi sovranazionali, l'accesso è limitato, per Europol[27], ai dati inerenti ai soggetti ricercati per l'arresto ai fini di estradizione, alle segnalazioni effettuate ai fini di una sorveglianza discreta o di un controllo specifico e agli oggetti ricercati a scopo di sequestro in un processo penale, e, per Eurojust[28], alle segnalazioni concernenti gli estradandi, i testimoni e i destinatari di citazioni e di notifiche nell'ambito di un procedimento penale. L'interoperabilità dei sistemi comporta, quale conseguenza indiretta, che i dati contenuti nel SIS possano trasmigrare a Stati e organismi terzi per il tramite di Europol ed Eurojust, cui è espressamente consentito di trasmettere le informazioni ottenute dal SIS, a condizione che sussista l'autorizzazione dello Stato membro interessato.

L'ampliamento della piattaforma di dati e del novero dei soggetti autorizzati ad accedervi segna una tappa del percorso vòlto ad accrescere le potenzialità del SIS, trasformandolo da strumento di controllo della circolazione nello spazio Schengen in banca dati compulsabile, oltre che a fini preventivi, anche a fini di informazione e di indagine. Tale mutazione genetica ha sollevato, per altro verso, alcuni dubbi riguardo alla tenuta dell'originario regime giuridico di protezione

---

25 Si tratta di due forme di segnalazioni previste ai fini di prevenzione di reati che pongano in pericolo la pubblica sicurezza. Per un approfondimento, si veda G. Calesini, *Diritto europeo di polizia*, Roma, Laurus Robuffo, 2007, p. 50.

26 A tali fonti deve aggiungersi il regolamento (CE) n. 1160/2005, regolante l'accesso al SIS da parte delle autorità degli Stati membri competenti per il rilascio dei documenti di immatricolazione dei veicoli (il testo è pubblicato in *GUUE*, L 191, 22 luglio 2005, p. 18).

27 A mente dell'art. 101-*bis*, inserito dalla decisione in commento, Europol ha il diritto di accedere ai dati inseriti nel sistema a norma degli artt. 95, 99 e 100 della Convenzione Schengen.

28 Il nuovo art. 101-*ter* rinvia, per delimitare il diritto di accesso di Eurojust alla banca dati, agli artt. 95 e 98 della Convenzione.

dei dati a fronte di una serie di strumenti modificativi che, pure incidendo in maniera sostanziale sulla funzionalità del sistema, non hanno implementato in alcun modo i meccanismi di salvaguardia della circolazione del dato[29]. Permane pressoché immutato, pertanto, il quadro giuridico predisposto dalla Convenzione, che articola la tutela del dato su due fronti.

Dal lato oggettivo, la CAAS ha elevato al rango di parametri valutativi del grado di tutela raggiunto dalla disciplina nazionale dei Paesi membri, subordinando all'esito di tale valutazione l'accesso al sistema, la Convenzione n. 108 del Consiglio d'Europa e la raccomandazione del Comitato dei Ministri R (87) 15. A tale *corpus* normativo mostra, peraltro, di richiamarsi la medesima Convenzione in sede di definizione dei principi minimi in tema di tutela oggettiva delle informazioni, la quale è assicurata dal rispetto dei parametri di legalità e di finalità limitata, mentre, per contro, non è stato recepito, in questa sede, quanto stabilito dalla Convenzione n. 108 del 1981 in materia di proporzionalità dei dati.

In particolare, il principio di legalità è attuato mediante il conferimento del ruolo di garante della correttezza del dato allo Stato che ha effettuato la segnalazione, il quale è l'unico autorizzato ad apportare modifiche o cancellazioni alle informazioni che ha introdotto. Il principio di finalità è assicurato dalla limitazione alla permanenza del dato in archivio per il tempo necessario al raggiungimento degli scopi che giustificano il suo inserimento, che non deve, comunque, superare i limiti massimi previsti dalla Convenzione. La portata di tale principio, tuttavia, è ridimensionata dalle ampie possibilità di deroga in caso di minacce gravi all'ordine e alla sicurezza pubblica e nei casi in cui sorga la necessità di prevenire un grave fatto di reato.

Dal lato soggettivo, la Convenzione riconosce al titolare del dato in circolazione un catalogo di diritti di accesso, rettifica e cancellazione delle notizie che si attivano a seguito di richiesta scritta dell'interessato, prevedendo, altresì, la facoltà della persona di scegliere in quale Paese membro indirizzare la richiesta. Anche su tale fronte, tuttavia, occorre segnalare che, in ipotesi circoscritte, il soggetto può vedersi negato il diritto di accesso al dato.

In ultimo, la Convenzione prevede un meccanismo di controllo sul rispetto delle garanzie minime operante a livello centrale e a livello nazionale. Tale compito viene demandato, per quanto attiene all'unità C-SIS, ad un'Autorità di con-

---

29 Si veda, in argomento, il *Parere del garante europeo della protezione dei dati (GEPT) sulla proposta di decisione del consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II) (COM (2005) 230); sulla proposta di regolamento del Parlamento europeo e del Consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II) (COM (2005) 236) e sulla proposta di regolamento del Parlamento europeo e del Consiglio sull'accesso al sistema di informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (COM(2005)237)*, in *GUUE*, C 91, 19 aprile 2006, p. 38.

trollo comune all'uopo istituita[30], e, con riferimento alle sezioni nazionali, ad un organo designato dalla Parte contraente.

L'*iter* di sviluppo del sistema di informazione Schengen è stato supportato, sul piano tecnico, dal progetto SIS 1+, che, consentendo il collegamento di nove dei nuovi Stati membri UE all'archivio, si pone quale *trait d'union* con l'istituzione del sistema di informazione di seconda generazione SIS II.

In aggiunta all'anzidetta esigenza di conferire nuove funzioni al sistema, il superamento dell'impianto originario si è reso necessario anche per consentire ai nuovi Stati membri dell'Unione europea di aderire allo spazio Schengen, atteso che la vecchia piattaforma poteva supportare al massimo diciotto unità nazionali. L'incarico di sviluppare il SIS II, affidato alla Commissione con regolamento (CE) n. 2424/2001[31] e con decisione 2001/886/GAI[32], è stato portato a termine nel 2007 con l'adozione di una doppia base giuridica, formata dal regolamento (CE) n. 1987/2006[33] e dalla decisione 2007/533/GAI[34], e diverrà operativo, esperite le prove tecniche[35], all'esito del processo di migrazione dal sistema SIS 1+, attualmente in uso[36].

Preliminarmente, occorre dare conto della duplice fonte normativa del SIS II. Il sistema appare disciplinato sia da uno strumento legislativo appartenente al "primo pilastro" (TCE), sia da un atto del "terzo pilastro" (Titolo VI TUE). Ciò è dovuto al fatto che l'archivio è stato istituito per una duplice finalità, costituita rispettivamente dal controllo dell'immigrazione e dal mantenimento dell'ordine pubblico e della sicurezza. La trasposizione della prima materia, ad opera del trattato di Amsterdam, nel "primo pilastro" ha reso necessaria, da un lato, l'adozione

---

30 A tal proposito, la mancata coincidenza tra l'autorità di controllo comune Schengen e il Garante europeo per la protezione dei dati è stata oggetto di critiche da parte di alcuni Autori. Il problema viene superato, come si vedrà *infra*, a seguito dell'adozione della decisione 2007/533/GAI. Si veda, sul punto, S. Peers, *The SIS II proposals. Statewatch Analysis*, <http://www.statewatch.org/news/2005/jun/05sisII.htm>.

31 In *GUUE*, L 328, 13 dicembre 2001, p. 4.

32 In *GUUE*, L 328, 13 dicembre 2001, p. 1. La fonte in parola è stata successivamente modificata dalla decisione 2006/1007/GAI, in *GUUE*, L 411, 30 dicembre 2006, p. 78.

33 In *GUUE*, L 381, 28 dicembre 2006, p. 4.

34 In *GUUE*, L 205, 7 agosto 2007, p. 63.

35 Le prove tecniche di sistema per consentire il passaggio al SIS II sono disciplinate dal regolamento (CE) n. 189/2008, pubblicato in *GUUE*, L 57, 1° marzo 2008, p. 1.

36 Il progetto SIS II consta di tre fasi. Alle prime due fasi, vertenti sulla elaborazione e sulle prove tecniche di sistema, segue la terza fase, allo stato non ancora conclusa, sulla migrazione dal SIS 1+ e sulle prove finali. La Commissione ha predisposto, al fine di delineare il quadro giuridico regolante il passaggio al nuovo sistema, due strumenti giuridici consistenti nella proposta di decisione COM (2008)0916 e nella proposta di regolamento 13488/2008. Sul punto, si veda la *Relazione della Commissione al Consiglio e al Parlamento europeo sullo sviluppo del sistema di informazione Schengen di seconda generazione*, 10 novembre 2008, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0710:FIN:IT:DOC>.

di regolamenti CE per quanto attiene al controllo delle frontiere, ferma restando, dall'altro lato, la scelta di disciplinare mediante decisioni GAI l'utilizzo del sistema ai fini di cooperazione di polizia e giudiziaria in materia penale. Affinché la natura mista del SIS non rechi pregiudizio all'unitarietà del sistema, entrambe le fonti manifestano l'opportunità che le norme contenute nelle decisioni GAI e nei regolamenti CE siano redatte in maniera del tutto identica[37], palesando così la finzione giuridica denominata «tecnica del doppio binario».

La decisione 2007/533/GAI, il cui contenuto, sul punto, è replicato quasi integralmente dall'omologa fonte comunitaria, ribadisce per il SIS II un'architettura che vede al centro un archivio di dati (SIS II centrale) e alla periferia, collegati al primo, gli omologhi archivi nazionali (N.SIS II). Il SIS II centrale si compone di un'unità di supporto tecnico, contenente la banca dati del SIS II (CS-SIS) e di un'interfaccia nazionale uniforme (NI-SIS), che comprende al suo interno il servizio tecnico-operativo SIRENE, la cui disciplina, contenuta nella decisione 2006/758/CE (c.d. manuale SIRENE)[38], è richiamata dalla decisione e dal regolamento sul SIS II rispettivamente agli artt. 7 e 8. Attraverso detto servizio, mediante la compilazione di una apposita scheda a campi obbligatori (sistema *hit-no hit*), che garantisce la standardizzazione dei dati da introdurre nel sistema informatico, vengono scambiate tutte le informazioni supplementari necessarie[39].

La struttura a stella garantisce che tutti i dati rilevanti del SIS II centrale vengano inseriti, aggiornati, cancellati e consultati tramite i vari N.SIS II, i quali, per l'uso interno al territorio del loro Stato, dispongono di una copia delle informazioni raccolte nel SIS II centrale[40]. Per contro, il singolo N.SIS II non può essere consultato da parte delle Autorità di uno Stato membro diverso (art. 4, par. 2, decisione 2007/533/GAI).

L'operatività del SIS II è affidata, nella fase transitoria, alla Commissione, e, in seguito, a un apposito organo di gestione, mentre la gestione dei singoli N.SIS II spetta agli Stati di appartenenza (art. 15 decisione 2007/533/GAI).

Quanto alla piattaforma di informazioni memorizzate nella banca dati, l'art. 20 della decisione ripropone la distinzione in due grandi categorie.

---

37 Cfr. il considerando n. 4 del regolamento (CE) n. 1987/2006 e della decisione 2007/533/GAI.

38 In *GUUE*, L 317, 16 novembre 2006, p. 41. Si può notare come non esista una fonte "parallela" di "terzo pilastro". Infatti, al considerando n. 7 della decisione si legge che «il fatto che la base giuridica necessaria per adottare la versione riveduta del manuale consti di due strumenti distinti non pregiudica il principio di unità del manuale». Da ultimo, si veda la decisione della Commissione 2008/333/CE, che adotta il manuale Sirene e altre disposizioni di attuazione per il sistema di informazione Schengen di seconda generazione (SIS II), in *GUUE*, L 123, 8 maggio 2008, p. 1.

39 Cfr. D. Grohmann, "La cooperazione giudiziaria in materia penale", in *Cittadinanza europea, accesso al lavoro e cooperazione giudiziaria*, Trieste, Edizioni Università di Trieste, 2005, p. 94.

40 Così, A. Perduca, *Una raccolta di dati su persone e oggetti con grande attenzione ai diritti individuali*, in "Guida al diritto. Diritto Comunitario e Internazionale", 2007, n. 5, p. 64.

Sotto il profilo oggettivo, la banca dati comprende un elenco di informazioni relative ad oggetti ricercati a scopo di sequestro, confisca, e a fini probatori[41].

Sotto il profilo soggettivo, l'archivio contiene i dati relativi alle persone segnalate: contiene, cioè, le informazioni che permettono alle autorità competenti «di identificare un individuo in vista di intraprendere un'azione specifica» (art. 3, lett. *a*), regolamento (CE) n. 1987/2006 e art. 3, lett. *a*), decisione 2007/533/GAI). Le tipologie di segnalazioni rimangono invariate, rispetto a quelle originariamente disciplinate dagli artt. 95-100 della Convenzione, anche se, rispetto all'originaria disciplina, si nota un miglioramento in termini di chiarezza delle denominazioni dei capi e un maggiore dettaglio nelle singole disposizioni. Vengono analiticamente disciplinate le seguenti segnalazioni: di persone ricercate per l'arresto a fini di consegna o di estradizione (artt. 26-31); di persone scomparse (artt. 32-33); di persone ricercate per presenziare ad un procedimento giudiziario (artt. 34-35); di persone e oggetti ai fini di un controllo discreto o di un controllo specifico (artt. 36-37); di oggetti ai fini di sequestro o di prova in un procedimento penale (artt. 38-39)[42]. In accordo agli scopi conseguiti, la decisione si differenzia dalla corrispondente disposizione comunitaria che prevede solo le segnalazioni di cittadini di Paesi terzi ai fini del rifiuto di ingresso e di soggiorno (Capo IV, regolamento (CE) n. 1987/2006).

Le informazioni relative alle persone, a mente di entrambi gli strumenti normativi, sono limitate ai dati anagrafici, comprensivi di segni fisici particolari, fotografie, impronte digitali, cittadinanza, nonché all'indicazione del grado di pericolosità, determinato da indici quali la presenza di armi, condotte violente, evasione, e delle ragioni della segnalazione, corredate dall'indicazione dell'autorità procedente, della decisione che ha dato origine alla segnalazione, dell'azione da intraprendere e di eventuali connessioni con altre segnalazioni (art. 20, par. 3, decisione 2007/533/GAI e 20, par. 2, regolamento (CE) n. 1987/2006). La sola decisione indica, in aggiunta, il tipo di reato in relazione al quale si procede.

L'analisi comparativa con la precedente disciplina di fonte convenzionale consente di rimarcare due novità di grande rilievo.

La prima attiene al raccordo normativo tra la banca dati e la normativa sul mandato d'arresto europeo, per effetto del quale le segnalazioni riguardanti per-

---

41 Gli artt. 36 e 38 decisione 2007/533/GAI si riferiscono a: veicoli, natanti, aeromobili, container, rimorchi, armi da fuoco, documenti di varia natura rubati o altrimenti sottratti ovvero smarriti, banconote registrate, valori mobiliari e mezzi di pagamento.

42 All'elenco riportato nel testo deve essere aggiunto l'art. 102-*bis* CAAS, che resterà in vigore anche a seguito della piena operatività del SIS II (cfr. art. 68, par. 1, decisione 2007/533/GAI) e a mente del quale possono avere accesso ai dati concernenti gli autoveicoli, in deroga alla previsione che vieta l'uso delle segnalazioni ai fini amministrativi (art. 102, par. 4, decisione 2007/533/GAI), gli enti deputati al rilascio dei documenti per l'immatricolazione degli autoveicoli medesimi, onde evitare di immatricolare veicoli che, ad una successiva verifica, risultino essere stati rubati.

sone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto e inserite nel SIS II producono, a norma dell'art. 26 della decisione 2007/533/GAI, lo stesso effetto del mandato d'arresto europeo emesso a norma della decisione quadro 2002/584/GAI, limitatamente ai Paesi in cui tale disciplina è operante[43]. Per gli Stati che non hanno provveduto alla ratifica della normativa sul mandato d'arresto europeo, la segnalazione nel SIS II equivale, invece, a una richiesta di arresto provvisorio, così come previsto dalle fonti internazionali in materia di assistenza giudiziaria.

La seconda novità attiene alla menzione dei dati biometrici – in particolare, impronte digitali e fotografie – nella tipologia di informazioni suscettibili di trattamento.

Se, da un lato, l'inserimento di criteri di identificazione univoci, quali i dati biometrici, nel novero delle informazioni incluse nell'archivio può consentire la risoluzione dei problemi legati all'identità dei singoli soggetti[44], dall'altro lato, l'inclusione di tale categoria di dati aumenta il rischio di conversione del SIS II in strumento di supporto di indagini a carattere transnazionale. Ciò è particolarmente evidente ove ci si ponga nella prospettiva, sollecitata dalla Commissione europea[45], dell'interoperabilità del SIS II con i sistemi di "primo pilastro" VIS ed Eurodac, contemplanti anch'essi tale categoria di dati, nell'obiettivo della creazione di una piattaforma tecnica comune[46].

---

43 In *GUUE*, L 190, 18 luglio 2002, p. 1. In Italia, la decisione quadro è stata attuata con l. 22 aprile 2005, n. 69, i cui artt. 6, 7, 8 e 11 contengono la disciplina dell'equivalenza tra segnalazione nel SIS e MAE. Per le prime applicazioni giurisprudenziali del principio, si veda Corte d'Appello di Bologna, ord. 21 giugno 2005, in "Foro italiano", 2005, II, cc. 522 sgg., con nota di G. Iuzzolino; Cass., sez. VI, 22 novembre 2005, Calabrese, *ivi*, 2006, II, cc. 274 sgg.; Cass., sez. VI, 12 dicembre 2006, A.G., in "Diritto penale e processo", 2007, p. 449; Cass., sez. un., 30 gennaio 2007, R.V., in *CED Cass.*, n. 235348. In dottrina, si veda F. Lo Voi, "Il procedimento davanti alla corte di appello e i provvedimenti *de libertate*. Il consenso", in *Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna*, a cura di M. Bargis ed E. Selvaggi, Torino, Giappichelli, 2005, pp. 241 sgg.; M. Romano, "L'arresto di polizia e la convalida", in *Il mandato d'arresto europeo*, a cura di G. Pansini e A. Scalfati, Napoli, 2005, pp. 65 sgg.; P. Troisi, "L'arresto operato dalla polizia giudiziaria a seguito della segnalazione nel sistema di informazione Schengen", in *Mandato di arresto europeo e procedure di consegna*, a cura di L. Kalb, Milano, Giuffrè, 2005, pp. 223 sgg.

44 Sul punto, la Comunicazione della Commissione del dicembre 2003 indica, a titolo esemplificativo, le ipotesi in cui le autorità arrestino una persona in possesso di documenti falsi e i cd. "falsi positivi" del sistema, che si verificano nelle ipotesi di omonimia. Si veda, a tal riguardo, la *Comunicazione della Commissione al Consiglio e al Parlamento europeo - Sviluppo del sistema di informazione Schengen II e possibili sinergie con un futuro sistema di informazione visti (VIS) (COM (2003) 771, dell'11 dicembre 2003)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0771:IT:HTML>.

45 Così, la *Comunicazione della Commissione al Consiglio e al Parlamento europeo concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni (COM (2005) 597, del 24 novembre 2005)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:IT:HTML>.

46 Al riguardo, cfr. *infra*, M. Gialuz, *op. cit.*, § 1.

Tali considerazioni, unitamente al carattere sensibile dei dati biometrici, impongono la predisposizione di specifiche garanzie in accordo alla particolare cautela che deve informarne il trattamento[47]. In tal senso, l'art. 22 della decisione detta norme specifiche sulla correttezza e utilizzabilità dei dati biometrici. Anzitutto, questi possono essere inseriti nel sistema «solo previo controllo speciale di qualità dell'informazione» (lett. *a*). Ma ciò che più conta è che «fotografie e impronte digitali sono usate solo per confermare l'identità di una persona individuata grazie all'interrogazione del SIS II con dati alfanumerici» (lett. *b*): il che significa, in sostanza, che, allo stato, il SIS II non consente di compiere interrogazioni generalizzate sulla base dei parametri biometrici. Peraltro, la lett. c precisa che le impronte digitali, non appena diventi possibile tecnicamente, potranno essere utilizzate «anche per identificare una persona in base al suo identificatore biometrico». Prima che questa funzione sia attuata nel SIS II, però, si prevede che «la Commissione present[i] una relazione sulla disponibilità e sullo stato di preparazione della tecnologia necessaria, in merito alla quale il Parlamento europeo è consultato».

Il SIS II, in linea di continuità con il suo immediato precedente, contempla, in aggiunta, le segnalazioni di persone o cose ai fini del controllo discreto e del controllo specifico (art. 36 decisione 2007/533/GAI).

La locuzione "controllo discreto" sostituisce la "sorveglianza discreta" del SIS I, trattandosi, peraltro, di una modifica puramente nominalistica, in quanto il contenuto permane immutato. Questa segnalazione, analogamente a quella finalizzata al controllo specifico, può avvenire sulla scorta di un corredo di presupposti che consistono nella sussistenza di indizi concreti che le persone intendano commettere o commettano taluno dei reati indicati dall'art. 2, par. 2, decisione quadro 2002/584/GAI, o in una prognosi di pericolosità futura fondata su reati già commessi, o, ancora, nella necessità di prevenire una minaccia grave proveniente dalle persone interessate o altre minacce gravi per la sicurezza interna ed esterna dello Stato[48]

L'analisi dei presupposti e il richiamo alle «minacce gravi per la sicurezza interna ed esterna dello Stato» induce a ritenere che la norma sia ispirata a una *ratio* di prevenzione dei reati di terrorismo internazionale, che, per altro aspetto, ha indotto i legislatori interni ad introdurre nei rispettivi ordinamenti forme di tutela penale, per certa misura anticipatorie rispetto all'instaurazione del procedimento[49].

---

47 La predisposizione di un quadro di garanzie adeguato è stata sollecitata anche dal *Parere del garante europeo della protezione dei dati (GEPT) sulla proposta di decisione del consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II)*, in *GUUE*, C 91, 19 aprile 2006, p. 38.

48 V. anche A. Perduca, *Una raccolta di dati*, cit., p. 65.

49 Da ultimo, v. E. Rosi, *Terrorismo internazionale: anticipazione della tutela penale e garanzie giurisdizionali*, in "Diritto penale e processo", 2008, pp. 455 sgg.

Sul piano operativo, la funzionalità del SIS II è rafforzata dalla previsione dell'art. 37 del regolamento e dell'art. 52 della decisione, in base ai quali le anzidette categorie di segnalazioni possono essere oggetto di connessione. In particolare, tali norme consentono agli Stati membri di creare legami tra i dati contenuti in archivio, specificando, ulteriormente, che le connessioni non possono essere strumentalizzate al fine di eludere i limiti di accesso al sistema. A tal fine, l'art. 52, par. 3, vieta espressamente alle autorità, che non siano legittimate ad accedere a talune categorie di segnalazioni, di visualizzare la relativa connessione. Tale previsione si pone a garanzia dei diritti dell'individuo in un meccanismo dalle potenzialità fortemente invasive della sua sfera privata. In un sistema in cui quanto più è consentita la diffusione di un dato, tanto più viene sacrificata la sfera del diritto alla riservatezza, l'impossibilità tecnica e giuridica, per talune autorità, di visualizzare la connessione a una segnalazione a cui non hanno accesso consente una corretta attuazione del principio di finalità limitata.

Il profilo operativo del sistema appare rafforzato, ulteriormente, dall'estensione del diritto di accesso alle segnalazioni contenute nel SIS II. La relativa legittimazione spetta, in via principale, alle autorità di polizia, doganali e all'autorità giudiziaria. È ribadito, altresì, il riconoscimento, introdotto dalla decisione 2005/211/GAI, del diritto di consultazione del database anche in capo ad organismi sopranazionali quali Europol ed Eurojust (artt. 41 e 42 decisione 2007/533/GAI). Una delle novità più significative introdotta dalle fonti in esame è costituita dall'inserimento nell'elenco dei soggetti autorizzati ad accedere ai dati delle autorità competenti in materia di asilo e immigrazione. Il che, si badi, ha suscitato notevoli perplessità: in particolare, si è posto l'accento sull'insufficienza di una segnalazione SIS a costituire motivo di rifiuto di una domanda d'asilo o del riconoscimento dello status di rifugiato da parte delle competenti autorità[50].

Il potenziamento del sistema di circolazione dei dati e l'allargamento della piattaforma di informazioni memorizzate nel SIS II ha reso necessaria la predisposizione di un adeguato sistema di protezione del dato sotto il duplice profilo della sicurezza della notizia memorizzata e delle tutele soggettive riconosciute all'interessato in attuazione del suo diritto all'autodeterminazione informativa. Le fonti regolatrici del sistema Schengen di seconda generazione eleggono a parametri di conformità della disciplina di tutela del dato in esse contenuta un *corpus* normativo necessariamente eterogeneo, in ragione della doppia base giuridica cui devono ricondursi.

Così, da un lato, il regolamento (CE) n. 1987/2006 rinvia a fonti di matrice comunitaria, quali la direttiva 95/46/CE e il regolamento (CE) n. 45/2001, mentre, dall'altro lato, la decisione 2007/533/GAI ribadisce il richiamo, già contenuto nel-

50 S. Peers, *The SIS II proposals. Statewatch Analysis*, cit. Sul punto, si veda anche il *Parere del garante europeo della protezione dei dati (GEPT) sulla proposta di decisione del consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II)*, cit., p. 47.

la CAAS, alla Convenzione n. 108 del 1981 e alla Raccomandazione R (87) 15. Di tali rinvii si dovrà tenere conto, pertanto, ai fini della valutazione di conformità e di adeguatezza delle norme di tutela dei dati trattati in base alle fonti anzidette[51].

Sotto il profilo della sicurezza del dato, il riconoscimento della doppia base giuridica del SIS II consente di superare la questione afferente alla mancata coincidenza tra l'Autorità di controllo comune, individuata dalla Convenzione Schengen quale organo responsabile della tutela dei dati compresi nell'archivio centrale, e il Garante europeo della protezione dei dati, istituito con il richiamato regolamento (CE) n. 45/2001.

In tale prospettiva, il controllo, a livello centrale, sulle attività di trattamento dei dati personali viene affidato al Garante europeo, e ciò con riferimento, sia ai dati trattati per le finalità di cui al regolamento (CE) n. 1987/2006, sia alle informazioni conservate per gli scopi di cui alla decisione 2007/533/GAI. Per contro, la vigilanza sulle unità periferiche rimane prerogativa dei singoli Stati membri, i quali agiscono per il tramite di un'autorità nazionale di controllo a tal fine designata.

I Paesi membri sono, altresì, responsabili per l'adozione di misure preventive volte a tutelare la sicurezza dei dati immessi nei rispettivi N.SIS II[52]. Il profilo della sicurezza, garantendo il controllo della legalità e dell'esattezza oggettiva della notizia che potrebbe essere minata dall'intervento di fattori esterni all'archivio, costituisce un aspetto rilevante, ma non esaustivo, della disciplina di profilassi del dato.

Alle norme in materia di *Datensicherung*, infatti, si affiancano le disposizioni in materia di protezione dei dati inseriti in archivio (cd. *Datenschutz*)[53], tra le quali occupa un posto di primo piano il versante della tutela soggettiva dei dati. Entrambe le fonti normative del SIS II – decisione e regolamento – dedicano un intero capo, rispettivamente il capo XII della decisione e il capo VI del regolamento alla materia della protezione dei dati.

In apertura, l'art. 56 della decisione e l'art. 40 del regolamento proclamano congiuntamente il divieto di trattamento di dati sensibili, ancorando tale divieto a due fonti distinte, in virtù della loro diversa base giuridica. In particolare, l'art. 40 del regolamento cita la direttiva 95/46/CE, mentre l'art. 56 della decisione rinvia all'art. 6 della Convenzione del Consiglio d'Europa n. 108 del 1981, che vie-

---

51 Così, il *Parere del garante europeo della protezione dei dati (GEPT) sulla proposta di decisione del consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II)*, cit., p. 40. Il Garante europeo considera, in aggiunta, l'impatto provocato dall'approvazione della proposta di decisione quadro sulla protezione dei dati personali nell'ambito del "terzo pilastro" sul regime di protezione dei dati del SIS II, *ivi*, p. 42.

52 L'art. 10 della decisione e del regolamento delega ogni singolo Stato membro, per il rispettivo N.SIS II, *inter cetera*, a proteggere fisicamente i dati, mediante la predisposizione di adeguate strutture tecniche, impedire alle persone non autorizzate l'accesso ai dati, impedire la copia di questi ultimi, controllare gli utenti del sistema per impedire il trasferimento indebito dei dati. Analoghe previsioni sono formulate dall'art. 16 per il SIS II centrale a carico dell'Autorità competente.

53 Si veda, *amplius*, *supra*, § 1.

ne più ampiamente richiamata dal successivo art. 57, quale parametro di conformità degli scambi informativi rientranti nel "terzo pilastro".

Il divieto di trattamento di dati sensibili, nonché l'integrale richiamo della Convenzione citata sembrano risolversi in mere petizioni di principio. Ciò è vero, da un lato, per quanto attiene al richiamo contenuto nell'art. 56, posto che, nel SIS II, possono trovare albergo le informazioni circa i «segni fisici particolari», l'«indicazione che le persone in questione sono violente», la «ragione della segnalazione» (art. 20, par. 2, lett. *b*), *h*), *i*), decisione 2007/533/GAI), che «non poco giocano ambiguamente [quanto] alla sensibilità del loro contenuto»[54]. Dall'altro lato, i principi fondanti la Convenzione del 1981 in materia di tutela dei dati, la cui integrale applicabilità al SIS II è ribadita dall'art. 57 della decisione, subiscono alcune deroghe di non poco rilievo. Sul punto, il principio di finalità del trattamento, per cui il dato non può essere trattato al di fuori degli scopi tassativamente previsti, può essere superato in forza dell'autorizzazione dello Stato che ha effettuato la segnalazione, nell'ipotesi – alquanto generica – in cui sussista la «necessità di prevenire una minaccia grave e imminente per l'ordine pubblico e la sicurezza pubblica» (art. 46, par. 5, della decisione 2007/533/GAI). Tale previsione, già presente nella Convenzione, è stata sottoposta a severa critica per la sua attitudine ad incidere sul diritto alla riservatezza del privato, vanificando il diritto all'autodeterminazione informativa[55].

Sul versante della tutela soggettiva, le fonti riconoscono un catalogo di diritti in capo al soggetto interessato dal contenuto dell'informazione.

In primo luogo, è attribuito ai singoli uno specifico diritto di accesso, rettifica e cancellazione dei dati. In particolare, al soggetto cui l'informazione si riferisce è garantito l'accesso ai propri dati conformemente alla legislazione dello Stato in cui egli fa valere tale diritto (art. 58, par. 2, decisione 2007/533/GAI; art. 41, par. 1, regolamento (CE) n. 1987/2006). Nel nostro Paese, in attesa di una legge di attuazione della decisione in commento, continuano ad applicarsi gli artt. 9 e 11 della l. 30 settembre 1993, n. 388, come modificati dall'art. 173 d.lgs. 30 giugno 2003, n. 196[56]. Tali fonti dispongono che l'Autorità a cui devono essere formulate le richieste per l'esercizio di diritti inerenti alle segnalazioni nel SIS II è il Garante per la protezione dei dati personali (art. 154, comma 2, lett. *a*), d. lgs. 196 del 2003).

In parziale applicazione dell'art. 109, par. 2, CAAS, l'art. 58, par. 2, della decisione prevede che il diritto all'accesso possa essere negato, ma non più laddove ciò possa «nuocere alla esecuzione dell'attività legale indicata nella segnalazione»,

---

54 Così M. Bonetti, *op. cit.*, p. 72.

55 Così, L.S. Rossi, "La protezione dei dati personali negli accordi di Schengen alla luce degli standards fissati dal Consiglio d'Europa e dalla Comunità europea", in *Da Schengen a Maastricht*, a cura di B. Nascimbene, Milano, Giuffrè, 1995, pp. 183 sgg.

56 Per una compiuta disamina dell'applicazione che la Convenzione Schengen ha avuto in ciascuno dei Paesi aderenti, v. D. Riccio, *Il Sistema*, cit., pp. 107 sgg.

bensì soltanto «se ciò è indispensabile per l'esecuzione di un compito legittimo connesso con una segnalazione o ai fini della tutela dei diritti e delle libertà di terzi». Il paragrafo successivo stabilisce, inoltre, che «chiunque ha il diritto di far rettificare dati che lo riguardano contenenti errori di fatto o di far cancellare dati che lo riguardano inseriti illecitamente».

In *pendant* con il principio di finalità limitata del trattamento, è garantito il diritto all'oblio[57] mediante la previsione della cancellazione automatica delle segnalazioni soggettive in seguito alla realizzazione dello scopo cui erano destinate, e comunque, dopo tre anni – uno, nel caso di persone soggette a controllo discreto o specifico – dal loro inserimento, a meno che lo Stato che le ha inserite non presenti richiesta motivata di proroga. I dati relativi a oggetti, invece, sono conservati per un periodo massimo di cinque anni nel caso di controllo discreto o specifico e per dieci anni negli altri casi, salvo espressa richiesta di proroga.

In chiusura, il Capo relativo alla protezione dei dati prevede per gli Stati la responsabilità per i danni causati alle persone dall'uso indebito dell'N.SIS II, nonché l'obbligo di punire con sanzioni effettive, proporzionate e dissuasive l'uso improprio dei dati inseriti nel SIS II e lo scambio di dati con modalità contrarie alla decisione o al regolamento (artt. 64 e 65 della decisione 2007/533/GAI e artt. 48 e 49 del regolamento (CE) n. 1987/2006).

Gli artt. 64 della decisione e 48 del regolamento debbono reputarsi trasposti nell'ordinamento italiano dalla l. 30 settembre 1993, n. 388 e dall'art. 15 d.lgs. n. 196 del 2003, che richiama l'art. 2050 c.c., in materia di risarcimento del danno cagionato da attività pericolose.

La disciplina attuativa degli artt. 65 della decisione e 49 del regolamento deve ritenersi, invece, contenuta nella l. 1° aprile 1981, n. 121, e, segnatamente, nell'art. 12, richiamato dall'art. 10 l. n. 388 del 1993, che prevede severe sanzioni penali in caso di divulgazione di dati conosciuti mediante l'impiego dei sistemi informatici in dotazione alle forze di polizia[58].

---

57 Si suole parlare di "diritto all'oblio", con riferimento alle ipotesi in cui il diritto alla cancellazione dei dati sussista, non solo nel caso della loro erroneità o illegittimità, ma anche in virtù della loro non ulteriore necessità, al fine di consentire all'interessato di non doversi permanentemente confrontare con il proprio passato. Il diritto all'oblio è stato teorizzato dalla dottrina francese: v. R. Lindon, *Les droits de la personnalité*, Paris, Dalloz, 1984, pp. 84 sgg. Per un corrispondente nella dottrina italiana, cfr., tra i tanti, G. Busia, "*Privacy*, attività di indagine e cooperazione internazionale in materia di giustizia e sicurezza", in *Equo processo: normativa italiana ed europea a confronto*, a cura di L. Filippi, Padova, Cedam, 2006, p. 39. In giurisprudenza, Pret. Roma, 25 gennaio 1979, in "Rivista di diritto industriale", 1979, II, pp. 253 sgg., con nota di A. Nuzzo, *ivi*, 1979, II, p. 256.

58 L'art. 12 l. 121 del 1981, più precisamente, dispone che: «[1] Il pubblico ufficiale che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a tre anni. [2] Se il fatto è commesso per colpa, la pena è della reclusione fino a sei mesi». Per una applicazione della norma, v. Cass., sez. I, 21 novembre 1988, Ardagna, in "Cassazione penale", 1990, pp. 323 ss.

3. Il Sistema di informazione antifrode (AFIS) e il Sistema informativo doganale (SID)

In ambito europeo, il tema della lotta alle frodi[59] individua un'area di intersezione tra la normativa di fonte comunitaria, che, a mente dell'art. 280 TCE, pone in capo agli Stati membri l'obbligo di combattere le attività illegali suscettibili di ledere gli interessi finanziari della Comunità, e il settore della cooperazione di polizia e giudiziaria, rientrante, come noto, nel "terzo pilastro", *ex* art 29, comma 2, TUE. La doppia base giuridica su cui poggia la disciplina di contrasto agli illeciti finanziari transnazionali si riflette, nell'ambito degli strumenti operanti nell'ambito della prevenzione e repressione delle frodi, sul sistema informatico antifrode AFIS (acronimo di *Anti-Fraud Information System*). Tale archivio, istituito allo scopo di consentire il transito e lo scambio tra gli Stati membri del flusso di informazioni in materia di frodi finanziarie, è disciplinato, secondo il suddetto schema del doppio binario[60], per un verso, da fonti comunitarie e, per altro verso, da decisioni GAI.

In tale schema giuridico, rientrano nell'ambito del "terzo pilastro" le attività, inerenti al settore in esame, che sono volte all'individuazione e alla prevenzione dei reati, mentre tutte le materie residue sono ancorate al pilastro comunitario[61].

Le funzioni riconducibili al "primo pilastro" sono disciplinate dal regolamento (CE) n. 515/1997[62], che prevede l'istituzione del Sistema di informazione doganale (SID), una banca dati attinente alla Vigilanza marittima (MARSUR), un Sistema di allarme rapido per le dogane (EWS-C), due archivi di informazioni marittime (MARInfo, YACHTInfo), un Sistema di allarme rapido per le accise (EWS-E), nonché un *database* di informazioni sui sequestri di sigarette (CigInfo).

---

59 L'art. 1 della Convenzione elaborata in base all'allora vigente art. K.3 TUE e relativa agli interessi finanziari delle Comunità europee del 26 luglio 1995 – c.d. Convenzione PIF, in *GUCE*, C 316, 27 novembre 1995, p. 49 – dispone che «costituisce frode che lede gli interessi finanziari delle Comunità europee: a) in materia di spese, qualsiasi azione od omissione intenzionale relativa: all'utilizzo o alla presentazione di dichiarazioni o di documenti falsi, inesatti o incompleti cui consegua la percezione o la ritenzione illecita di fondi provenienti dal bilancio generale delle Comunità europee o dai bilanci gestiti dalle Comunità europee o per conto di esse; alla mancata comunicazione di un'informazione in violazione di un obbligo specifico cui consegua lo stesso effetto; alla distrazione di tali fondi per fini diversi da quelli per cui essi sono stati inizialmente concessi; b) in materia di entrate, qualsiasi azione od omissione intenzionale relativa: all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti cui consegua la diminuzione illegittima di risorse del bilancio generale delle Comunità europee o dei bilanci gestiti dalle Comunità europee o per conto di esse; alla mancata comunicazione di un'informazione in violazione di un obbligo specifico cui consegua lo stesso effetto; alla distrazione di un beneficio lecitamente ottenuto, cui consegua lo stesso effetto».

60 Si veda *supra*, § 2.

61 Così, P. Pallaro, *Libertà della persona e trattamento dei dati nell'Unione europea*, Milano, Giuffrè, 2002, pp. 362 sgg.

62 In *GUCE*, L 82, 22 marzo 1997, p. 1.

Si tratta di attività connesse alle dogane dell'Unione, i cui dazi costituiscono una delle voci di entrata del bilancio comunitario e la cui elusione od evasione costituisce frode che lede gli interessi finanziari della Comunità stessa. Completano l'AFIS altre banche dati, relative a differenti voci di bilancio[63]. I sistemi informativi appena elencati garantiscono la cooperazione tra gli Stati membri ed un apposito ufficio della Commissione europea, preposto alla "lotta antifrode" (OLAF, istituito con decisione 1999/352/CE[64]), che interagisce con i Paesi scambiando informazioni per mezzo di tali sistemi.

Le informazioni inserite negli archivi comprendono anche dati personali, il cui regime di trattamento è sottoposto alle prescrizioni del regolamento (CE) n. 45/2001. Tale fonte prevede che i dati devono essere trattati in modo corretto e lecito, essere pertinenti, non eccedenti rispetto alle finalità che il trattamento si propone, esatti e aggiornati, nonché cancellati trascorso il periodo di tempo necessario al raggiungimento dello scopo che ci si prefigge con il loro utilizzo. Gli artt. 13 ss. del regolamento prevedono una serie di diritti soggettivi per gli interessati dal trattamento – accesso, rettifica, blocco e cancellazione – in relazione ai quali è competente la Corte di giustizia, fatta salva la possibilità di ricorrere al Garante europeo per la protezione dei dati. Il regolamento si riferisce ai soli organismi comunitari: tanto basterebbe per escluderne l'applicazione agli enti coinvolti nella cooperazione di polizia e giudiziaria in materia penale. *Ad abundantiam*, l'art. 20 del regolamento si preoccupa di precisare che i diritti in esso disciplinati possono essere limitati qualora ciò sia necessario «per salvaguardare le attività volte a prevenire, indagare, accertare e perseguire reati». Viene in rilievo, ancora una volta, la tensione tra le esigenze proprie della prevenzione e della repressione e quelle legate alla tutela della riservatezza dei singoli.

Il regolamento (CE) n. 45/2001 non si applica naturalmente a quella parte di AFIS che rinviene la propria base giuridica nel titolo VI del TUE. Si tratta del cd. "SID terzo pilastro", disciplinato da apposita Convenzione sull'uso dell'informatica nel settore doganale[65], elaborata nel 1995 in forza dell'allora vigente art. K.3 (oggi art. 34) TUE e ratificata dall'Italia con l. 30 luglio 1998, n. 291.

In base alla disciplina contenuta nella Convenzione, il SID «ha lo scopo […] di facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali rendendo più efficaci, mediante la rapida diffusione di informazioni, le procedure di cooperazione e di controllo delle amministrazioni doganali degli Stati membri» (art. 2, par. 2).

---

63 Regolamenti (CE) n. 1469/1995, 595/1991, 1681/1994, 1831/1994, 1150/2000 e 2584/2000, relativi rispettivamente ad archivi attinenti alle frodi FEAOG, ai fondi strutturali e alle c.d. «risorse proprie» della Comunità.

64 In *GUCE*, L 136, 31 maggio 1999, p. 20.

65 In *GUCE*, C 316, 27 novembre 1995, p. 34.

Il sistema presenta una struttura a stella molto simile a quella del SIS: esso, infatti collega più unità periferiche – una per ogni Stato membro – ad un'unità centrale, avente sede a Bruxelles, e contiene informazioni su persone ed oggetti sottoposti a controllo da parte dell'autorità doganale a ciò designata. In Italia, tale autorità è stata individuata nell'Agenzia delle dogane, a mente dell'art. 3 l. n. 291 del 1998, attuato a livello operativo dal D.M. 23 febbraio 2007.

Per il raggiungimento dei suoi scopi, il sistema contiene le categorie di dati elencate nell'art. 3, recante menzione di merci, mezzi di trasporto, imprese, persone, tendenze in materia di frode, disponibilità di competenze professionali.

I dati personali inseriti nel SID sono omologhi a quelli inseriti nel SIS II, ad eccezione dei dati biometrici. Essi sono raccolti ai fini della «sorveglianza discreta» o di un «controllo specifico», espressioni da intendersi nel senso precisato al paragrafo precedente, quantunque la nuova disciplina del SIS si esprima in termini di «controllo discreto» anziché di «sorveglianza discreta».

Se le azioni indicate vengono realizzate, è possibile raccogliere e trasmettere, in tutto o in parte, allo Stato membro che ha fornito i dati, le informazione riguardanti l'avvenuta individuazione della merce, del mezzo di trasporto, dell'impresa o della persona oggetto della segnalazione, il luogo, l'ora o il motivo del controllo, l'itinerario e la destinazione del viaggio, gli accompagnatori, il mezzo di trasporto utilizzato, gli oggetti trasportati, le circostanze relative all'individuazione della merce, dei mezzi di trasporto, della società e della persona.

La Convenzione precisa che i dati possono essere inseriti se, sulla base di precedenti attività illecite, vi sono motivi sostanziali per ritenere che la persona interessata «abbia effettuato, stia effettuando o intenda effettuare gravi infrazioni alle leggi nazionali» (art. 5, par. 2). Si conferma, dunque, la duplice anima repressiva e preventiva delle banche dati in esame.

L'accesso ai dati inseriti nel SID è riservato unicamente alle autorità nazionali designate da ciascuno Stato membro. Si tratta prevalentemente delle amministrazioni doganali, ma possono accedervi anche altre autorità competenti, individuate da ciascuno Stato membro e comunicate agli altri Stati nonché al comitato esecutivo istituito a mente dell'art. 16 e composto dai rappresentanti delle amministrazioni doganali dei Paesi membri (art. 7).

Il termine di conservazione dei dati non è stabilito in misura fissa: tuttavia, è previsto che essi non debbano permanere nel sistema oltre al tempo necessario allo scopo per cui furono inseriti ed è prevista altresì una verifica annuale in tal senso (art. 12, par. 1).

Il sistema di tutela dei dati è del tutto analogo a quello contemplato dalla Convenzione Schengen per il SIS I. Il controllo sulle unità periferiche è rimesso alle autorità nazionali ed è esercitato secondo i singoli diritti nazionali, mentre il controllo sull'unità centrale è affidato a un'autorità centrale di controllo, investita, al pari di quella del SIS I, di funzioni di indirizzo e raccomandazione.

La Convenzione SID è stata modificata da un protocollo di emendamento[66], che ha inserito alcune disposizioni (quelle contenute negli artt. 12 A - 12 E), volte a disciplinare un archivio di identificazione dei fascicoli ai fini doganali (FIDE), il quale ha lo scopo di «consentire alle autorità nazionali competenti in materia di indagini doganali [...], che aprano un fascicolo o che indaghino su una o più persone o imprese, di individuare le autorità competenti degli altri Stati membri che stanno indagando o che hanno indagato su dette persone o imprese [...] mediante informazioni sull'esistenza di fascicoli d'indagine» (art. 12A della Convenzione SID).

Le Autorità competenti, a tal fine, introducono nell'archivio i dati dei fascicoli d'indagine, contenenti i dati personali di cui all'art. 12B, par. 2. L'art. 12E definisce i tempi di conservazione dei dati nell'archivio, che variano a seconda dell'esito dell'accertamento penale: tre anni, se l'azione penale non è stata esercitata, sei anni se l'azione penale è stata esercitata ma non vi è stata condanna, dieci anni se vi è stata condanna.

4. Europol e il TECS

Europol, l'Ufficio europeo di polizia, viene istituito mediante una Convenzione[67] firmata il 26 luglio 1995 sulla base dell'art. K 3 del Trattato di Maastricht (ora artt. 29 e 30 TUE).

Esso è concepito come un organismo intergovernativo operante nel settore della prevenzione e di *intelligence*, vòlto a rafforzare il coordinamento delle indagini tra le competenti autorità degli Stati membri in ordine alle fattispecie delittuose, indicate dall'art. 2, par. 2, della Convenzione istitutiva e dalle successive decisioni del Consiglio[68], suscettibili di ledere almeno due Paesi membri e in relazione alle

---

66 Il protocollo FIDE di emendamento alla Convenzione SID è stato adottato dal Consiglio in data 8 marzo 2003 e pubblicato in *GUUE*, C 139, 13 giugno 2003, p. 2. Successivamente, la Commissione ha elaborato la proposta di regolamento COM (2006) 866 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0866:FIN:IT:PDF>, che prevede la creazione di un repertorio centrale europeo dei dati e, qualora approvata, fornirebbe il quadro giuridico per l'archivio europeo d'identificazione dei fascicoli a fini doganali.

67 In *GUCE*, C 316, 27 novembre 1995, p. 1. La Convenzione è stata ratificata dall'Italia con la l. 23 marzo 1998, n. 93, la quale, oltre a recepire il testo internazionale detta alcune norme applicative volte ad assicurare il corretto funzionamento dell'accordo. Successivamente, la Convenzione è stata modificata da protocolli aggiuntivi, anch'essi ratificati dagli Stati aderenti.

68 Si tratta di: traffico illecito di stupefacenti e di materie nucleari e radioattive, organizzazioni clandestine di immigrazione, tratta di esseri umani, traffico di autoveicoli rubati. Le competenze di Europol sono ora più ampie, in virtù di svariati e sopravvenuti atti del Consiglio dell'Unione: la decisione del 3 dicembre 1998 (1999/C 26/06), in materia di terrorismo; la decisione del 29 aprile 1999 (1999/C 149/02), in tema di falsificazione di monete e altri mezzi di pagamento; la decisione del 6 dicembre 2001 (2001/C 362/02), relativa alle «forme gravi di criminalità» enumerate in un apposito allegato; l'atto del 27 novembre 2003 (2004/C 2/01), in tema di «frode fiscale e doganale».

quali sussistano indizi concreti circa l'esistenza di un'organizzazione criminale.

Al fine di conseguire i propri obiettivi di contrasto alla criminalità, Europol assume le funzioni indicate all'art. 3 della Convenzione, fra le quali ricopre un particolare rilievo la gestione delle «raccolte informatizzate di informazioni contenenti dati conformemente agli articoli 8, 10 e 11» della Convenzione stessa. I suddetti rinvii normativi richiamano, rispettivamente, il sistema di informazione, gli archivi di analisi e il sistema di indice[69]: si tratta dei tre elementi principali di cui si compone la banca dati TECS, acronimo di "*The Europol Computer System*"[70].

Il sistema di informazione contiene i dati necessari per lo svolgimento della attività di *intelligence*. Esso è accessibile, al fine di controllare di quali informazioni disponga la banca dati, sia dagli Stati membri, che da Europol[71].

Gli archivi di analisi costituiscono il *quid pluris* che differenzia il sistema TECS dagli omologhi SIS II e SID, consentendo la realizzazione di una forma di cooperazione verticale tra Europol e gli Stati membri. All'interno degli archivi trovano infatti cittadinanza categorie di informazioni ulteriori rispetto al sistema computerizzato, le quali vengono elaborate da gruppi di analisi costituiti *ad hoc* al fine di supporto di indagini transnazionali o di risoluzione di problemi specifici. L'accesso agli archivi, pertanto, è limitato agli Stati partecipanti a specifici progetti di analisi.

Il sistema di indice può essere compulsato da ogni Stato membro al fine di conoscere se una data informazione è memorizzata o meno nell'archivio, ferme restando le limitazioni alla conoscibilità del contenuto della notizia per gli Stati non facenti parte del gruppo di analisi.

Il sistema di informazione Europol, analogalmente al SIS e al SID, si articola in una unità centrale e più unità nazionali[72], differenziandosi, peraltro, dal sistema Schengen per quanto attiene al ruolo svolto dall'unità centrale, alla quale sono riconosciute specifiche funzioni di analisi, elaborazione e modifica dei dati.

Il sistema è alimentato da due flussi di informazioni. Il primo proviene direttamente dagli Stati membri, per il tramite delle Unità Nazionali Europol (UNE)[73]

---

69 Cfr. M. Bonifazi, *Europol. Ufficio europeo di polizia*, Napoli, Edizioni giuridiche Simone, 2000, p. 30.

70 J. Zeiger, *Das Europol-Computersystem. Eine Funke Hoffnung im Kampf gegen das internationale Verbrechen*, in "Kriminalistik", 1998, p. 313.

71 In particolare, l'art. 7 Convenzione riconosce un diritto di accesso diretto al sistema in capo agli ufficiali di collegamento, e un accesso indiretto, per il tramite degli ufficiali e previa dimostrazione del requisito della necessità ai fini di specifiche indagini, alle unità nazionali limitatamente ai dati riguardanti i soggetti di cui all'art. 8, par. 1, n. 2, Convenzione.

72 Ogni Stato membro costituisce un'unità nazionale, quale *trait d'union* tra la sede centrale e le competenti autorità degli stati membri, e invia all'Europol almeno un ufficiale di collegamento incaricato di difendere gli interessi dello stato presso l'ufficio centrale. Sul punto, si veda G. Calesini, *op. cit.*, p. 131.

73 In Italia, l'UNE è istituita presso il Dipartimento della pubblica sicurezza (art. 3 l. n. 93 del 1998) e segnatamente presso la Direzione centrale della polizia criminale (art. 1 d.m. interno-tesoro 1° febbraio 1996).

o degli *Europol Liaison Officers* (ELO)[74], mentre il secondo, comprensivo, sia dei dati comunicati da Stati od organismi terzi, sia dei dati prodotti dall'attività di analisi dello *staff* Europol, proviene dalle strutture interne all'ufficio.

A tali canali informativi istituzionali si affianca il riconoscimento in capo ad Europol del diritto di accedere all'archivio SIS II (art. 41 decisione 2007/533/GAI)[75], nonché al sistema di informazione visti (VIS): l'art. 3 del regolamento (CE) n. 767/2008 e soprattutto l'art. 7 della decisione 2008/633/GAI consentono all'Europol di consultare il VIS, quando è necessario per l'adempimento delle sue funzioni, ai fini di attività specifiche di analisi ovvero per la realizzazione di analisi generali di tipo strategico, a condizione (in quest'ultimo caso) che i dati VIS siano resi anonimi dall'Europol prima di tale trattamento e siano conservati in una forma che non consenta più di identificare la persona interessata.

La sinergia tra i suddetti sistemi operativi, prodromica alla realizzazione di una piattaforma comune di informazioni[76], tra cui figurano anche i dati biometrici, opera nella direzione dell'accrescimento della flessibilità e delle potenzialità operative dei sistemi in commento. Tuttavia, ha destato alcune perplessità[77] la scelta, condivisa sia dalla decisione istitutiva del SIS II che dalla decisione n. 633 del 2008, di non limitare l'accesso di Europol ai sistemi ospiti a finalità specifiche e tassativamente indicate, al fine di contribuire al mantenimento di una distinzione tra i sistemi.

Nel sistema di informazione sono conservati i dati relativi a tre categorie di persone (c.d. *targets*): quelle già condannate, quelle sospettate di aver commesso un reato[78] di competenza dell'Europol e quelle in ordine alle quali si può presumere, in presenza di determinate circostanze, che ne commetteranno in futuro (art. 8, par. 1, Convenzione Europol).

I dati identificativi ammessi alla raccolta contengono sempre le seguenti informazioni: cognome, cognome da nubile e nome, nonché eventuali *alias* o ap-

---

74 Si tratta di ufficiali di collegamento che ogni UNE deve inviare all'Europol, in numero determinato dal consiglio di amministrazione di Europol (art. 5, par. 1, Convenzione Europol), al fine di «difendere gli interessi (dell'UNE stessa) nell'ambito dell'Europol conformemente alla legislazione nazionale dello Stato membro di origine e nel rispetto delle disposizioni applicabili al funzionamento dell'Europol» (art. 5, par. 2, Convenzione Europol).

75 Si veda *supra*, § 2.

76 In questa prospettiva, cfr. *Comunicazione della Commissione concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni, COM (2005)597 def.*, 24 novembre 2005, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:IT:DOC>.

77 Si allude, in particolare, alle riserve espresse dal Garante europeo dei dati personali nel documento *Comments on the Communication of the Commission on interoperability of European databases*, 10 marzo 2006, <http://www.statewatch.org/news/2006/mar/EDPS-2006-4-interoperability.pdf>.

78 W. Wagner, *"Halt, Europol!". Probleme der europäischen Polizeikooperation für parlamentarische Kontrolle und Grundrechtsschutz*, Frankfurt am Main, 2004, p. 10.

pellativi correnti, data e luogo di nascita, cittadinanza, sesso, e, se necessario, altri elementi utili all'identificazione, quali caratteristiche fisiche particolari, obiettive e inalterabili. A ciò si aggiungono l'indicazione del *nomen iuris*, data e luogo dei reati commessi, degli strumenti usati e delle sigle dei fascicoli, delle condanne riportate e finanche dei meri sospetti di appartenenza ad un'organizzazione criminale (art. 8, par. 2, Convenzione Europol).

In ragione della natura dettagliata di tali categorie di dati, la dottrina ritiene che il loro trattamento dovrebbe essere circondato da particolari cautele[79], pretermesse, tuttavia, dalla disciplina convenzionale, la quale si limita a circoscrivere il diritto di accesso al sistema di informazione, riservando la facoltà di inserimento dei dati agli organi direttivi di Europol, alle unità UNE, agli ELO e agli agenti Europol a ciò debitamente autorizzati. Inoltre, la Convenzione stabilisce che soltanto l'ente che ha immesso i dati nel sistema è legittimato a modificarli, rettificarli o cancellarli, anche su segnalazione di altre unità che abbiano riscontrato qualche imprecisione nei dati stessi (art. 9, par. 2, Convenzione Europol).

Tutti i dati utili che non debbano essere destinati al sistema di informazione confluiscono negli archivi di lavoro a fini di analisi. Ove per "analisi", a mente dell'art. 10 Convenzione Europol, si deve intendere «la raccolta, il trattamento o l'utilizzazione di dati con lo scopo di venire in aiuto all'indagine criminale». Essa può essere strategica, se indirizzata allo studio di un fenomeno o di un problema in termini generali oppure operativa, se volta alla soluzione di casi determinati[80].

In ragione della funzione perseguita, la piattaforma di dati ammessi agli archivi di analisi è estesa ad ulteriori categorie di soggetti, contemplando, in aggiunta alle persone sospettate e condannate, anche le informazioni concernenti i potenziali testimoni, le persone offese dal reato e le persone di contatto e di accompagnamento non occasionale.

La tipologia dei dati identificativi oggetto di trattamento – definita nell'Atto del Consiglio del 3 novembre 1998[81], come modificato dalla decisione del 15 ottobre 2007[82] – è differenziata in relazione all'inerenza del dato all'una o all'altra categoria soggettiva. In particolare, per gli autori di reato, presunti o accertati, l'elenco di informazioni comprende, in aggiunta ai dati anagrafici, anche le caratteristiche fisiche particolari e inalterabili, i dati identificativi biometrici, quali impronte digitali e risultati dell'esame del DNA – seppure limitati alle indicazioni strettamente necessarie a consentire l'identificazione – e ulteriori informazioni professionali, economiche e comportamentali (art. 6, par. 2, Atto del Consiglio).

---

79 Così, P. Pallaro, *op. cit.*, p. 330.

80 V. M. Bonifazi, *Europol*, cit., p. 32.

81 Cfr., Atto del Consiglio del 3 novembre 1998, che adotta le norme applicabili agli archivi di analisi dell'Europol (1999/C 26/01), in *GUUE*, C 26, 30 gennaio 1999, p. 1.

82 Cfr. decisione 2007/673/CE, recante modifica dell'atto del Consiglio che adotta le norme applicabili agli archivi di analisi dell'Europol, in *GUUE*, L 277, 20 ottobre 2007, p. 23.

Da tale complesso normativo appare evidente, dunque, che il sistema di informazione Europol ammette il trattamento di dati sensibili, la cui elaborazione automatizzata, in base all'art. 6 della Convenzione n. 108 del 1981, dovrebbe essere vietata, salvo che gli Stati membri apprestino idonee garanzie di tutela. Tuttavia, occorre osservare, al riguardo, che la Convenzione Europol, pur ammettendo la raccolta di dati sensibili, la subordina all'osservanza del principio di stretta necessità in vista del raggiungimento delle finalità di Europol. L'eccezione al divieto risulta pertanto conforme al principio di finalità limitata, tanto più ove si osservi che la creazione di una piattaforma informativa di tale portata permette a Europol di sviluppare una complessa attività di *intelligence*[83], costituendo in tal modo il nucleo fondamentale di tutto il sistema informatizzato[84].

Strettamente collegato con gli archivi di analisi è il sistema di indice, il quale costituisce una guida alla consultazione dei primi[85]. Più precisamente, si tratta di un sistema che, se interrogato attraverso appositi moduli di ricerca, fornisce determinate informazioni presenti nel sistema[86]. Vi possono accedere il direttore, i vicedirettori, gli ELO e gli agenti Europol a ciò debitamente autorizzati (art. 11, par. 2, Convenzione Europol).

In considerazione, sia della tipologia delle informazioni contenute nella banca dati Europol, sia delle modalità di trattamento delle medesime, la Convenzione si preoccupa di dettare una disciplina specifica in materia di protezione delle informazioni, applicabile al sistema informatizzato e agli archivi d'analisi. Una disciplina che occupa un posto di primo piano come emerge chiaramente dalla predisposizione di un apposito titolo IV dedicato alle disposizioni comuni per il trattamento delle informazioni (artt. 13-25). Ciò, in quanto l'Ufficio europeo non si limita a fungere da mero *trait d'union* tra le competenti autorità degli Stati membri, ma svolge, altresì, un ruolo attivo vòlto all'analisi e alla rielaborazione delle informazioni memorizzate nell'archivio, con evidenti ripercussioni in tema di aumento del rischio per la tutela dei dati ivi contenuti.

La normativa si apre con un richiamo ai principi contenuti nella Convenzione n. 108 del 1981 e nella raccomandazione R (87)15 del Consiglio d'Europa quali parametri di conformità, sia della disciplina contenuta nella Convenzione Europol, sia delle disposizioni adottate dai singoli Stati membri in materia di protezione dei dati[87].

---

83 Con riguardo alla nozione di *intelligence*, si veda S. Ciampi, *op. cit.*, § 7.

84 V. A. Leonardi, *La gestione dei dati personali in Europol*, in "Rassegna dell'Arma dei Carabinieri", *2001, n. 3*, p. 85. Cfr. anche W. Wagner, *op. cit.*, p. 10 e J. Zeiger, *op. cit.*, p. 313, che definiscono gli archivi di analisi come "Herzstück Europols".

85 Così, A. Leonardi, *op. cit.*, p. 85.

86 W. Wagner, *op. cit.*, p. 11.

87 Cfr., al riguardo, G. Busia, *op. cit.*, pp. 64 s.

In attuazione di tali principi, viene predisposta una dettagliata disciplina a garanzia, sia della protezione, che della sicurezza dei dati raccolti.

Per quanto attiene agli organi deputati al controllo sulla protezione dei dati, sono designate due diverse autorità, rispettivamente a livello nazionale e centrale.

Per quanto concerne i Paesi membri, l'art. 23 Convenzione Europol prevede che ciascuno Stato designi un'autorità di controllo, che, in Italia, si identifica con il Garante per la protezione dei dati personali[88]. Questi è incaricato di «accertarsi, in modo indipendente e nel rispetto della legislazione nazionale, che l'introduzione, la consultazione e la trasmissione, in qualsiasi forma, all'Europol di dati di carattere personale da parte di detto Stato membro avvengano in modo lecito e che non siano lesi i diritti delle persone» (art. 23 Convenzione Europol) [89].

A livello sopranazionale, l'art. 24 della Convenzione istituisce un'autorità comune di controllo (cd. ACC-JSB), composta dai rappresentanti delle autorità garanti degli Stati membri. Dinnanzi a tale autorità il cittadino ha la possibilità di presentare un ricorso avverso le risposte dell'Europol rispetto alle richieste di accesso ai dati formulate *ex* artt. 19 e 20 della Convenzione. Non esiste alcuna possibilità di vaglio giurisdizionale sulle decisioni dell'autorità comune di controllo, salva la competenza facoltativa della Corte di giustizia delle Comunità europee a pronunciarsi in via pregiudiziale sull'interpretazione delle disposizioni della Convenzione istitutiva dell'ufficio[90].

A ulteriore presidio della protezione dei dati, l'art 18 prevede che la comunicazione dei dati a Stati e organismi terzi sia subordinata alla duplice condizione della necessità della trasmissione per la prevenzione dei reati di competenza di Europol e della garanzia di un adeguato livello di protezione delle informazioni da parte del destinatario.

In *pendant* con le disposizioni in materia di protezione dei dati, la Convenzione Europol detta alcune norme attinenti alla sicurezza fisica[91] e alla segretezza delle informazioni raccolte. Così, mentre l'art. 25 elenca una serie di misure predisposte a tutela della integrità fisica del dato, gli artt. 31 e 32 si preoccupano di garantire il segreto sulle informazioni raccolte.

Analogamente a quanto accade nel SID e nel SIS, anche nella Convenzione Europol la conservazione del dato è soggetta a limiti temporali. I dati permangono nel TECS solo fino a quando sono necessari allo scopo della segnalazione, dopo-

88 Cfr., il combinato disposto degli artt. 4, comma 2 l. n. 93 del 1998 e 154, comma 2, lett. *b*) d.lgs. 196 del 2003.

89 Sul punto, si legga, ancora, G. Busia, *op. cit.*, p. 66.

90 V. l'Atto del Consiglio del 23 luglio 1996 che stabilisce, sulla base dell'articolo K.3 del trattato sull'Unione europea, il protocollo concernente l'interpretazione, in via pregiudiziale, da parte della Corte di giustizia e delle Comunità europee, della convenzione che istituisce un Ufficio europeo di polizia, in *GUUE*, C 299, 9 ottobre 1996, p. 1.

91 Sul punto, si veda *supra*, § 1.

diché devono essere cancellati. All'esito del termine massimo di permanenza dei dati personali nel sistema, fissato dall'art. 21 della Convenzione in tre anni e ridotto ad un anno, a seguito dei successivi emendamenti contenuti nei protocolli modificativi della Convenzione[92], la necessità di una ulteriore conservazione in archivio deve essere sottoposta a nuova valutazione. Tuttavia, poiché, di prassi, tale termine ricomincia a decorrere ad ogni aggiornamento della segnalazione, è insito nel sistema il pericolo di elusione dei suddetti limiti temporali.

Sul piano della tutela soggettiva, è riconosciuto ai singoli interessati il diritto di richiedere ad Europol l'accesso ai dati che li riguardano, nonché la loro rettifica o cancellazione[93]. Il diritto di accesso si traduce nel diritto di inoltrare una domanda presso l'autorità competente di uno Stato membro scelto dall'interessato e di ricevere una risposta anche in caso di rifiuto, che può essere opposto nei soli casi tassativamente previsti dall'art. 19, par. 3, Convenzione Europol. La procedura di rettifica e di cancellazione dei dati può essere attivata dal titolare dell'informazione mediante trasmissione della relativa richiesta a Europol. In caso di inerzia o di rifiuto, l'interessato può adire l'autorità comune di controllo.

Completa il quadro delle garanzie soggettive il regime di responsabilità per danni. L'art. 38 della Convenzione stabilisce che «ciascuno Stato membro è responsabile, conformemente alla sua legislazione nazionale, di qualsiasi danno causato ad una persona in ragione di dati contenenti errori di diritto o di fatto, memorizzati o trattati in sede di Europol». Pertanto, ogni richiesta di risarcimento dei danni cagionati da Europol per il trattamento illecito dei dati dovrà essere rivolta alle autorità a ciò preposte nei singoli Stati membri, secondo la normativa *ivi* vigente. È necessario, d'altra parte, osservare che «soltanto lo Stato membro nel quale si è verificato il danno può essere oggetto di un'azione legale a scopo di indennizzo da parte della vittima». Se ne deduce che Europol, in quanto tale, non potrà mai, a mente della Convenzione, essere citato in giudizio[94]. Tale conclusione pare confermata dal tenore dell'art. 41 Convenzione, che prevede per i dipendenti di Europol diversi «privilegi e immunità»[95].

---

92 Ci si riferisce, in particolare, al protocollo recante modifica della Convenzione Europol, del 27 novembre 2003, in *GUUE*, C 2, 6 gennaio 2004, p. 3, entrato in vigore il 18 aprile 2007.

93 Cfr., artt. 19 e 20 della Convenzione Europol. Va ricordata, inoltre, la decisione del consiglio di amministrazione dell'Europol 2007/C72/17, in *GUUE*, 29 marzo 2007, C-72, p. 37, regolante il diritto d'accesso ai documenti che vertono su aspetti relativi alle attività, alle politiche e alle decisioni di Europol. Si veda, sul punto, il commento di E. Selvaggi, *Una marginale operazione di trasparenza nell'attesa della Procura Europea*, in "Guida al diritto. Diritto comunitario e internazionale", 2007, n. 3, p. 34.

94 L'art. 288 TCE, secondo cui la Corte di giustizia è competente a conoscere e a liquidare il danno cagionato dai propri funzionari nell'esercizio delle loro funzioni non si applica al secondo e al "terzo pilastro", in quanto non richiamato dall'art. 41 Tue, che elenca le norme di diritto comunitario applicabili anche alla restante parte dell'UE.

95 Sul punto, si veda l'Atto del Consiglio del 19 giugno 1997 che stabilisce sulla base dell'articolo K.3 del trattato sull'Unione europea e dell'articolo 41, paragrafo 3 della convenzione Europol,

Secondo alcuni Autori, il sistema di garanzie offerte ai singoli dalla Convenzione è ampiamente soddisfacente[96]. A parere di altri, invece, non è condivisibile che, malgrado il richiamo alle citate fonti internazionali in materia di tutela dei dati – segnatamente, la Convenzione n. 108 e la raccomandazione R (87) 15 –, nel TECS possano essere inseriti e trattati, seppure in casi di necessità, dati personali sensibili, in maniera «scollegata da garanzie e controlli»[97]. È stato, infatti, rilevato che la Convenzione Europol misconosce «la protection de la vie privée, une aide juridique d'accès facile, l'obligation de respecter les droits de l'homme»[98]. Nella stessa ottica, si è sostenuto che la normativa in parola presenta profili di «eccessiva indeterminatezza»[99], lasciando emergere la percezione di una «scarsa trasparenza»[100].

Le critiche appena riportate potrebbero sembrare eccessive, soprattutto se si considera che la Convenzione Europol dedica numerose norme alla qualità del trattamento dei dati, sia in riferimento alla loro protezione, che alla loro sicurezza. Inoltre, è significativo il riconoscimento dei diritti di accesso, rettifica e cancellazione dei dati e la possibilità di ricorso all'autorità comune di controllo in ordine all'esercizio dei diritti medesimi, nonché l'obbligo di cancellazione dei dati non più necessari alle attività dell'ufficio. Nondimeno, si deve segnalare come l'assenza di un controllo giurisdizionale sulle decisioni di tale autorità possa essere vista come un sensibile indebolimento delle garanzie per i singoli. È altresì censurabile il sistema di immunità, che impedisce le azioni legali nei confronti di Europol e dei suoi dipendenti[101].

5. Il futuro di Europol: la decisione del Consiglio

La Convenzione Europol è stata oggetto di una serie di modifiche contenute in tre protocolli aggiuntivi, approvati ed entrati in vigore nel 2007, all'esito di un

---

il protocollo relativo ai privilegi e alle immunità di Europol, dei membri dei suoi organi, dei suoi vicedirettori e agenti, in *GUUE*, C 221, 19 luglio 1997, p. 1.

96 In tal senso, G. Busia, *op. cit.*, p. 66.

97 Così, M. Bonetti, *op. cit.*, p. 70; P. Pallaro, *op. cit.*, pp. 324 ss.; P. Tonini, "Il progetto di un pubblico ministero europeo nel *Corpus Juris*", in *La giustizia penale italiana nella prospettiva internazionale*, Atti del XII Convegno di studio Enrico de Nicola, Milano, Giuffré, 2000, p. 113.

98 Queste le parole di L. Van Outrive, "La collaboration policière en Europe: de Schengen à Europol", in *Da Schengen a Maastricht*, cit., p. 78.

99 Così, P. Bilancia, "La tutela della *privacy* e la banca dati dell'Europol dopo il trattato di Amsterdam", in *La legge italiana sulla* privacy, a cura di M.G. Losano, Bari, Laterza, 2001, p. 267.

100 Ancora, P. Bilancia, *op. cit.*, p. 273.

101 Sul punto, cfr. A. Nachbaur, *Europol – Beamte und Immunität – ein Stüdenfall des Rechtsstates*, in "Kritische Justiz", 1998, p. 326; W. Wagner, *op. cit.*, pp. 7 sgg.

lungo e complesso *iter* di revisione[102]. La farraginosità della procedura modificativa della Convenzione, che richiede la previa ratifica dei protocolli da parte di tutti gli Stati membri, ha posto in rilievo l'opportunità di predisporre una nuova base giuridica per Europol. Collocandosi in questa prospettiva, il 20 dicembre 2006 la Commissione ha presentato una proposta di decisione elaborata sulla base dell'art. 34, par. 2, lett. *c*) TUE[103]. L'entrata in vigore dell'atto in parola siglerà il definitivo superamento della Convenzione istitutiva dell'Ufficio europeo di polizia e la sua sostituzione con uno strumento più appropriato ai fini della fondazione di un organo interno all'Unione e più flessibile in relazione alle successive esigenze di modifica[104].

La decisione si propone di conseguire il potenziamento di Europol, attraverso il duplice *iter* dell'ampliamento della sfera di competenza e del rafforzamento del suo sistema di informazione[105].

---

102 Si tratta, rispettivamente, dei seguenti atti: protocollo recante modifica all'art. 2 e all'allegato della Convenzione Europol, del 30 novembre 2000, in *GUUE*, C 358, 13 dicembre 2000, p. 1, entrato in vigore il 29 marzo 2007; protocollo relativo ai privilegi e alle immunità di Europol, del 28 novembre 2002, in *GUUE*, C 312, 16 dicembre 2002, p. 1, entrato in vigore il 29 marzo 2007; protocollo recante modifica della Convenzione Europol, del 27 novembre 2003, in *GUUE*, C 2, 6 gennaio 2004, p. 3, entrato in vigore il 18 aprile 2007. Tale ultimo atto apporta sostanziali modifiche alla Convenzione, introducendo, in particolare, l'art. 6 *bis*, recante la facoltà di procedere al trattamento dei dati anche al fine di determinarne la pertinenza rispetto alle funzioni istituzionali di Europol. L'attuazione di tale disposizione è regolata dalla decisione del Consiglio 2007/413/GAI, in *GUUE*, L 155, 15 giugno 2007, p. 78.

103 Proposta di decisione del Consiglio che istituisce l'Ufficio europeo di polizia (Europol), COM (2006) 817 def., su cui è stato raggiunto un ampio e definitivo accordo nella riunione del Consiglio del 9 aprile 2008 (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0817:FIN:IT:PDF>). Cfr., da ultimo, la versione pubblicata in *Documento del Consiglio n. 8706/3/08*, 9 ottobre 2008, <http://register.consilium.europa.eu/pdf/it/08/st08/st08706-re03.it08.pdf>. Va segnalato, inoltre, che il 23 maggio 2008 la Commissione ha approvato una Proposta di regolamento che modifica il regolamento (Euratom, CECA, CEE) n. 549/69 del Consiglio che stabilisce le categorie di funzionari ed agenti delle Comunità europee ai quali si applicano le disposizioni degli articoli 12, 13, secondo comma, e 14 del protocollo sui privilegi e sulle immunità delle Comunità (COM(2008) 305 def., in *GUUE*, C 154 E, p. 257), la quale è necessaria per assicurare l'applicazione della decisione istitutiva di Europol a decorrere dal 1° gennaio 2010 (cfr. la *Relazione alla proposta di regolamento*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0305:FIN:IT:PDF>.

104 A mente del considerando n. 5, la decisione realizza la trasformazione di Europol in un'entità dell'Unione. Essa, in quanto tale, sarà finanziata dal bilancio generale dell'UE, con evidenti ripercussioni sotto il profilo del rafforzamento del ruolo di controllo democratico del Parlamento europeo. Si vedano, al riguardo, le considerazioni espresse nella *Relazione della Commissione per le libertà civili, la giustizia e gli affari interni sulla proposta di decisione del Consiglio che istituisce l'Ufficio europeo di polizia (EUROPOL) (COM(2006)0817 def. – C6 0055/2007 – 2006/0310(CNS))*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2007-0447+0+DOC+PDF+V0//IT>, p. 36.

105 L'art. 5 enuncia le finalità di Europol, fra cui emerge quella di «raccogliere, conservare, trattare, analizzare e scambiare le informazioni e l'*intelligence*».

Quanto al primo aspetto, l'art. 4 della decisione estende il mandato di Europol ad ogni forma grave di criminalità, rientrante tra quelle comprese nell'allegato, che interessi due o più Stati membri, sopprimendo il requisito convenzionale della sussistenza di gravi indizi circa l'operatività di una struttura criminosa e consentendo, per tale via, il supporto di Europol ai singoli Stati anche nelle indagini penali transnazionali in cui non emerga fin dall'inizio il coinvolgimento della criminalità organizzata[106].

Quanto al secondo aspetto, relativo al potenziamento del meccanismo di circolazione delle informazioni, occorre premettere che, accanto al mantenimento delle tradizionali componenti del sistema informatizzato Europol – il sistema di informazione, gli archivi di lavoro ai fini di analisi e la funzione di indice – la decisione introduce la facoltà in capo ad Europol di istituire anche altri sistemi di trattamento dei dati, previa consultazione dell'autorità di controllo comune ed approvazione del Consiglio.

La previsione di strumenti alternativi si colloca *a latere* del potenziamento del sistema principale di informazione, realizzato mediante l'inserimento di nuove classi di dati e l'ampliamento del diritto di accesso da parte delle autorità competenti. In particolare, mentre permangono immutate le categorie di soggetti sottoposti a segnalazione[107], l'art. 12, par. 2, della proposta di decisione – nella versione di ottobre 2008 – introduce il trattamento di nuovi dati di identificazione, quali i documenti di identità, i passaporti e i dati biometrici, comprensivi di dati dattiloscopici e del profilo DNA, espressamente limitato alla parte non codificante[108].

In relazione a tale piattaforma di dati, l'art. 13 del testo della proposta di decisione ribadisce la legittimazione alla consultazione del sistema da parte degli Stati membri e delle autorità interne di Europol, introducendo la facoltà di accesso diretto in capo alle unità nazionali anche in relazione ai dati riguardanti i potenziali criminali[109]. Parimenti, è confermata la struttura bifronte di alimentazione del sistema di informazione, le cui fonti sono rappresentate, per un verso, dai Paesi membri e, per altro verso, da Europol stesso, in veste di collettore dei dati prodotti dalle attività di analisi e delle informazioni provenienti da Stati e organismi terzi. Su tale fronte, la novità è rappresentata dalla inclusione degli

---

106 Così, la *Relazione sulla proposta di decisione del Consiglio COM (2006) 817 def.*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0817:FIN:IT:PDF>, p. 5.

107 Ossia, da un lato, le persone indiziate e condannate per un reato di competenza di Europol e, dall'altro, le persone in relazione alle quali sussistono indici di probabilità di commissione di siffatti reati (art. 12, par. 1).

108 Cfr. il *Documento del Consiglio n. 8706/3/08*, cit.

109 Il superamento del requisito della sussistenza di esigenze investigative collegate a specifiche indagini, cui l'art. 7 Convenzione Europol subordinava l'accesso delle unità nazionali in relazione alle categorie di persone di cui all'art. 8, par. 1, n. 2 Convenzione, è dovuto alla necessità di non compromettere l'operatività di Europol. Così, la *Relazione della Commissione sulla proposta di decisione del Consiglio COM (2006) 817 def.*, cit., p. 6.

organismi privati nel novero dei canali di alimentazione di Europol. In parziale accoglimento delle sollecitazioni espresse dal Garante europeo circa la necessità di salvaguardare la correttezza oggettiva dei dati provenienti da privati[110], la decisione ne subordina l'accesso al sistema alla condizione che siano state trasmesse dall'unità nazionale di uno Stato membro in conformità della legislazione nazionale o che provengano da un Paese terzo con cui Europol ha stipulato un accordo di cooperazione. Nulla è stabilito, invece, riguardo all'accertamento della legittimità delle modalità di raccolta e del trattamento dei dati in conformità della direttiva 95/46/CE[111].

Ponendosi nella prospettiva di agevolare lo scambio di dati con organi e Paesi terzi e di assicurare l'interconnessione del suo sistema di trattamento dati con quelli degli altri organi UE, la decisione prevede la possibilità per Europol, da un lato, di istituire canali privilegiati di scambio di informazioni mediante la conclusione di accordi, tanto con le istituzioni dell'UE, quali OLAF ed Eurojust, quanto con Paesi ed uffici esterni all'Unione.

A ciò si aggiunga il summenzionato riconoscimento in capo a Europol del diritto di accedere all'archivio SIS II e al sistema di informazione visti (VIS)[112].

A completamento del rinnovato quadro giuridico, la decisione si preoccupa di rafforzare, altresì, i meccanismi di protezione dei dati raccolti nel sistema.

Il quadro giuridico eletto a parametro di conformità delle norme a tutela dei dati è rappresentato dalla Convenzione del Consiglio d'Europa sulla protezione dei dati personali del 1981 e dalla Raccomandazione R(87) 15 del 1987 del Comitato dei Ministri, cui si affianca la decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali in funzione di normativa applicabile allo scambio di informazioni tra gli Stati membri ed Europol.

All'interno di questa cornice normativa si situa la normativa sulla protezione e la sicurezza dei dati contenuta nel capo V della decisione.

In particolare, ai sensi dell'art. 10 il trattamento delle informazioni e dell'*intelligence* subisce un considerevole ampliamento, essendo consentito ad Europol nella misura in cui è necessario al soddisfacimento dei suoi obiettivi, compreso quello di stabilire se i dati sono rilevanti per lo svolgimento dei suoi compiti[113].

---

110 Cfr. il *Parere del Garante europeo della protezione dei dati sulla proposta di decisione del Consiglio che istituisce l'Ufficio europeo di polizia (Europol) (COM (2006)817 def.)*, in *GUUE*, C 255, 27 ottobre 2007, p. 15.

111 Il Garante europeo, con riferimento alla proposta di decisione COM (2006) 817 def., auspicava invece maggiori garanzie a salvaguardia della correttezza dei dati, con riferimento, in particolare, alle modalità di raccolta e selezione dei medesimi in conformità della legislazione nazionale dello Stato di provenienza (cfr., ancora, *Parere del Garante europeo della protezione dei dati sulla proposta di decisione del Consiglio che istituisce l'Ufficio europeo di polizia (Europol)*, cit., p. 16.

112 Si veda *supra*, § 2 e 4. Cfr. anche *infra*, M. Gialuz, *op. cit.*, § 5.

113 Tale previsione ha sollevato dubbi di conformità con il principio di proporzionalità, nella parte in cui non prevede che il trattamento del dato sia limitato al fine specifico di valutare la

La conservazione dei dati in archivio è ammessa per il tempo necessario al raggiungimento degli scopi di Europol. La proposta di decisione fa propria la scelta adottata dalla Convenzione in prima istanza, nel testo antecedente le modifiche del 2003, di sottoporre la valutazione circa la necessità della permanenza del dato in archivio a cadenze triennali, anziché annuali.

Sul piano delle garanzie soggettive, gli artt. 30 sgg. riconoscono al titolare dell'informazione il diritto di accesso al dato, attivabile tramite la presentazione di apposita domanda presso la competente autorità di uno Stato membro a sua scelta, cui Europol può opporre rifiuto solo nei casi espressamente previsti dalla decisione, e i diritti di rettificazione e cancellazione.

Il rispetto del quadro giuridico sulla tutela delle informazioni raccolte è garantito, a mente dell'art. 28, dall'istituzione di un responsabile per la protezione dei dati del tutto indipendente, incaricato di assicurare la legittimità del trattamento dei dati e la conoscenza dei diritti spettanti ai titolari delle informazioni ai sensi della decisione.

6. EPOC III di Eurojust

L'edificazione di un organismo centrale europeo che agevoli il coordinamento tra le autorità giudiziarie degli Stati membri[114] si erige sulle fondamenta dell'art. 31 TUE – come modificato dal Trattato di Nizza –, che costituisce la base giuridica della decisione 2002/187/GAI istitutiva di Eurojust[115].

Le funzioni principali di Eurojust riguardano il coordinamento tra le autorità giudiziarie degli Stati membri responsabili dell'azione penale, l'assistenza in relazione ad indagini riguardanti le fattispecie criminose elencate dalla decisione istitutiva[116], anche sulla base delle informazioni fornite da Europol, e la coopera-

---

sua pertinenza alle funzioni di sistema. Così, il *Parere del Garante europeo della protezione dei dati sulla proposta di decisione del Consiglio che istituisce l'Ufficio europeo di polizia (Europol)*, cit., p. 15.

114 L'idea di realizzare un'unità di coordinamento giudiziario composta da magistrati o funzionari nazionali di pari competenza si deve al vertice europeo di Tampere del 1999. Sul punto, si veda il § 46 delle *Conclusioni della Presidenza. Consiglio europeo di Tampere*, in "Cassazione penale", 2000, p. 309.

115 In *GUUE*, L 63, 6 marzo 2002, p. 1, modificata dalla successiva decisione 2003/659/GAI, in *GUUE*, L 245, 29 settembre 2003, p. 44. La decisione istitutiva di Eurojust ha trovato attuazione in Italia con l. 14 marzo 2005, n. 41.

116 Cfr. G. De Amicis, *Riflessioni su Eurojust*, in "Cassazione penale", 2002, pp. 3611 sgg.; A. Saccucci, *Cooperazione giudiziaria tra gli Stati europei: nasce "Eurojust"*, in "Diritto penale e processo", 2002, p. 651. Più precisamente, Eurojust è competente in relazione ai reati di criminalità informatica, criminalità ambientale, riciclaggio, partecipazione ad organizzazioni criminali negli Stati dell'Unione, frode, corruzione nonché a ogni altro reato che colpisca gli interessi finanziari dell'Unione. Inoltre, Eurojust è competente per tutti quei reati che presentino delle relazioni con quelli appena enunciati o con quelli per cui è competente l'Europol (art. 4 decisione 2002/187/GAI) .

zione con la Rete giudiziaria europea. A tali fini, la decisione istitutiva riconosce a Eurojust[117] una serie di poteri strumentali, quali la facoltà di inoltrare alle autorità statali competenti richieste di avviare indagini, di coordinarle, di rinunziarvi e di istituire delle squadre investigative comuni.

Lo strumento principale di cui Eurojust si avvale per l'esercizio delle proprie funzioni è costituito dall'impiego di una banca dati, consultabile attraverso procedimenti automatizzati o casellari manuali (art. 14 decisione 2002/187/GAI)[118]. Il *software* per la gestione di tale *database* prende il nome di EPOC, acronimo di *European Pool against Organized Crime*, giunto alla sua terza versione[119].

L'analisi strutturale della base informativa consente di individuare al suo interno due macropartizioni.

La prima consiste in un archivio automatizzato contenente un indice dei dati relativi alle indagini, all'interno del quale possono essere conservati, sia dati non personali, sia dati personali (art. 16, par. 1, decisione 2002/187/GAI). L'indice agevola la gestione e il coordinamento delle indagini penali mediante il confronto incrociato delle informazioni, consentendo, ad un tempo, il controllo sulla legittimità del trattamento dei dati.

La seconda comprende i c.d. archivi di lavoro temporaneo, creati per consentire il trattamento dei dati relativi ai casi specifici di competenza dei membri nazionali di Eurojust (art. 16, par. 3, decisione 2002/187/GAI). In particolare, a ogni caso viene assegnato un archivio di lavoro temporaneo in cui sono contenuti informazioni e documenti relativi al caso medesimo, distinti in dati personali e non personali.

Ogni archivio si compone di parti private – accessibili ai singoli gruppi di lavoro, quali delegazioni dell'Eurojust, singoli procuratori e loro assistenti negli uffici dell'autorità giudiziaria nazionale – e di una parte condivisa, accessibile a tutti i gruppi di lavoro coinvolti nel caso.

Entrambe le partizioni dell'archivio sono alimentate dalle informazioni di cui ogni membro nazionale dispone e che rinviene dall'accesso, espressamente

---

117 Devono essere tenuti distinti, peraltro, i poteri conferiti ad Eurojust in composizione collegiale dalle prerogative attribuite ai singoli membri nazionali. Sul punto, per tutti, F. De Leo, *Il coordinamento giudiziario in Italia e in Europa e le sue prospettive*, in "Questione giustizia", 2005, p. 1135.

118 Cfr., sul punto, M. Bonetti, *op. cit.*, p. 101; G. De Amicis, *op. cit.*, p. 3615; B. Piattoli, *Sistema di protezione dei dati personali nel terzo pilastro: esigenze di tutela e di rafforzamento delle indagini*, in "Diritto penale e processo", 2007, p. 1689; A. Saccucci, *op. cit.*, p. 652.

119 Cfr. <http://www.giustizia.it/ministero/struttura/progetto__epoc__III.htm>. Il *software* EPOC III, la cui attività di sperimentazione è terminata nel maggio 2008, è stato configurato in funzione di sviluppo ed evoluzione del sistema EPOC II. Per altro verso, tale sistema è utilizzato anche in Italia dalla Direzione Nazionale Antimafia e dalle Direzioni Distrettuali Antimafia. Ciò, a conferma del parallelismo, prospettato in dottrina, tra la logica cui Eurojust si ispira e quella della Direzione nazionale antimafia. Sul punto, si veda F. De Leo, *op. cit.*, p. 1134; P. Tonini, *Manuale di procedura penale*, Milano, Giuffrè, 2008[9], p. 864.

previsto dall'art. 9, par. 4, decisione 2002/187/GAI, alle banche dati appartenenti al sistema giudiziario del proprio ordinamento[120].

Per quanto attiene al contenuto dell'archivio, a mente dell'art. 15 della decisione istitutiva, Eurojust può trattare soltanto i dati identificativi delle persone fisiche e giuridiche che siano comprese nelle categorie di indagati, imputati, testimoni o persone offese in un procedimento penale che rientri nella sua sfera di competenza[121]. Il grado di specificazione delle informazioni ammesse all'archivio è diversificato in relazione all'appartenenza ad una delle suddette categorie.

In particolare, in relazione ai soggetti indiziati o imputati, ai dati anagrafici e al luogo di residenza si affiancano ulteriori informazioni, quali documenti di identità, patenti di guida e passaporti, conti bancari, circostanze che fanno presumere la rilevanza internazionale del caso ed indizi di appartenenza a un'organizzazione criminale. Con riguardo alle persone offese e ai testimoni di un procedimento penale, l'elenco delle informazioni accolte in archivio è limitato ai dati anagrafici e di residenza e alle informazioni concernenti la descrizione della *notitia criminis* e il grado di completezza delle indagini preliminari. In entrambi i casi, il catalogo di dati identificativi non è tassativo, in quanto, con norma di chiusura, l'art. 15, par. 3, dispone, per entrambe la categorie, la memorizzazione in archivio, benché in casi eccezionali e per un periodo di tempo limitato, di «altri dati personali relativi alle circostanze di un reato qualora siano di rilevanza immediata e rientrino nell'ambito di indagini in corso, al cui coordinamento l'Eurojust contribuisce», comprensivi anche dei dati sensibili che siano «necessari per le indagini nazionali pertinenti e per il coordinamento all'interno dell'Eurojust».

L'operatività del sistema[122] è rafforzata dalla possibilità di stabilire molteplici relazioni di collegamento tra i dati immessi in archivio. L'EPOC è in grado di scoprire automaticamente i potenziali collegamenti funzionali a stabilire le relazioni tra i casi, le quali si rinvengono quando la medesima fattispecie di reato è trasversale a due o più casi. Non appena il sistema rileva in via automatica l'esistenza di un potenziale collegamento, gli operatori vengono immediatamente informati dal sistema al fine di consentire loro di disporre le opportune verifiche in merito alla sussistenza o meno di un collegamento reale, in esito alle quali il collegamento medesimo verrà contrassegnato come confermato o rifiutato.

Sul versante della protezione dei dati, la decisione istitutiva di Eurojust elegge a parametro di conformità della disciplina *ivi* contenuta la Convenzione del Consiglio d'Europa n. 108 del 1981 (art. 14, par. 2, decisione 2002/187/GAI).

La normativa in tema di trattamento dei dati soddisfa, sia il principio di legalità, ove stabilisce che i dati devono essere elaborati conformemente alla legge,

---

120 Si legga, sul punto, M. Bonetti, *op. cit.*, p. 100, nota 164.

121 Al riguardo, ancora, M. Bonetti, *op. cit.*, p. 101.

122 Sulla configurazione e gli aspetti operativi del sistema EPOC, si rinvia a <http://www.giustizia.it/newsonline/data/multimedia/1273.pdf>.

sia i principi di correttezza e proporzionalità dei dati, che sono elevati a standards qualitativi delle informazioni raccolte in archivio, sia, infine, il principio di finalità limitata, per cui la conservazione dei dati, da sottoporre a verifica triennale, non può eccedere il tempo strettamente necessario al conseguimento delle finalità istitutive[123]. Qualche dubbio di conformità ai parametri convenzionali può sorgere, invero, in relazione all'ammissione al trattamento dei dati sensibili, cui la Convenzione, in linea di principio, oppone espresso divieto. La latitudine di tale previsione è temperata, per contro, dall'art. 15, par. 4, della decisione Eurojust, che ne subordina il trattamento all'inserimento nell'indice e all'immediata informazione al delegato per la protezione dei dati. Tale dichiarazione di principio è specificata dal regolamento interno dell'Eurojust[124], il cui art. 18, proponendosi di offrire maggiori garanzie alla persona interessata dal trattamento eccezionale dei dati di cui all'art. 15, par. 3, della decisione istitutiva, dispone che «l'Eurojust adotta misure tecniche adeguate per garantire che il delegato alla protezione dei dati sia automaticamente informato dei casi» in cui ricorre l'ipotesi appena prospettata.

Su un altro versante, questa norma impone un chiarimento riguardo alla figura del «delegato alla protezione dei dati».

Nel quadro degli organi di controllo del trattamento dei dati personali designati dalla decisione istitutiva di Eurojust, il delegato svolge una duplice funzione, di garanzia della legittimità dell'utilizzo dei dati contenuti nel sistema e di informativa al collegio. Designato dal collegio tra i membri del personale, al delegato per la protezione dei dati viene assegnato il compito precipuo di verificare la legittimità delle operazioni di raccolta e impiego dei dati e di comunicare al collegio eventuali irregolarità (art. 17 decisione 2002/187/GAI)[125].

Ove rilevi una violazione delle norme sul trattamento dei dati e il collegio non si attivi entro un termine ragionevole, il delegato può adire l'autorità di controllo comune[126], la quale ha il compito di decidere sui ricorsi presentati, sia dal

---

123 Secondo la *Relazione del Parlamento europeo del 14 novembre 2001 sul Progetto di decisione del Consiglio che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità organizzata (12727/1/2001 - C5-0514/2001 - 2000-0817(CNS))*, la conservazione dei dati deve essere informata al parametro di stretta necessità in relazione alle finalità perseguite (il testo è disponibile in <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0398+0+DOC+WORD+V0//IT&language=IT>).

124 Approvato con atto del Consiglio del 28 febbraio 2005, recante «Disposizioni del regolamento interno dell'Eurojust relative al trattamento e alla protezione dei dati personali», è disponibile in *GUUE*, C 68, 19 marzo 2005, p. 1.

125 Cfr., in argomento, B. Piattoli, *Cooperazione giudiziaria e pubblico ministero europeo*, Milano, Giuffré, 2002, p. 167; A. Saccucci, *op. cit.*, p. 652.

126 Ai sensi dell'art. 23 della decisione istitutiva, l'autorità di controllo comune è composta, a garanzia della sua indipendenza, da giudici nazionali che non cumulino la qualifica di membri di Eurojust o da soggetti che svolgano attività tali da conferire loro un'indipendenza adeguata, designati da ogni Stato membro.

delegato, sia dai singoli interessati che lamentino la violazione dei diritti loro riconosciuti dalla decisione.

Sul piano delle tutele soggettive, l'art. 19 della decisione istitutiva riconosce al titolare dell'informazione specifici diritti di accesso ai dati, rettifica e cancellazione. Il diritto d'accesso viene attivato dalla presentazione di una domanda, da parte dell'interessato, ad uno Stato membro a sua scelta, a cui potrà essere opposto rifiuto solo in presenza di un rischio di compromissione delle attività di Eurojust, di un'indagine in corso o dei diritti di terzi[127]. Avverso il diniego all'accesso, oltre che alla richiesta di rettifica e cancellazione dei dati, è data facoltà di ricorso all'autorità di controllo comune.

Lo scambio di informazioni tra Eurojust e i Paesi terzi o le organizzazioni internazionali è subordinato alla conclusione di un accordo di collaborazione, in mancanza del quale la trasmissione dei dati è consentita solo a condizione che i terzi assicurino un livello comparativamente sufficiente di protezione dei dati.

La conclusione di specifici accordi rileva anche ai fini dell'interoperabilità tra Eurojust e gli altri sistemi automatizzati operanti in ambito UE. A tal proposito, ove l'interconnessione tra i sistemi non sia espressamente prevista dai rispettivi strumenti istitutivi – sul modello dell'art. 42 della decisione 2007/533/GAI, recante l'accesso diretto di Eurojust alla banca dati SIS II – gli aspetti relativi alle forme di coordinamento tra i sistemi e l'accesso reciproco ai dati contenuti negli archivi sono regolati da specifici accordi, quale quello avente ad oggetto i rapporti di cooperazione informativa tra Europol ed Eurojust. Tale accordo, concluso il 9 giugno 2004 sulla base dell'art. 26, par. 1, della decisione 2002/187/GAI, prevede, in particolare, che Eurojust possa chiedere a Europol di aprire un archivio di analisi, lasciando quest'ultimo libero di dare corso o meno a tale richiesta. Non è ammesso, per contro, l'accesso diretto reciproco ai rispettivi archivi.

Da ultimo, l'adeguatezza del quadro giuridico regolante Eurojust al crescente rafforzamento dei meccanismi di cooperazione informativa in ambito UE è stata discussa nell'ambito di un'iniziativa, avanzata da quattordici Stati membri, mirante a potenziare il ruolo e le capacità di Eurojust su tre livelli[128].

---

127 La previsione è conforme a quanto rimarcato dalla *Relazione del Parlamento europeo del 14 novembre 2001 sul Progetto di decisione del Consiglio che istituisce l'Eurojust*, cit., p. 33, in cui si sottolinea che il diritto d'accesso non deve poter essere limitato dalle disposizioni nazionali dello Stato contraente.

128 Cfr. l'Iniziativa del Regno del Belgio, della Repubblica ceca, della Repubblica d'Austria, della Repubblica di Estonia, della Repubblica francese, della Repubblica italiana, del Granducato di Lussemburgo, del Regno dei Paesi Bassi, della Repubblica di Polonia, della Repubblica portoghese, della Repubblica slovacca, della Repubblica di Slovenia, del Regno di Spagna, e del Regno di Svezia, in vista dell'adozione di una decisione del Consiglio, del ..., relativa al rafforzamento dell'Eurojust e che modifica la decisione 2002/187/GAI, in *GUUE*, C 54, 27 febbraio 2008, p. 4. V. l'ultima versione pubblicata in *Documento del Consiglio n. 13683/08*, 6 ottobre 2008, <http://register.consilium.europa.eu/pdf/it/08/st13/st13683.it08.pdf>.

Il primo livello attiene all'estensione delle funzioni degli organi di cui si compone Eurojust, sia nelle ipotesi in cui opera a livello collegiale, sia nella prospettiva della definizione di una base di poteri comuni ed equivalenti a tutti i membri nazionali.

Il secondo livello riguarda il consolidamento del sistema informativo, mediante la modificazione di alcuni punti cardine della disciplina normativa della banca dati.

In particolare, l'art. 1, par. 15, del progetto di decisione del Consiglio introduce la possibilità di istituire un sistema automatico di gestione dei fascicoli, composto da archivi di lavoro temporanei e da un indice contenente dati personali e non personali. La possibilità di creare archivi di lavoro temporanei, in relazione ai casi specifici di cui si occupano, è estesa ai membri nazionali, i quali possono consentire o limitare l'accesso all'archivio alle altre autorità. L'accesso ai dati è consentito, in via generale, al personale autorizzato di Eurojust, ai membri nazionali di Eurojust, ai loro assistenti e, inoltre, ai corrispondenti nazionali nella misura in cui sono collegati al sistema di gestione dei fascicoli. Alle autorità nazionali è data facoltà di accedere, sia all'indice, sia agli archivi creati o gestiti dai membri dello Stato cui appartengono, salvo che l'ingresso al sistema non sia stato espressamente negato.

La piattaforma di dati ammessa all'archivio è ampliata dall'art. 1, par. 14, del progetto, che introduce il trattamento di ulteriori dati identificativi personali, quali il numero di telefono, gli indirizzi di posta elettronica e i dati di immatricolazione dei veicoli. Una novità di rilievo è costituita dalla ulteriore previsione dell'inserimento dei dati biometrici, e, segnatamente, fotografie, impronte digitali e profili DNA espressamente limitati alla parte non codificante del DNA, in accordo alla sollecitazione espressa sul punto dal Garante europeo della protezione dei dati[129].

Il terzo livello su cui interviene la proposta di decisione attiene al consolidamento delle interconnessioni con gli organismi operanti in ambito comunitario. In particolare, l'art. 1, par. 24, prevede la possibilità per Eurojust di instaurare e mantenere relazioni di cooperazione con Europol, oltre che con gli organismi di "primo pilastro" quali OLAF e gli organi di controllo delle frontiere. Lo scambio delle informazioni con gli altri archivi informatizzati è subordinato alla conclusione di specifici accordi, previa consultazione dell'autorità di controllo comune e approvazione del Consiglio.

---

129 Si veda il *Parere del garante europeo della protezione dei dati personali sull'iniziativa del Regno del Belgio, della Repubblica ceca, della Repubblica d'Austria, della Repubblica di Estonia, della Repubblica francese, della Repubblica italiana, del Granducato di Lussemburgo, del Regno dei Paesi Bassi, della Repubblica di Polonia, della Repubblica portoghese, della Repubblica slovacca, della Repubblica di Slovenia, del Regno di Spagna, e del Regno di Svezia, in vista dell'adozione di una decisione del Consiglio, del ..., relativa al rafforzamento dell'Eurojust e che modifica la decisione 2002/187/GAI, n. 2008/C 54/02*, in *GUUE*, C 310, dicembre 2008, p. 1.

Principio di accessibilità e banche dati di "primo pilastro"

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

SOMMARIO: 1. Premessa. – 2. Il sistema Eurodac. – 3. Il sistema di informazione visti (VIS). – 4. (Segue): il regolamento VIS. – 5. (Segue) l'accesso al VIS delle autorità di *law enforcement*. – 6. Considerazioni conclusive.

1. Premessa

Il fine di conservare e sviluppare uno spazio di libertà, sicurezza e giustizia (art. 2 TUE) è stato perseguito dall'Unione europea anche attraverso la creazione di diversi sistemi informativi centralizzati. Tra questi, vanno annoverati sistemi che rispondono a diverse finalità. Anzitutto, si contano diverse banche dati costituite specificamente per finalità di cooperazione di polizia e giudiziaria, quali il TECS di Europol o EPOC-III di Eurojust; in secondo luogo, vi sono sistemi dotati di una finalità mista, come il SIS o il SID; infine, si segnalano banche dati pensate per garantire la libera circolazione delle persone o i controlli alle frontiere oppure per assicurare la corretta applicazione delle norme in materia di asilo. Tra queste, vanno menzionate una banca dati già operativa, qual è Eurodac, e una banca dati in costruzione, quale il sistema di informazione visti (VIS).

Sotto il profilo della collocazione nel sistema istituzionale, i primi due sistemi informativi si situano in tutto e per tutto nel "terzo pilastro", mentre i secondi si trovano a cavallo tra il primo e il terzo pilastro, tanto che è stata per essi adottata la tecnica del "doppio binario"[1]. L'Eurodac e il VIS, invece, possono essere qualificati come sistemi di "primo pilastro". È ben vero che la distinzione tra i pilastri è già in via di superamento ed è destinata a essere superata completamente con l'entrata in vigore del Trattato di Lisbona[2], ma essa non può comunque essere sottovalutata, viste le differenze tuttora esistenti sul terreno dei processi decisionali, delle garanzie di protezione dei dati e dell'accesso alla Corte di giustizia.

Di più: nel caso specifico, la separazione tra i pilastri dovrebbe consentire di marcare una differenza assai più importante, che andrà tenuta ferma anche dopo il superamento dell'attuale architettura istituzionale dell'Unione. Si tratta della distinzione tra le tematiche relative alla cooperazione di polizia e giudiziaria in materia penale, da un lato, e quelle relative all'immigrazione, all'asilo e alla libertà di circolazione, dall'altro[3].

---

1 Cfr. *supra*, F. Decli - G. Marando, "Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia", § 2.

2 Sul ruolo della Corte di giustizia nel superamento dei pilastri, cfr. E. Sanfrutos Cano, "The Third Pillar and the Court of Justice: A 'Praetorian Communitarization' of Police and Judicial Cooperation in Criminal Matters?", in *Security versus Justice? Police and Judicial Cooperation in the European Union*, a cura di E. Guild e F. Geyer, Ashgate, Aldershot, 2008, pp. 51 sgg. Sulle prospettive future, tra i tanti, B. Carrera - F. Geyer, "The Reform Treaty and Justice and Home Affairs – Implications for the *common* Area of Freedom, Security and Justice", in *Security versus Justice?*, cit., pp. 289 sgg.; F. Clementi, "Lo spazio di libertà, sicurezza e giustizia", in *Le nuove istituzioni europee. Commento al Trattato di Lisbona*, a cura di F. Bassanini e G. Tiberi, Bologna, il Mulino, 2008, pp. 185 sgg.; S. Peers, *EU Criminal Law and the Treaty of Lisbon*, in "European Law Review", 2008, p. 507.

3 Sulla necessaria distinzione tra questi *issues* insiste F. Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, <http://www.libertysecurity.org/IMG/pdf__Databases__and__Systems__of__Information__Exchange__in__the__Area__of__Freedom__Security__and__Justice.pdf>, p. 4.

Com'è noto, si registra una tendenza a sfumare i confini tra questi ambiti. Una tendenza giustificata dall'esigenza di promuovere la sicurezza, che ha via via assunto un ruolo predominante nella stessa agenda politica dell'Unione europea, sia per ragioni "strutturali", che per ragioni contingenti[4]. In particolare dopo gli attentati terroristici di New York, Madrid e Londra, l'Unione europea si è preoccupata soprattutto di implementare la sicurezza, ponendo in secondo piano i valori concorrenti della libertà e giustizia[5]. Nel rafforzamento della sicurezza, un ruolo fondamentale ha assunto proprio lo scambio di informazioni: non a caso, il Programma dell'Aia ha riconosciuto che il rafforzamento della libertà, della sicurezza e della giustizia passa soprattutto attraverso «un approccio innovativo nei confronti dello scambio transfrontaliero di informazioni in materia di applicazione della legge»[6]. A tal fine, il Consiglio europeo ha individuato tre direttrici fondamentali.

Anzitutto, nella parte dedicata al rafforzamento della sicurezza, il Consiglio europeo ha coniato espressamente il canone di disponibilità, per garantire un'efficace circolazione "orizzontale" delle sole *law enforcement informations*[7].

In secondo luogo, ha posto le basi per il riconoscimento di quello che si è definito "principio di accessibilità", che si affianca al canone di disponibilità. Se quest'ultimo si riferisce espressamente allo scambio tra autorità di *law enforcement*, il canone di accessibilità va inteso come quello in forza del quale le stesse autorità nazionali e quelle europee (in particolare Europol ed Eurojust) debbono, entro certi limiti, poter accedere alle informazioni rilevanti per l'applicazione della legge contenute nei sistemi di informazione europei. Nel Programma dell'Aia siffatta prospettiva è ancora solo abbozzata: nella parte relativa al rafforzamento della sicurezza, infatti, si auspica l'«accesso diretto (on-line), anche per l'Europol, alle basi di dati centrali dell'UE già esistenti quali il SIS».

---

4 Cfr. *supra*, M. Gialuz, "La cooperazione informativa quale motore del sistema europeo di sicurezza", § 1.

5 Secondo D. Bigo, "EU Police Cooperation: National Sovereignity Framed by European Security", in *Security versus Justice?*, cit., p. 93, «the development of the European Union in the area of freedom, security and justice can be seen as a pilgrimage from one European city to another, with different 'stations' in which devoted civil servants execute rituals in the name of a new god: security». Sulla priorità che la sicurezza ha assunto rispetto alla libertà nel Programma dell'Aia, cfr. T. Balzacq - S. Carrera, "The Hague Programme: the Long Road to Freedom, Security and Justice", in *Security Versus Freedom? A Challenge for Europe's Future*, a cura di T. Balzacq e S. Carrera, Ashgate, Aldershot, 2006, p. 18; D. Bigo, "Liberty, whose Liberty? The Hague Programme and the Conception of Freedom", *ivi*, pp. 36 sgg., il quale peraltro ritiene che la ridefinizione dello stesso concetto di libertà come «tool for maximising security» abbia radici più risalenti rispetto alla recrudescenza del terrorismo internazionale degli inizi del 2000.

6 Testualmente, *Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea*, in *GUUE*, C 53, 3 marzo 2005, p. 7.

7 Cfr. *supra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea", § 2.

Infine, nella sezione dedicata alla gestione dei flussi migratori, il Consiglio europeo ha tratteggiato la prospettiva dell'interoperabilità tra i diversi sistemi informativi europei di larga scala, già esistenti o in via di costituzione[8]. Invero, ha incaricato il Consiglio «di valutare la possibilità di massimizzare l'efficacia e l'interoperabilità dei sistemi d'informazione dell'UE nella lotta contro l'immigrazione clandestina e di migliorare i controlli alle frontiere e la gestione di tali sistemi, sulla scorta di una comunicazione della Commissione sull'interoperabilità tra il Sistema d'informazione Schengen (SIS II), il Sistema d'informazione visti (VIS) ed EURODAC»[9].

Queste prospettive sono state ulteriormente specificate in atti successivi delle istituzioni dell'Unione, soprattutto nell'ottica della lotta al terrorismo internazionale. Significativa, in tal senso, appare la dichiarazione del Consiglio europeo sul terrorismo del 25 marzo 2004, nella quale si auspicava la realizzazione di «sinergie fra i sistemi d'informazione attuali e futuri (SIS II, VIS ed EURODAC) per sfruttarne il valore aggiunto, nel rispettivo ambito giuridico e tecnico, ai fini della prevenzione e del contrasto del terrorismo»[10]. Assai simile il senso della dichiarazione del Consiglio GAI resa all'indomani degli attentati terroristici di Londra, nella quale si enunciava l'intenzione del Consiglio di sviluppare «sistemi d'informazione più validi e flessibili ai fini della protezione delle nostre frontiere esterne e della nostra sicurezza interna»[11].

A un anno di distanza dall'adozione del Programma dell'Aia, la Commissione ha presentato al Consiglio e al Parlamento europeo una comunicazione concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni (COM(2005)597 def.)[12]. In tale importante documento di carattere politico e stra-

---

8 Sull'importanza di tenere distinti il principio di disponibilità («focussed on the exchange of available information between different National authorities and agencies for law enforcement purposes only») rispetto all'interoperabilità dei sistemi informativi (che si riferisce all'«effective interlinking of different databases»), cfr. E. Brouwer, "Data Surveillance and Border Control in the EU: Balancing Efficiency and Legal Protection", in *Security Versus Freedom?*, cit., pp. 137-138.

9 Così, *Programma dell'Aia*, cit., p. 7.

10 Cfr. la *Dichiarazione del Consiglio dell'Unione europea sulla lotta al terrorismo. Documento del Consiglio n. 79/06*, 29 marzo 2004, <http://register.consilium.europa.eu/pdf/it/04/st07/st07906.it04.pdf>, p. 8.

11 Cfr. la *Dichiarazione del Consiglio sulla risposta dell'UE agli attentati di Londra*, in *Documento del Consiglio n. 11158/05*, 13 luglio 2005, <http://register.consilium.europa.eu/pdf/it/05/st11/st11158.it05.pdf>, p. 3.

12 Il documento è pubblicato in <http://register.consilium.europa.eu/pdf/it/05/st15/st15122.it05.pdf>. Sui pericoli per il diritto all'autodeterminazione informativa che potrebbero derivare dall'interoperabilità tra i diversi sistemi informativi, cfr. V. Mitsilegas, "Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance", in *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, a cura di A. Baldaccini, E. Guild, H. Toner, Oxford e Portland, Hart Publishing, 2007, p. 391, il quale pone in rilievo soprattutto il profilo legato all'elusione del canone di finalità limitata.

tegico – volto a illustrare come i sistemi informatici nel settore della giustizia e affari interni, «al di là della loro attuale finalità, possano sostenere efficacemente le politiche connesse alla libera circolazione delle persone e servire nella lotta contro il terrorismo e le forme gravi di criminalità» –, la Commissione fornisce una definizione dell'interoperabilità quale «concetto tecnico più che giuridico o politico»: essa va intesa come la «capacità dei sistemi informatici, e dei processi operativi da questi supportati, di scambiare dati e di condividere informazioni e conoscenze».

Siffatta impostazione lascia perplessi. Anzitutto, è stato giustamente rilevato che l'interoperabilità non può essere un problema meramente tecnico[13]: al di là del fatto che gli sviluppi tecnologici non sono mai in sé neutrali dal punto di vista politico, non lo può essere a maggior ragione la scelta di collegare archivi informatici per ragioni di *law enforcement*[14]. È evidente, infatti, che la possibilità di scambiare dati inseriti in archivi diversi genera il rischio di un'elusione dei principi fondamentali in materia di protezione dei dati e, in particolare, del canone di finalità limitata[15]: la separazione tra le banche dati e l'utilizzo di standard tecnologici differenti è uno degli strumenti più efficaci per garantire il rispetto del canone di finalità limitata e impedire la «funzione di scorrimento» (*function creep*)[16]. Pertanto, lo stesso Parlamento europeo ha auspicato un dibattito politico sullo sviluppo dell'interoperabilità e ha collegato la tematica dell'interoperabilità a quella dell'adozione di una rigorosa normativa in materia di tutela dei dati nel "terzo pilastro"[17].

In secondo luogo, la nozione tecnica di interoperabilità è assai generica e finisce per ricomprendere potenzialmente, sia quella prospettiva che si è definita come accessibilità, sia una prospettiva di interazione tra i grandi sistemi informativi (ossia quella che sembrava essere il cuore della direttiva contenuta nel Programma dell'Aia), sia un'ipotetica prospettiva più stringente, quale potrebbe essere quella dell'interconnessione tra diverse banche dati.

---

13 Cfr. V. Mitsilegas, "Databases in the area of freedom, security and justice: Lessons for the centralisation of records and their maximum exchange", in *Towards a European Criminal Record*, a cura di C. Stefanou ed H. Xanthaki, Cambridge, Cambridge University Press, 2008, p. 324.

14 P. De Hert - S. Gutwirth, *Interoperability of police databases within the EU: an accountable political choice?*, <http://papers.ssrn.com/sol3/papers.cfm?abstract__id=971855>, pp. 3, 10.

15 V. *Comments on the Communication of the Commission on interoperability of European databases*, 10 marzo 2006, <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2006/06-03-10__Interoperability__EN.pdf>, p. 3.

16 V. *Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM (2004) 835 def.)*, in *GUUE*, C 181, 23 luglio 2005, p. 27.

17 Cfr. *Raccomandazione del Parlamento europeo destinata al Consiglio su interoperabilità e sinergie tra banche dati europee nel settore giustizia e affari interni, B6-0336/2006*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B6-2006-0336+0+DOC+PDF+V0//IT>, p. 2.

In realtà, nel documento viene sviluppato soprattutto il profilo legato al canone di accessibilità, in quanto viene riconosciuto come un limite proprio l'impossibilità per le autorità incaricate dell'applicazione della legge di accedere al VIS, ai dati relativi all'immigrazione contenuti nel SIS II e ai dati conservati nell'Eurodac[18]. In tal senso, la Commissione ha auspicato l'estensione dell'accesso a tali sistemi di informazione per finalità di *law enforcement*. Ciò che si spiega anche perché già oggi Eurodac contiene e, in prospettiva, SIS II e VIS conterranno dati biometrici, che possono risultare assai utili per l'identificazione degli autori di reati gravi[19]. Da questo punto di vista, nella parte dedicata al miglioramento dell'efficienza dei sistemi esistenti, la Commissione ha insistito soprattutto sulla possibilità di effettuare interrogazioni con parametri biometrici, come previsto per Eurodac e VIS, ma non per il SIS di seconda generazione[20].

Per quel che riguarda le possibili interazioni tra tali sistemi, la Commissione ha prospettato l'opportunità di garantire un accesso più ampio delle autorità competenti in materia di asilo e di immigrazione ai dati contenuti in Eurodac, VIS e SIS II; ha poi insistito soprattutto sulla necessità di razionalizzare l'architettura dei sistemi – introducendo la possibilità di condividere alcune funzioni, come la componente AFIS del VIS per interrogazioni sulla base di parametri biometrici – e l'assetto organizzativo, accentrando la gestione dei sistemi in un'unica autorità.

Ora, considerato che il SIS II è stato oggetto di approfondimento in altro contributo di questo volume[21], merita svolgere una breve analisi delle due principali banche dati di "primo pilastro", per verificare, in primo luogo, se e in quale misura esse abbiano anche finalità di sicurezza e, in secondo luogo, se e in quale misura i propositi relativi all'accessibilità fissati dal documento del 2005 abbiano trovato effettivamente attuazione.

---

18 Su tale approccio non può non influire l'idea che vi sia una «close association between the movement of third country nationals to and within the European Union (EU) and criminality and law enforcement»: a tale riguardo, R. Cholewinski, "The Criminalisation of Migration in EU Law and Policy", in *Whose Freedom, Security and Justice?*, cit., pp. 301, 315.

19 Sulla biometria quale «key element of new EU policies aimed at increasing safety, interoperability, availability and efficient border control», cfr., per tutti, A. Sprokkereef, "Data Protection and the Use of Biometric Data in the EU", in *The Future of Identity in the Information Society*, Boston, Publisher Springer, 2008, p. 277.

20 In effetti, la decisione 2007/533/GAI (pubblicata in *GUUE*, L 205, 7 agosto 2007, p. 63) ha disatteso l'auspicio espresso dalla Commissione e ha confermato l'impostazione iniziale volta a consentire l'utilizzo del dato biometrico solo per confermare l'identificazione: al riguardo, si legga V. Christou, *Legislative development: the Council Decision of 12 june 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, in "Columbia Journal of European Law", 2008, p. 654.

21 Cfr. *supra*, F. Decli - G. Marando, *op. cit.*, § 2.

Eurodac (acronimo di "*Euro*pean *dac*tylographic system") è il primo sistema di identificazione delle impronte digitali costituito in ambito comunitario[22]. È stato previsto dal regolamento (CE) n. 2725/2000[23], con lo scopo specifico di concorrere alla determinazione dello Stato membro competente, ai sensi della convenzione di Dublino e del successivo regolamento (CE) n. 343/2003[24], per l'esame di una domanda di asilo presentata in uno Stato membro e di facilitare l'applicazione di tale disciplina. Questa, infatti, richiede che si determini l'identità dei richiedenti asilo e delle persone fermate in relazione all'attraversamento irregolare delle frontiere esterne della Comunità. Siccome si tratta di soggetti spesso privi di documento di identità, il legislatore comunitario ha ritenuto di istituire un apposito sistema in grado di immagazzinare e confrontare i dati biometrici di tali persone.

Secondo il regolamento (CE) 2725/2000, peraltro, la banca dati di Eurodac non comprende solo le informazioni relative alle impronte digitali di ogni richiedente asilo di età non inferiore ai quattordici anni (artt. 4 e 5 regolamento (CE) n. 2725/2000: si parla di "operazioni di categoria 1"). Accanto a questi, vengono inseriti anche i dati relativi agli immigrati illegali[25]. Infatti, vengono acquisite le impronte agli «stranieri di età non inferiore a quattordici anni, che siano fermati dalle competenti autorità di controllo in relazione all'attraversamento irregolare via terra, mare o aria della propria frontiera in provenienza da un paese terzo e che non siano stati respinti» (art. 8: "operazioni di categoria 2"). E, ancora, possono essere trasmessi all'unità centrale i dati relativi alle impronte digitali di

---

22 Su tale sistema informativo, che, nonostante la sua grande rilevanza, non è stato oggetto di particolare attenzione da parte della dottrina, si leggano J.P. Aus, *Supranational Governance in an "Area of Freedom, Security and Justice": Eurodac and the Politics of Biometric Control*, University of Sussex, Working Paper n. 72, <http://www.sussex.ac.uk/sei/documents/wp72.pdf>; Id., *Eurodac: A Solution Looking for a Problem?*, in "European Integration online Papers", 2006, <http://eiop.or.at/eiop/texte/2006-006a.htm>; E.R. Brouwer, *Eurodac: Its Limitations and Temptations*, in "European Journal of Migration and Law", 2002, p. 231; Ead., *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*, Leiden Boston, Martinus Nijhoff Publishers, 2008, pp. 118 sgg.; G. Calesini, *Diritto europeo di polizia*, Roma, Laurus Robuffo, 2007, pp. 111 sgg.; O. Ferguson Sidorenko, *The Common European Asylum System*, The Hague, T.M.C. Asser Press, 2007, p. 57; E. Guild, "The Bitter Fruits of a Common Asylum Policy", in *Security Versus Freedom?*, cit., pp. 66 sgg.; P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffré, 2002, pp. 314 sgg.; S. Peers, *Key Legislative Developments on Migration in the European Union*, in "European Journal of Migration and Law", 2001, p. 231; I. van der Ploeg, *The illegal body: 'Eurodac' and the politics of biometric identification*, in "Ethics and Information Technology", 1999, p. 37.

23 In *GUCE*, L 316, 15 dicembre 2000, p. 1. La disciplina di dettaglio dell'Eurodac è posta dal Regolamento (CE) n. 407/2002 (in *GUCE*, L 62, 5 marzo 2002, p. 1).

24 In *GUUE*, L 50, 25 febbraio 2003, p. 1.

25 Sull'estensione del sistema Eurodac all'immigrazione illegale, si legga E.R. Brouwer, *Digital borders and real rights*, cit., pp. 123 sg.

«stranieri illegalmente presenti in uno Stato membro» esclusivamente al fine di accertare la previa presentazione di una domanda d'asilo in altro Stato membro (art. 11: "operazioni di categoria 3").

Per le prime due categorie di soggetti vengono registrati: lo Stato membro d'origine, luogo e data del fermo; i dati relativi alle impronte digitali; il sesso; il numero di riferimento assegnato dallo Stato membro d'origine; la data di rilevamento delle impronte digitali e la data della trasmissione dei dati all'unità centrale (art. 8, par. 2); nonché, solo per i richiedenti asilo, anche la data di inserimento dei dati nella banca dati centrale e i particolari relativi ai destinatari ai quali sono stati trasmessi i dati e data/date della/delle trasmissioni (art. 5). Non vengono, invece, inserite le informazioni relative al nome e alla nazionalità dei soggetti, al fine evidente di escludere alla radice i possibili abusi del *database*[26]. Inoltre, per quel che riguarda i dati relativi ai soggetti che hanno irregolarmente attraversato i confini, si prevede espressamente che possano essere conservati «all'unico scopo di confrontarli con i dati relativi ai richiedenti asilo trasmessi successivamente alla stessa unità centrale» (art. 9, par. 1). Per gli stranieri illegalmente presenti in uno Stato membro, invece, si esclude alla radice la possibilità di registrazione nella banca dati delle impronte digitali (art. 11, par. 3): le impronte possono essere trasmesse all'unità centrale «esclusivamente ai fini del confronto con i dati sulle impronte digitali dei richiedenti asilo trasmessi da altri Stati membri e già registrati nella banca dati centrale».

Vi sono pertanto significative garanzie a tutela del rispetto del canone di finalità limitata. Ciò nondimeno, è stato rilevato che Eurodac, proprio in quanto contiene informazioni relative agli stranieri che abbiano attraversato irregolarmente le frontiere dell'Unione, «*de facto* also functions as a – potentially deterring – instrument of immigration control and for the maintenance of 'law and order' within the *AFSJ*»[27].

Il sistema Eurodac è entrato in funzione a partire dal gennaio 2003 in tutti gli Stati membri (esclusa la Danimarca), in Norvegia e in Islanda[28]. Nel maggio 2004, i dieci nuovi Stati membri si sono aggiunti al gruppo iniziale, seguiti dalla Danimarca e, successivamente, da Romania e Bulgaria. In seguito, sono stati siglati accordi con la Svizzera e il Liechtenstein al fine di consentire a tali paesi di utilizzare il sistema.

Esso comprende un'unità centrale, che opera presso la Commissione e gestisce un archivio centrale informatizzato di dati sulle impronte digitali, nonché

---

26 In tal senso, E. Guild, *op. cit.*, p. 66.

27 Così, in termini critici, J.P. Aus, *Supranational Governance*, cit., p. 12.

28 Va segnalato, peraltro, che successivamente questi Paesi hanno accettato la disciplina posta dal regolamento c.d. Dublino II e dal regolamento Eurodac e così oggi vengono trattati allo stesso modo degli Stati membri (cfr. A. Nicol, "From Dublin Convention to Dublin Regulation: a Progressive Move?", in *Whose Freedom, Security and Justice?*, cit., p. 274).

l'infrastruttura telematica necessaria per le trasmissioni tra gli Stati membri e la banca dati centrale[29].

Per quel che concerne il profilo relativo alla protezione dei dati trattati nell'ambito di Eurodac, occorre rilevare, da un lato, come si applichi la disciplina generale posta dalla direttiva 95/46/CE[30], e, dall'altro, come il regolamento (CE) n. 2725/2000 ponga una disciplina speciale agli artt. 15 ss. In estrema sintesi, sul piano oggettivo, il regolamento riafferma chiaramente i canoni di legalità e finalità limitata (artt. 1, 13, par. 1, lett. e, par. 4) e prevede alcune restrizioni sull'accesso ai dati registrati nell'Eurodac: l'art. 15 del regolamento stabilisce, anzitutto, che ciascuno Stato membro può accedere soltanto ai dati da esso trasmessi – ad eccezione di quelli relativi alla presenza di precedenti domande di asilo – e, in secondo luogo, che le autorità degli Stati membri che hanno accesso ai dati registrati nella banca dati centrale sono designate da ciascuno Stato membro e vengono comunicate alla Commissione. Sono inoltre previsti precisi termini di conservazione – pari a dieci anni per i richiedenti asilo (art. 6) e a due anni per gli stranieri fermati in relazione all'attraversamento irregolare di una frontiera esterna (art. 10, par. 1) –, nonché la cancellazione anticipata dopo il conseguimento della cittadinanza (art. 7) oppure a seguito del rilascio di permesso di soggiorno o dell'abbandono del territorio dello Stato (art. 10, par. 2). Sul piano soggettivo, il regolamento riconosce alle persone interessate il diritto a essere informate sul responsabile del trattamento e sulle finalità dello stesso (art. 18, par. 1), nonché i diritti di chiedere la rettifica e la cancellazione dei dati (art. 18, par. 2 e 3).

Al fine di garantire l'effettività di tali garanzie, il regolamento aveva previsto che il controllo su Eurodac venisse svolto inizialmente da un'autorità comune di controllo, alla quale è subentrato nel 2004 il Garante europeo per la protezione dei dati personali. Questi è competente per il monitoraggio delle attività svolte dall'autorità centrale, mentre per quel che riguarda il livello nazionale la supervisione è affidata alle autorità nazionali. I due livelli operano in stretta collaborazione, tanto che è stato costituito un *Eurodac Supervision Coordination Group*, formato da rappresentanti delle autorità nazionali e del Garante europeo, il quale ha pubblicato una prima relazione sull'attività di supervisione nel 2007[31].

Sul piano operativo, si è notato come il sistema abbia funzionato in modo ambivalente. Nel periodo 2003-2005, infatti, sono stati trasmessi con successo i dati

---

29 Evidentemente, la banca dati centrale è equipaggiata con un sistema AFIS (*Automated Fingerprint Information System*), che consente di effettuare il confronto dei dati inviati dagli Stati membri con quelli già inviati da altri Stati e memorizzati nella banca dati. Quanto al collegamento tra la banca dati centrale e quelle periferiche, esso è garantito dall'infrastruttura TESTA (*Trans-European Services for Telematics between Administrations*).

30 In *GUCE*, L 281, 23 novembre 1995, p. 31.

31 Si tratta di *EURODAC Supervision Coordination Group. Report of the first coordinated inspection*, <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/07-07-17__Eurodac__report__EN.pdf>.

relativi a 657.753 richiedenti asilo e sono stati registrati nella banca dati centrale i dati relativi a 48.657 cittadini di paesi terzi fermati mentre attraversavano clandestinamente una frontiera esterna. Nello stesso arco temporale, sono stati registrati i dati relativi a 101.884 cittadini di paesi terzi in posizione irregolare nel territorio di uno Stato membro[32]. Nei due anni successivi, sono aumentate significativamente le registrazioni con riguardo ai richiedenti asilo e ai soggetti fermati in occasione dell'attraversamento dei confini esterni[33]

Peraltro, la Commissione ha registrato che il dato relativo agli stranieri entrati illegalmente nel territorio dell'Unione, pur aumentando di anno in anno – ciò che dimostra il crescente interesse degli Stati membri per questo tipo di controllo – è ancora assai basso, se si considera la forte pressione migratoria irregolare alle frontiere esterne dell'Unione europea. Per altro verso, la Commissione ha rilevato come gli Stati membri siano chiaramente interessati a usare i dati relativi ai cittadini di paesi terzi in posizione irregolare nel loro territorio: su questa base, anche considerando l'utilità dei dati relativi agli stranieri irregolari ai fini dell'applicazione del sistema di Dublino, la Commissione ha espresso la volontà di proporne la conservazione, come avviene per i dati relativi agli stranieri che attraversano illegalmente una frontiera, per un periodo iniziale di due anni[34].

Significativi profili problematici si sono riscontrati proprio con riferimento alla tutela dei dati personali. Anzitutto, è la stessa Commissione ad aver verificato le difficoltà per quanto riguarda l'obbligo di cancellare alcuni dati (articoli 7 e 10, paragrafo 2 del regolamento Eurodac), per esempio nei casi in cui un richiedente asilo ottenga la cittadinanza. Per ammissione della stessa Commissione, «la cancellazione non è effettuata sistematicamente, soprattutto perché lo Stato membro che ha inserito i dati non è informato della nuova posizione dell'interessato»[35].

Ancor più rilevante, nella nostra ottica, è il secondo risvolto problematico segnalato dall'*Eurodac Supervision Coordination Group*, in relazione alle autorità che gestiscono l'unità nazionale Eurodac. L'ispezione di questa autorità è stata motivata proprio con il fatto che, nonostante la normativa Eurodac preveda l'uso dei dati ai soli fini del diritto d'asilo, «in some Member States, the national unit is operated by police forces, which may raise some questions as to a strict use limita-

---

32 I dati si rinvengono nella *Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione del sistema di Dublino (COM (2007) 299 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0299:FIN:IT:PDF>, p. 5. Secondo S. Peers, *EU Justice and Home Affairs Law*, Oxford, Oxford University Press, 2006², p. 324, la pratica ha confermato le perplessità manifestate al momento dell'istituzione dell'Eurodac «about the willingness of border officials to take fingerprints of all persons who cross the border irregularly».

33 Cfr. *Communication from the Commission to the European Parliament and the Council. Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007*, <http://www.statewatch.org/news/2009/jan/eu-com-eurodac-annual-report.pdf>, p. 5.

34 Cfr., ancora, *Relazione della Commissione*, cit., p. 11.

35 Testualmente, *Relazione della Commissione*, cit., p. 10.

tion of the system. In others, there seems to be a very strict limitation of the use of category 3 searches about undocumented aliens, for fear of abuse by law enforcement or immigration services»[36]. Sebbene il gruppo non abbia accertato abusi e abbia riscontrato la predisposizione di specifiche garanzie a tutela del canone di finalità limitata, residuano non poche perplessità sull'effettivo rispetto del divieto di utilizzare i dati trattati dall'Eurodac per finalità di *law enforcement*[37].

D'altra parte, come si è notato, nella comunicazione relativa all'interoperabilità delle banche dati, la Commissione aveva rimarcato l'utilità delle informazioni contenute nei sistemi informativi di "primo pilastro". Con riferimento a Eurodac, in particolare, aveva sostenuto che «è possibile che le informazioni biometriche contenute in tale sistema siano le sole disponibili per l'identificazione di una persona sospettata di aver commesso un reato o un atto di terrorismo, qualora questa sia stata registrata come richiedente d'asilo, ma non figuri in nessun'altra banca dati o vi sia registrata solo con dati alfanumerici non esatti (nel caso, ad esempio, abbia fornito un'identità falsa o usato documenti contraffatti)»; proprio con riguardo a tali evenienze, la Commissione aveva prospettato la possibilità di sviluppi della disciplina di Eurodac volti a consentire alle autorità incaricate della sicurezza interna di «accedere a Eurodac in casi ben definiti, qualora vi sia il fondato sospetto che l'autore di un reato grave abbia presentato domanda d'asilo»[38].

Successivamente, il Consiglio ha invitato la Commissione a presentare una proposta intesa a modificare il regolamento (CE) n. 2725/2000 proprio al fine di attuare il canone di accessibilità, consentendo «ai servizi di polizia e di contrasto degli Stati membri e all'Europol di avere accesso a determinate condizioni all'Eurodac a fini di consultazione nel quadro dell'esercizio delle loro competenze nel settore della prevenzione, dell'individuazione e dell'investigazione di reati

---

36 Così, *EURODAC Supervision Coordination Group. Report*, cit., p. 12. D'altra parte, si è notato che, «from the start, the police had a vested interest in using such a database beyond the area of asylum» (così, H. Busch, *The dream of total data collection - status quo and future plans for EU information systems*, <http://www.statewatch.org/analyses/no-61-eu-databases.pdf>, p. 3).

37 Cfr. l'Interrogazione scritta P-1344/03 di Charles Tannock al Consiglio, nella quale si richiedeva al Consiglio di «indicare se dispone di informazioni sullo status di immigrati degli attentatori di Madrid o su loro eventuali spostamenti verso altri Stati membri», di «far sapere se in futuro i dati Eurodac saranno messi a disposizione di Europol, del coordinatore antiterrorismo presso il Consiglio, signor Gijs de Vries, o delle autorità di sicurezza e di polizia degli Stati membri, dietro loro richiesta, ai fini della lotta contro il terrorismo»; si legga anche la risposta del commissario Vitorino (<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2004-1744+0+DOC+XML+V0//IT&language=IT>) e del Segretariato generale del Consiglio (*Documento del Consiglio n. 12697/04*, 23 settembre 2004, <http://register.consilium.europa.eu/pdf/it/04/st12/st12697.it04.pdf>, p. 3).

38 Così, la *Comunicazione della Commissione al Consiglio e al Parlamento europeo*, cit., p. 9. In precedenza, è significativa la proposta di utilizzare i dati inseriti nell'Eurodac per fini di polizia, avanzata dalla delegazione tedesca al Consiglio "Giustizia e affari interni" del 27 settembre 2001 (*Documento del Consiglio n. 13176/01*, 24 ottobre 2001, < http://register.consilium.europa.eu/pdf/it/01/st13/13176i1.pdf>, p. 2).

terroristici e di altri reati gravi»[39]. Tale sollecitazione non sembra peraltro essere stata ancora recepita dalla Commissione: questa ha avviato una consultazione sull'opportunità di operare una tale riforma, ma sembra aver ottenuto reazioni negative[40]. Ad ogni modo, la Commissione ha nel frattempo elaborato un progetto vòlto alla modifica del regolamento che disciplina l'Eurodac[41].

Si tratta di una proposta che si inserisce in un pacchetto di iniziative intese a garantire un livello superiore di armonizzazione e norme migliori di protezione nel contesto del sistema europeo comune di asilo. In questo quadro, il progetto è diretto specificamente a migliorare il funzionamento di Eurodac, ma non contempla l'ampliamento del campo di applicazione della banca dati, né l'estensione dell'accesso alle autorità di *law enforcement*. Da un lato, prevede l'affidamento dell'Eurodac a un'autorità di gestione, che è la medesima fissata dal regolamento SIS II e dal regolamento VIS (art. 4, par. 7). Dall'altro, il progetto apporta alcune modifiche al regolamento proprio in risposta alle preoccupazioni connesse alla protezione dei dati, in ordine all'individuazione della specifica unità responsabile a livello nazionale, alla precisazione della misura in cui il suo operato è connesso alle finalità dell'Eurodac e alla migliore definizione delle diverse fasi di gestione della banca dati (Commissione, Autorità di gestione, sistema centrale)[42]. In prospettiva futura, invece, si prevede che il sistema di confronto biometrico (BMS) sia condiviso tra SIS II, VIS e Eurodac[43].

---

39 Testualmente, il *Progetto di conclusioni del Consiglio sull'accesso dei servizi di polizia e di contrasto degli Stati membri e dell'Europol all'Eurodac. Documento del Consiglio n. 10002/07*, 25 maggio 2007, <http://register.consilium.europa.eu/pdf/it/07/st10/st10002.it07.pdf>, p. 3.

40 Cfr. F. Panzetti, "Le politiche di sicurezza interna alla vigilia della comunitarizzazione", in *L'Unione europea e il governo della globalizzazione*, a cura di R. Gualtieri e F. Pastore, Bologna, il Mulino, 2008, p. 263.

41 Si tratta della *Proposta di un regolamento del Parlamento europeo e del Consiglio che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (CE) n. [.../...] [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] (COM(2008)825 def.)*, 3 dicembre 2008, <http://register.consilium.europa.eu/pdf/it/08/st16/st16934.it08.pdf>.

42 Proprio l'attenzione alla protezione dei dati ha portato il Garante europeo a esprimere un'opinione favorevole sulla proposta: cfr. *Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (COM(2008)825)*, <http://www.statewatch.org/news/2009/feb/eu-edps-eurodac-opinion.pdf>, pp. 8-9.

43 Cfr. la *Proposta di un regolamento del Parlamento europeo e del Consiglio che istituisce l'"Eurodac"*, cit., p. 7.

Se Eurodac rappresenta una realtà, il sistema di informazione visti (*Visa Information System* - VIS) è ancora in fase di costruzione. Si tratta di una banca dati che dovrebbe rappresentare un tassello fondamentale della politica comune dell'Unione europea in materia di visti e costituire una delle iniziative chiave per garantire la libera circolazione delle persone in uno spazio di libertà, sicurezza e giustizia (art. 61 TCE). L'idea trova una prima autorevole esplicitazione nel Consiglio europeo di Laeken. Nelle conclusioni, infatti, i Capi di Stato e di Governo invitavano il Consiglio e gli Stati membri ad adottare le disposizioni necessarie per l'attuazione di un sistema comune di identificazione dei visti (punto 42)[44].

Il Consiglio raccolse la sollecitazione e, nel piano globale per la lotta all'immigrazione clandestina e alla tratta degli esseri umani nell'Unione europea, approvato il 28 febbraio 2002, tra le misure e azioni concernenti la politica in materia di visti, inserì proprio la creazione di un sistema europeo di identificazione dei visti (punti da 34 a 40). A tal fine, adottò un documento sugli "Orientamenti per la creazione di un sistema comune di scambio di dati in materia di visti", secondo il quale il VIS doveva essere istituito per rispondere a diversi obiettivi: quello di semplificare la lotta contro la frode, migliorando l'informazione reciproca degli Stati membri (negli uffici consolari e ai valichi di frontiera) in merito alle domande di visto e al relativo trattamento; quello di migliorare la cooperazione consolare e lo scambio di informazioni tra le autorità consolari centrali; quello di agevolare la verifica dell'identità tra il detentore del visto e il titolare dello stesso, sia al posto di controllo della frontiera esterna che in occasione dei controlli dell'immigrazione e di polizia; quello di contribuire a prevenire il "visa shopping" e di agevolare l'applicazione della convenzione di Dublino, sulla determinazione dello Stato competente per l'esame di una domanda di asilo; quello di contribuire all'identificazione e alla documentazione di clandestini privi di documenti e, infine, al «miglioramento della gestione della politica comune in materia di visti, nonché alla sicurezza interna e alla lotta contro il terrorismo»[45]. Il Consiglio invitò, inoltre, la Commissione a preparare uno studio di fattibilità sulla creazione del VIS, indicando alcune direttive circa le caratteristiche del sistema, che avrebbe dovuto ricalcare, quanto a struttura, il SIS[46].

La Commissione, per parte sua, a neanche un anno dalla presentazione dello studio di fattibilità sul VIS, ha avanzato una proposta di decisione del Consiglio che istituisce il Sistema di informazione visti (COM (2004) 99 def.), la quale è

---

44 V. *Conclusioni della Presidenza*, <http://www.consilium.europa.eu/ueDocs/cms__Data/docs/pressData/it/ec/68836.pdf>, p. 13.

45 Così, *Documento del Consiglio n. 9615/02*, 5 giugno 2002, <http://register.consilium.europa.eu/pdf/it/02/st09/09615i2.pdf>, p. 4. Cfr. anche il *Documento del Consiglio n. 6535/04*, 20 febbraio 2004, <http://register.consilium.europa.eu/pdf/it/04/st06/st06535.it04.pdf>, p. 4.

46 V. *Documento del Consiglio n. 9615/02*, cit., p. 6.

stata concepita, sin dall'origine, con un obiettivo limitato: quello di permettere lo sviluppo del VIS tramite il finanziamento comunitario, nella piena consapevolezza che una «proposta esaustiva di atto normativo che istituisce il VIS sarà presentata in una fase successiva»[47].

La proposta è stata approvata dal Consiglio nel giugno del 2004 e la decisione 2004/512/CE ha avviato il processo istitutivo del sistema di informazione visti, fornendo la base giuridica per la sua iscrizione nel bilancio dell'Unione (considerando n. 4)[48]. La decisione ha previsto l'istituzione di un sistema di scambio tra gli Stati membri di informazioni riguardanti i visti, che permette alle autorità nazionali autorizzate di inserire e aggiornare dati relativi ai visti, nonché di consultare tali dati per via elettronica (art. 1, par. 1). Si tratta di un sistema basato su un'architettura centralizzata ed è costituito da un sistema d'informazione centrale (denominato "sistema centrale d'informazione visti" o "CS-VIS"), con un'interfaccia in ciascuno Stato membro (denominata "interfaccia nazionale" o "NI-VIS") e dall'infrastruttura di comunicazione tra il sistema centrale d'informazione visti e le interfacce nazionali (art. 1, par. 2).

Si prevedeva, inoltre, il ricorso alla procedura di «comitologia» per gestire gli sviluppi tecnici del VIS e la presentazione, da parte della Commissione, di una relazione annuale sulla situazione relativa allo sviluppo del sistema di informazione[49].

Al fine di dare esecuzione a tale decisione, la Commissione si è tempestivamente attivata lungo due direttrici parallele.

Da un lato, nel dicembre del 2004 ha presentato una proposta di regolamento concernente il VIS e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM (2004) 835 def.), avente come base giuridica gli artt. 62, par. 2, lett. *b*, punto ii) e 66 TCE, e volta «a definire lo scopo, le funzionalità e le competenze del VIS, a conferire alla Commissione il mandato di istituire e gestire il VIS nonché a stabilire le procedure e le condizioni per lo scambio di dati tra Stati membri in merito alle domande di visto per soggiorni di breve durata, onde agevolare l'esame di tali richieste e le relative decisioni»[50].

---

47 Testualmente, la *Relazione alla proposta di decisione del Consiglio che istituisce il Sistema di informazione visti (VIS)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0099:FIN:IT:PDF>, p. 2, secondo la quale solo «tale atto normativo futuro definirà in particolare il sistema e le sue modalità di funzionamento, ivi comprese le categorie di dati che vi saranno registrate, le finalità ed i criteri di inserimento, le norme relative al contenuto delle schede VIS, i diritti d'accesso delle autorità ai fini di inserimento, aggiornamento e consultazione dei dati, nonché le norme relative alla protezione dei dati di carattere personale ed al relativo controllo».

48 In *GUUE*, L 213, 15 giugno 2004, p. 5.

49 Cfr. l'ultima *Relazione della Commissione al Consiglio e al Parlamento Europeo sullo stato di avanzamento del sistema di informazione visti (VIS) nel 2007 (COM (2008) 714 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0714:FIN:IT:PDF>.

50 Così la *Relazione alla proposta di regolamento concernente il VIS e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM (2004) 835 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0835:FIN:IT:PDF>, p. 2.

Dall'altro lato, la Commissione ha preso atto che lo sviluppo del VIS nell'ambito del settore della sicurezza interna e della lotta al terrorismo richiedeva l'elaborazione di uno specifico strumento giuridico di "terzo pilastro". A più riprese il Consiglio aveva rilevato l'utilità di garantire alle autorità degli Stati membri competenti in materia di sicurezza interna l'accesso al VIS, in quanto i dati relativi ai visti sono necessari all'assolvimento dei loro compiti in relazione alla prevenzione, all'individuazione e all'investigazione dei reati di terrorismo e di altri gravi reati[51]. È così che è nata la Proposta di decisione del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità degli Stati membri competenti in materia di sicurezza interna e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di atti terroristici e di altre gravi forme di criminalità (COM (2005) 600 def.)[52].

Nonostante la differente natura del processo decisionale, i due progetti hanno seguito un *iter* parallelo e, data la stretta correlazione, i lavori sul "pacchetto legislativo VIS" si sono spesso sovrapposti. Dopo che, nel 2005 e nel 2006, il Garante europeo aveva espresso il parere rispettivamente sulla proposta di regolamento[53] e sulla proposta di decisione[54], nel giugno 2007, il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sui due strumenti[55]. È assai significativo notare che le due proposte sono state valutate congiuntamente. Ciò

---

51 Cfr. *Documento del Consiglio n. 6899/05*, 1° marzo 2005, <http://register.consilium.europa.eu/pdf/it/05/st06/st06899.it05.pdf>, p. 3. In termini generali, sull'opportunità di accordare alle autorità di *law enforcement* l'accesso a sistemi di informazione e di identificazione su vasta scala, cfr. *supra*, § 1.

52 Cfr. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0600:FIN:IT:PDF>, p. 2.

53 Cfr. *Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo*, cit., p. 13.

54 V. *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di decisone del Consiglio relativa all'accesso per la consultazione del sistema d'informazione visti (VIS) da parte delle autorità degli Stati membri competenti in materia di sicurezza interna e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di atti terroristici e di altre grave forme di criminalità (COM (2005) 600 def.)*, in *GUUE*, C 97, 25 aprile 2006, p. 6.

55 Cfr. la *Relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM(2004)0835 – C6-0004/2005 – 2004/0287(COD))*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2007-0194+0+DOC+PDF+V0//IT>. I principali gruppi parlamentari si sono espressi positivamente (cfr. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0227+0+DOC+XML+V0//IT>). In termini critici si è espresso il deputato Athanasios Pafilis (GUE/NGL), secondo il quale il VIS, «che legalizza la raccolta, l'elaborazione e lo scambio di dati personali e biometrici su ogni cittadino straniero che richiede un visto per tutti i paesi dell'UE, al quale hanno accesso tutte le autorità istruttorie e i servizi segreti di ciascuno Stato membro, non fa altro che aggiungere un altro anello alla catena che l'UE usa per soffocare i diritti individuali». Con riguardo al Consiglio, cfr. *Documento del Consiglio n. 13607/07*, 9 ottobre 2007, <http://register.consilium.europa.eu/pdf/it/07/st13/st13607.it07.pdf>.

emerge in modo innegabile, sia dai lavori del Consiglio[56], sia da quelli dell'assemblea parlamentare, ove i due progetti sono stati affrontati «come un pacchetto unico, raggiungendo così una sorta di codecisione anche sulla misura relativa al terzo pilastro»[57].

A seguito di un lavoro durato circa tre anni, nella Gazzetta ufficiale del 13 agosto 2008 sono stati dunque pubblicati il regolamento (CE) n. 767/2008, concernente il sistema di informazione visti e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata e la decisione 2008/633/GAI relativa all'accesso per la consultazione al VIS da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi. Il sistema dovrebbe essere operativo a partire dalla fine del 2009.

4. (Segue): il regolamento VIS

Il regolamento (CE) n. 767/2008 (cosiddetto regolamento VIS) disciplina quella che è destinata a divenire «la più ampia banca dati biometrica al mondo», dal momento che «conterrà informazioni relative a circa 20 milioni di richiedenti e conserverà le impronte digitali di 70 milioni di persone alla volta»[58].

Una delle novità più significative è costituita proprio dalla previsione dell'inserimento dei dati biometrici nel VIS. Considerata la delicatezza di tali dati[59], si sono approfonditi i benefici e le controindicazioni della loro raccolta[60], e, infine,

---

56 Cfr. il *Documento del Consiglio n. 8185/07*, 12 aprile 2007, <http://register.consilium.europa.eu/pdf/it/07/st08/st08185.it07.pdf>.

57 Sono le parole di Sarah Ludford, relatore nella Commissione per le libertà civili, la giustizia e gli affari interni, pronunciate nella seduta del 7 giugno 2007 (cfr. <http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20070606&secondRef=ITEM-018&language=IT&ring=A6-2007-0194>). Secondo la relatrice, proprio tale processo decisionale starebbe a dimostrare che «la separazione tra il primo e il terzo pilastro è semplicemente inefficiente e assurda».

58 Così, Sarah Ludford, nell'intervento indicato nella nota precedente. D'altronde, il dato relativo al numero dei richiedenti il visto è riportato nell'importante ricerca effettuata dall'*European Policy Evaluation Consortium* (EPEC), intitolata *Study for the Extended Impact assessment of the Visa Information System. Final Report*, dicembre 2004, <http://ec.europa.eu/justice__home/doc__centre/freetravel/visa/doc/study__eia__epec__en.pdf>, p. 4.

59 Come ha rilevato il Garante europeo per la protezione dei dati, «la biometria non costituisce solo un'altra tecnologia dell'informazione: essa modifica in maniera irrevocabile la relazione tra corpo e identità, in quanto le caratteristiche del corpo umano possono essere 'lette' da una macchina e sottoposte a un successivo trattamento» (*Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo*, cit., p. 19).

60 Cfr., in particolare, *Study for the Extended Impact*, cit., pp. 51 sgg. V. anche il documento prodotto dal *Working Party on the protection of individuals with regard to the processing of personal data* ("Gruppo Articolo 29") (*Opinion No 7/2004 on the inclusion of biometric elements in*

si è deciso di includerli nella banca dati. Tanto che il regolamento prevede la registrazione nel VIS, non solo dei dati alfanumerici sul richiedente e sui visti richiesti, rilasciati, rifiutati, annullati, revocati o prorogati (art. 5, par. 1, lett. *a*, art. 9, parr. 1-4 e artt. 10-14)[61], ma anche della fotografia del richiedente (art. 5, par. 1, lett. *b* e art. 9, par. 5) e delle impronte digitali (art. 5, par. 1, lett. *c* e art. 9, par. 6)[62].

Per quel che riguarda la finalità del VIS, l'art. 2 del regolamento individua anzitutto una finalità "generica", consistente nel «migliorare l'attuazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra le autorità centrali competenti per i visti, agevolando lo scambio di dati tra Stati membri in ordine alle domande di visto e alle relative decisioni». Segnala inoltre diverse finalità "immediate", quali quelle di: agevolare la procedura relativa alla domanda di visto; evitare l'elusione dei criteri di determinazione dello Stato membro competente per l'esame della domanda; agevolare la lotta contro la frode; agevolare i controlli ai valichi di frontiera esterni e all'interno del territorio degli Stati membri; contribuire all'identificazione di qualsiasi persona che non soddisfi o non soddisfi più le condizioni d'ingresso, soggiorno o residenza nel territorio degli Stati membri; agevolare l'applicazione del regolamento (CE) n. 343/2003; contribuire a prevenire minacce alla sicurezza interna degli Stati membri.

Siffatta configurazione ha suscitato qualche perplessità. Il Garante europeo per la protezione dei dati personali aveva, infatti, raccomandato al legislatore europeo di distinguere chiaramente tra finalità del VIS e vantaggi derivanti del sistema. L'unica finalità effettiva avrebbe dovuto essere quella "generica", mentre la prevenzione delle frodi e del «visa shopping» avrebbero dovuto essere configurati come vantaggi. Inoltre, secondo il Garante, si sarebbe dovuto espungere il riferimento esplicito alla prevenzione delle minacce alla sicurezza interna degli Stati membri, che andrebbe considerata come un «vantaggio 'secondario'» (ancorché assai significativo) del sistema informativo[63]. La preoccupazione del

---

residence permits and visas taking account of the establishment of the European information system on visas (VIS), <http://europa.eu.int/comm/justice__home/fsj/privacy/docs/wpdocs/2004/wp96__en.pdf>).

61 Va segnalato che il regolamento prevede che si istituiscano dei collegamenti tra i diversi fascicoli relativi allo stesso soggetto (art. 5, par. 1, lett. d e art. 8, parr. 3-4).

62 Si badi che l'art. 9, par. 6, prevede che l'autorità competente per il rilascio dei visti inserisca le impronte digitali, «conformemente alle pertinenti disposizioni dell'Istruzione consolare comune». Al fine di adeguare l'Istruzione consolare comune alla prevista introduzione di elementi biometrici, la Commissione ha presentato una proposta di regolamento del parlamento europeo e del consiglio (COM (2006) 269 def., <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0269:FIN:IT:PDF>): essa prescrive alle autorità competenti degli Stati membri di rilevare «gli identificatori biometrici del richiedente comprendenti l'immagine del volto e le impronte delle dieci dita, nel rispetto delle norme di garanzia previste dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dalla Convenzione delle Nazioni Unite sui diritti del fanciullo» (art. 1, par. 2).

63 Così, *Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo*, cit., pp. 17, 27.

Garante era evidentemente quella di precisare la natura del VIS, escludendo chiaramente che si tratti di un sistema istituito per finalità di sicurezza: ove si riconosca anche la finalità di sicurezza – per quanto accessoria – argomentava il Garante – sarebbe naturale concedere alle autorità di *law enforcement* un accesso sistematico e generalizzato alla banca dati.

Il rilievo pare del tutto condivisibile. È ben vero che, come si vedrà, nella decisione 2008/633/GAI l'accesso alle autorità di *law enforcement* è stato circondato di significative garanzie; nondimeno, è possibile che il legislatore europeo modifichi in futuro tale bilanciamento e ampli i varchi di accesso al VIS, proprio facendo leva sul fatto che tale sistema è stato istituito *anche* per finalità di sicurezza.

In relazione all'accesso, va rilevato che il regolamento ne contempla uno differenziato (ossia a dati diversi), a seconda dello scopo dello stesso. Vengono disciplinate quattro diverse fattispecie di accesso ai dati: a fini di verifica ai valichi di frontiera esterni (art. 18); a fini di verifica all'interno del territorio degli Stati membri dell'identità del titolare del visto, dell'autenticità del visto o della sussistenza delle condizioni d'ingresso, di soggiorno o di residenza (art. 19); a fini di identificazione delle persone che non soddisfano le condizioni per l'ingresso, il soggiorno o la residenza nel territorio degli Stati (art. 20); per la determinazione della competenza per le domande di asilo (art. 21); per l'esame della domanda di asilo, da parte delle autorità competenti in materia di asilo (art. 22).

Per quanto attiene ai termini di conservazione, il regolamento prevede un periodo massimo di cinque anni, che decorrono dalla data di scadenza del visto, qualora sia stato rilasciato; dalla nuova data di scadenza del visto, qualora un visto sia stato prorogato; dalla data della creazione del fascicolo nel VIS, qualora la domanda sia stata ritirata, chiusa o interrotta; dalla data della decisione delle autorità competenti per i visti, qualora un visto sia stato rifiutato, annullato, ridotto o revocato (art. 23, par. 1). Alla scadenza del termine, si prevede la cancellazione automatica del fascicolo e dei collegamenti fatti verso il medesimo (art. 23, par. 2). È prevista, inoltre, la cancellazione anticipata dei dati, qualora il richiedente abbia acquisito la cittadinanza di uno Stato membro (art. 25). Va segnalato che tale disciplina è stata valutata positivamente, sia dal Garante europeo, che dal Gruppo di lavoro "articolo 29"[64].

La gestione operativa del VIS centrale e delle interfacce nazionali viene affidata – dopo un periodo transitorio – a un organo di gestione (l'Autorità di gestione), che dovrebbe essere il medesimo previsto dall'art. 15 del regolamento (CE) n. 1987/2006. Infatti, nelle dichiarazioni comuni che accompagnano il regolamento SIS II e il regolamento VIS, il Consiglio e il Parlamento europeo hanno con-

---

64 Cfr. rispettivamente *Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo*, cit., p. 22, e *Parere 2/2005 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata*, <http://ec.europa.eu/justice__home/fsj/privacy/docs/wpdocs/2005/wp110__it.pdf>, p. 25.

venuto che la succitata autorità assuma la forma di un'agenzia e hanno invitato la Commissione a compiere una valutazione di impatto[65]. Nello studio eseguito proprio in vista dell'istituzione di tale agenzia, la possibilità che tutti i sistemi informatici su larga scala siano riuniti in un'unica sede, sotto una gestione unica e girino sulla stessa piattaforma viene ritenuta tale da consentire di potenziare la produttività e ridurre i costi operativi nel lungo periodo. La valutazione d'impatto considera pertanto che una nuova agenzia di regolamentazione sia in realtà la migliore opzione per lo svolgimento dei compiti dell'"Autorità di gestione" del SIS II, del VIS e anche – come si è visto[66] – dell'Eurodac[67]. Nel periodo transitorio viene affidata alla Commissione la responsabilità della gestione del VIS.

Per quel che riguarda la tutela dei dati, sotto il profilo oggettivo, il regolamento si preoccupa di garantirne la sicurezza, prescrivendo che ciascuno Stato membro adotti un articolato piano a tal fine (art. 32). Inoltre, esso affida alle autorità di controllo nazionali la verifica del trattamento eseguito a livello locale (art. 41), mentre attribuisce al Garante europeo della protezione dei dati la vigilanza sul trattamento effettuato dall'Autorità di gestione (art. 42).

Sul piano soggettivo, invece, il regolamento VIS riconosce agli interessati il diritto a essere informati, non solo sull'autorità di controllo nazionale competente e sullo scopo del trattamento, ma anche sulle categorie di destinatari dei dati, sul periodo di conservazione e sul diritto di accesso, di rettifica e di cancellazione (art. 37, par. 1)[68]. Viene, infatti, garantito un ampio diritto di accesso, di rettifica e di cancellazione (art. 38): particolarmente significative appaiono le disposizioni che obbligano lo Stato membro che non riconosca l'inesattezza o l'illegittimità dei dati registrati nel VIS, anzitutto, a fornire «senza indugio all'interessato una giustificazione scritta della ragione per cui non intende correggere o cancellare i dati che lo riguardano» (art. 38, par. 5) e, in secondo luogo, a trasmettere le «in-

---

65 V. *Dichiarazione comune del Parlamento europeo, del Consiglio e della Commissione sull'articolo 26 relativo alla gestione operativa*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0227+0+DOC+XML+V0//IT#top>. Sull'unicità delle agenzie, si veda la valutazione espressa dall'allora Vicepresidente della Commissione Franco Frattini nella seduta del Parlamento europeo del 7 giugno 2007 (<http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20070606&secondRef=ITEM-016&language=IT&ring=A6-2007-0194>): «se vi dovrà essere un organismo di gestione operativa, esso non potrà essere limitato solamente a VIS, dovrà essere un unico strumento operativo di gestione di SIS II e di VIS insieme».

66 V. *supra*, § 2.

67 Cfr. la *Relazione alla proposta di un regolamento del Parlamento europeo e del Consiglio che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (CE) n. [.../...] [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] (COM (2008) 825 def.)*, <http://register.consilium.europa.eu/pdf/it/08/st16/st16934.it08.pdf>, p. 4.

68 In tal modo, è stata accolta una raccomandazione del Garante europeo: cfr. *Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo*, cit., p. 25.

formazioni in merito alla procedura da seguire qualora non accetti la giustificazione fornita» (art. 38, par. 6).

5. (Segue): l'accesso al VIS delle autorità di *law enforcement*

Il secondo strumento normativo del "pacchetto VIS" è costituito dalla decisione 2008/633/GAI, volta a disciplinare l'accesso delle autorità di *law enforcement* al sistema di informazione visti.

Come si è notato, essa trae origine dalle posizioni espresse dal Consiglio, il quale, nel marzo del 2005, aveva rilevato la grande utilità dei dati contenuti nel VIS ai fini della prevenzione e repressione del terrorismo e di altri gravi reati, e aveva pertanto invitato la Commissione ad avanzare una proposta basata sul titolo VI del TUE.

La Commissione ha valutato diverse opzioni. Scartata l'ipotesi di non intraprendere alcuna azione[69], ha esaminato l'idea di creare una base giuridica che consentisse un accesso *illimitato* al VIS alle autorità degli Stati membri competenti in materia di sicurezza interna e a Europol. Anche tale soluzione è stata esclusa: la previsione di un accesso diretto e in relazione a qualsiasi reato avrebbe, infatti, trasformato il VIS in una normale banca dati per la lotta contro la criminalità. Ciò che è apparso, da un lato, non conforme con «l'obiettivo fondamentale del sistema VIS originario» e, dall'altro, sproporzionato, in quanto «avrebbe un'incidenza ingiustificata sui diritti fondamentali delle persone i cui dati sono registrati nel VIS, che devono essere presunte innocenti e non essere trattate come sospetti nell'ambito di un'inchiesta penale»[70].

È per queste ragioni che la Commissione ha deciso di proporre una base giuridica che riconosce alle autorità degli Stati membri competenti in materia di sicurezza interna e a Europol soltanto un accesso *limitato* al VIS.

Questo approccio è stato particolarmente apprezzato dal Garante europeo per la protezione dei dati. Nel parere sulla proposta di regolamento, il Garante aveva manifestato una riserva di fondo sulla previsione di un'interoperabilità, ossia di un accesso generalizzato delle autorità di *law enforcement* al VIS, che avrebbe

---

69 La Commissione ha ritenuto che, essendo lo scambio dei dati VIS escluso dall'ambito di applicazione della proposta di decisione quadro del Consiglio sullo scambio di informazioni a norma del principio di disponibilità (posto che questa riguarda la cooperazione di polizia: cfr. *supra*, S. Ciampi, *op. cit.*, § 9), gli Stati membri avrebbero prima o poi rinnovato la richiesta di uno specifico strumento normativo in tale settore (cfr. la *Relazione alla Proposta di decisione del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità degli Stati membri competenti in materia di sicurezza interna e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di atti terroristici e di altre gravi forme di criminalità, (COM (2005) 600 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0600:FIN:IT:PDF>, p. 4).

70 Così, *Relazione alla Proposta di decisione del Consiglio relativa all'accesso*, cit., p. 5.

violato il principio di finalità[71]. Nel successivo parere sulla proposta di decisione, il Garante, ribadito che il VIS è un sistema di informazione sviluppato in vista dell'attuazione della politica europea in materia di visti e non uno strumento per l'applicazione della legge, ha riconosciuto che il bilanciamento tra i diversi valori in gioco – l'attività di prevenzione e repressione dei reati, da un lato, e il diritto alla protezione dei dati, dall'altro – raggiunto nella proposta era «globalmente soddisfacente»[72].

Ulteriore rifinitura di quel bilanciamento è venuta dal Parlamento, che, grazie alla trattazione congiunta dello strumento di terzo e di "primo pilastro", ha potuto giocare un ruolo fondamentale nell'*iter* di approvazione della decisione.

Il carattere "limitato" dell'accesso deriva da una serie articolata di vincoli e garanzie.

Anzitutto, sotto il profilo oggettivo, si deve notare come la disponibilità dei dati contenuti nel VIS non sia estesa all'attività di prevenzione e repressione di qualsiasi reato, ma sia circoscritta a quella relativa a taluni reati. Si tratta dei «reati di terrorismo», individuati mercé il richiamo agli artt. 1-4 della decisione quadro 2002/475/GAI[73], nonché dei «reati gravi», identificati in quelli previsti dall'art. 2, par. 2, della decisione quadro sul mandato d'arresto europeo[74]. La decisione specifica, inoltre, che l'autorità designata può ottenere l'informazione a due condizioni: da un lato, la consultazione deve risultare necessaria in un «caso specifico»[75]; dall'altro, debbono sussistere «fondati motivi per ritenere che la consultazione dei dati VIS contribuisca in misura sostanziale alla prevenzione, all'individuazione o all'investigazione di qualsiasi dei reati in questione»[76]. In

---

71 Cfr. *Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo*, cit., p. 27. Analogamente, E. De Busser, *The architecture of data exchange*, in "International Review of Penal Law", 2007, p. 53.

72 In tal senso, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di decisione del Consiglio relativa all'accesso per la consultazione del sistema d'informazione visti (VIS)*, cit., p. 10.

73 In *GUCE*, L 164, 22 giugno 2002, p. 3. Dopo la sostituzione degli artt. 3 e 4 della decisione quadro 2002/475/GAI, operata dalla decisione quadro 2008/919/GAI (*GUUE*, L 330, 9 dicembre 2008, p. 21), sembra che il richiamo vada inteso alle nuove disposizioni.

74 Si tratta, come noto, della decisione quadro 2002/584/GAI (*GUCE*, L 190, 18 luglio 2002, p. 1).

75 La proposta della Commissione (COM (2005) 600 def.) definiva in modo molto stringente tale presupposto, precisando che un «caso particolare» sussiste «quando l'accesso per la consultazione è connesso a un evento specifico, delimitato geograficamente e cronologicamente, o ad un pericolo imminente associato con attività criminali, ovvero ad una persona specifica relativamente alla quale esistono fondati motivi per ritenere che commetterà reati terroristici o altre gravi forme di criminalità o che ha un vincolo rilevante con una tale persona» (art. 5, par. 1, lett. c). La precisazione è stata successivamente abbandonata.

76 Si noti che l'inciso "in misura sostanziale" è stato inserito accogliendo una precisa richiesta del Garante europeo (cfr. *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di decisione del Consiglio relativa all'accesso per la consultazione del sistema d'informazione visti (VIS)*, cit., p. 10).

parte diversa la disciplina che riguarda l'Europol. Si consente infatti l'accesso, da un canto, quando è necessario per l'adempimento delle sue funzioni ai sensi dell'art. 3, par. 1, punto 2, della convenzione Europol o ai fini di attività specifiche di analisi di cui all'art. 10; dall'altro, «quando è necessario per l'adempimento delle sue funzioni ai sensi dell'art. 3, par. 1, punto 2, della convenzione Europol e per la realizzazione di analisi generali di tipo strategico ai sensi dell'art. 10 della convenzione Europol, a condizione che i dati VIS siano resi anonimi dall'Europol prima di tale trattamento e siano conservati in una forma che non consenta più di identificare la persona interessata» (art. 7).

In secondo luogo, sotto il profilo soggettivo, la decisione riconosce la legittimazione alle sole autorità designate, ossia alle autorità competenti in materia di prevenzione, individuazione e investigazione di reati di terrorismo e altri reati gravi, che siano state designate da ciascuno Stato membro (artt. 2, par. 1, lett. *e*, e 3, par. 1). In seno a tali autorità, vengono individuate le unità operative legittimate all'accesso[77], o meglio, a richiedere i dati al punto di accesso.

È prevista, infatti, una garanzia procedurale per cui l'ingresso nella banca dati non avviene direttamente, ma attraverso uno o più punti di accesso[78]. Le unità operative interessate a un dato contenuto nel sistema debbono presentare una richiesta motivata (scritta o elettronica) al punto di accesso centrale, il quale è chiamato a compiere una verifica preliminare sulla sussistenza effettiva delle condizioni per l'accesso al sistema VIS. Solo se tutte le condizioni di accesso sono soddisfatte, il personale debitamente autorizzato del punto di accesso centrale tratta le richieste e i dati VIS consultati vengono trasmessi all'unità richiedente, con modalità tali da non comprometterne la sicurezza (art. 4, par. 1). In caso eccezionale d'urgenza, però, si prevede che il punto di accesso tratti immediatamente le richieste e verifichi solo a posteriori se tutte le condizioni di cui all'art. 5 sono soddisfatte (art. 4, par. 2)[79].

---

77 L'elenco delle unità operative viene conservato a livello nazionale da ciascuno Stato membro (art. 3, par. 5).

78 Il carattere indiretto dell'accesso è stato difeso dal Parlamento. Nel corso dei lavori preparatori, si è insistito sulla necessità che vi fosse un'autorità diversa da quella richiedente che verifichi in via preliminare la sussistenza delle condizioni di accesso. Ciò, in quanto, ad avviso dei parlamentari, «il VIS è essenzialmente una base di dati del primo pilastro il cui fine principale non è la prevenzione, individuazione e investigazione di reati terroristici e di altre gravi forme di criminalità» (Cfr. il *Documento del Consiglio n. 8185/07*, cit., p. 6). Nella proposta originaria della Commissione era prevista la designazione di un'unica autorità nazionale quale punto di accesso centrale al VIS (art. 4, par. 1), mentre nella versione definitiva della decisione si è preferito consentire agli Stati membri di indicare uno o più punti di accesso centrali (art. 3, par. 3).

79 Anche il Parlamento europeo ha condiviso la previsione di una procedura d'urgenza: cfr. l'intervento dell'on. Sarah Ludford nella seduta del 7 giugno 2007, nel quale ha riconosciuto che «dopo trattative alquanto difficili, gli Stati membri hanno infine riconosciuto che questo sistema non è in prima istanza uno strumento di applicazione della legge e che pertanto qualsiasi accesso da parte dei servizi di polizia o intelligence non può essere diretto e immediato, bensì sarà indiretto, controllato e filtrato attraverso punti di accesso centrali, dove sarà verificata la legittimità di

Infine, va notato che la consultazione avviene in due fasi. Nella prima è consentita la ricerca sulla base di alcuni dati, tra i quali rientrano le generalità del soggetto, le impronte digitali e altri dati relativi (tra gli altri) al tipo di visto, al viaggio o alla residenza (art. 5, par. 2). Solo in caso di risposta positiva è previsto l'accesso a qualsiasi dato figurante nel modulo di domanda, alle fotografie e ai dati registrati in relazione ai visti rilasciati, rifiutati, annullati, revocati o progati (art. 5, par. 2)[80].

Oltre a queste specifiche garanzie che concorrono a delimitare l'accesso delle autorità di *law enforcement* al sistema di informazione visti, la decisione è assai rigorosa sotto il profilo della tutela del diritto alla protezione dei dati. Inizialmente, era previsto un richiamo esplicito alla decisione quadro sulla protezione dei dati personali elaborati nel quadro della cooperazione giudiziaria e di polizia in materia penale e il Parlamento aveva insistito sul collegamento tra la proposta relativa all'accesso al VIS e quella relativa alla protezione dei dati personali. Il Consiglio ha, invece, preferito escludere un rinvio espresso alla decisione 2008/977/GAI[81] e prevedere una disciplina specifica nella decisione VIS.

Anzitutto, sono state inserite tutta una serie di disposizioni – in materia di sicurezza dei dati (art. 9), di responsabilità (art. 10), di autocontrollo (art. 11), di sanzioni (art. 12) – che ricalcano quelle previste nel regolamento VIS[82]. Accanto a queste, si è posta una norma per regolare il profilo essenziale del trasferimento dei dati ottenuti attraverso l'accesso al VIS a paesi terzi o a organizzazioni internazionali: l'art. 8, par. 4, consente tale trasmissione soltanto in casi eccezionali d'urgenza e previa autorizzazione dello Stato membro che ha inserito i dati. Da questo punto di vista, quindi, la disciplina appare più rigorosa di quella prevista dalla normativa generale posta dall'art. 13 della decisione 2008/977/GAI.

Al contrario, con riferimento all'informazione del trattamento alla persona interessata, la scelta effettuata dalla decisione VIS appare meno garantista rispetto a quella cristallizzata nella decisione quadro: se questa prevede che gli Stati membri «provvedono affinché la persona interessata sia informata della raccolta o del trattamento di dati personali da parte delle rispettive autorità competenti,

---

ogni richiesta. Tuttavia, poiché anche al Parlamento, al pari degli Stati membri, preme che siano predisposti strumenti idonei a contrastare la criminalità e il terrorismo, abbiamo concordato una procedura d'urgenza per i casi di emergenza che può essere sintetizzata come 'prima chiedi, poi giustifica', da applicarsi in situazioni eccezionali di minacce incombenti».

80 Si noti che, nel progetto iniziale, era consentita anche la ricerca immediata sulla base delle fotografie. È stato il Garante europeo a mettere in guardia dai rischi di una ricerca in un archivio molto ampio sulla base delle fotografie (v. *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di decisione del Consiglio relativa all'accesso per la consultazione del sistema d'informazione visti (VIS)*, cit., p. 8): la sua richiesta di inserire le fotografie tra le informazioni supplementari è stata recepita dal Consiglio.

81 In *GUUE*, L 350, 30 dicembre 2008, p. 60.

82 Rispettivamente, gli artt. 32, 33, 35 e 36 regolamento (CE) n. 767/2008.

conformemente alla legislazione nazionale» (art. 16), la decisione VIS rinvia alla disciplina nazionale ed esclude alla radice la comunicazione delle informazioni laddove ciò sia «indispensabile per l'esecuzione di un compito legale» (art. 14, par. 4).

6. Considerazioni conclusive

L'analisi degli sviluppi relativi ai sistemi di informazione che, con un margine accettabile di approssimazione, si sono definiti di "primo pilastro" e del loro rapporto con l'attività di *law enforcement* induce a due conclusioni.

La prima è legata alla stessa natura di Eurodac e VIS. È ben vero che tali banche dati sono pensate per garantire la migliore applicazione della disciplina in materia di asilo e per assicurare la libertà di movimento, ma a questa finalità se ne affianca una (esplicita o implicita) di *law enforcement*. Tale natura composita emerge già sul piano normativo. Nel caso del VIS risulta già dalla definizione delle finalità del sistema informativo. Come si è detto, lo stesso strumento di "primo pilastro" che disciplina in termini generali il VIS riconosce chiaramente tra le sue finalità quella di agevolare la lotta contro la frode e di contribuire a prevenire le minacce alla sicurezza interna agli Stati membri (considerando n. 5 e art. 2 del regolamento (CE) n. 767/2008)[83]. Essa è, invece, meno chiara nel caso dell'Eurodac e si può desumere indirettamente dall'estensione oggettiva dei dati che possono essere raccolti: vengono, infatti, immagazzinate anche le informazioni relative ai soggetti che hanno attraversato in modo irregolare le frontiere. Sembra di poter affermare, quindi, che, anche al fondo di queste banche dati di "primo pilastro" vi è in realtà un intreccio molto stretto tra finalità di libertà e di sicurezza. Nondimeno, solo per il VIS – in relazione al quale la finalità "mista" è esplicita – il legislatore europeo ha attuato puntualmente il canone di accessibilità, così come aveva fatto – sia pure in termini meno equilibrati – in relazione al SIS[84].

La seconda considerazione riguarda proprio il bilanciamento tra il valore della sicurezza e il diritto alla protezione dei dati. A fronte delle ripetute sollecitazioni nel senso di allargare le vie di accesso alle banche dati di "primo pilastro" per finalità di *law enforcement*, sembra che le soluzioni accolte dal legislatore europeo siano sinora improntate a un certo equilibrio. Con riferimento a Eurodac, non è stata presentata una proposta per disciplinare l'accesso e si sta invece lavorando a un testo che risponda alle preoccupazioni legate all'affidamento della gestione delle unità nazionali alle autorità di *law enforcement*. Con riguardo al VIS, invece, pare che la disciplina accolta dalla recente decisione 2008/633/GAI offra un

---

83 In effetti, anche secondo E. Brouwer, "Data Surveillance and Border Control in the EU", cit., p. 147, «from the start, VIS is planned as a multipurpose tool».

84 Con la decisione 2005/211/GAI (*GUUE*, L 68, 15 marzo 2005, p. 44).

bilanciamento ragionevole tra i diversi valori in gioco, nella parte in cui prevede un accesso limitato e circondato da una serie di garanzie effettive.

Non vi è dubbio che un tale approccio più attento agli equilibri tra *efficiency* e *accountability* nelle politiche di creazione di uno spazio di libertà, sicurezza e giustizia sia la conseguenza di due fattori istituzionali, che dipendono proprio dalla collocazione delle banche dati in esame nel "primo pilastro": da una parte, la procedura decisionale, che attribuisce un ruolo decisivo al Parlamento europeo; dall'altra, il coinvolgimento diretto in materia del Garante europeo per la protezione dei diritti dell'uomo.

Information sharing nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione

ANTONELLA MARANDOLA
Professore associato di Procedura penale
Università di Trieste

Sommario: 1. Il trattato di Prüm come strumento di cooperazione rafforzata in materia penale. – 2. Lo scambio di informazioni nel Trattato di Prüm: un'attuazione del principio di disponibilità con alcuni limiti e una zona d'ombra. – 3. (Segue): L'istituzione e la conservazione delle banche dati. – 4. (Segue): Le ipotesi particolari di trasmissione di informazioni. – 5. Diritto alla sicurezza *vs* diritto alla riservatezza. – 6. Le prospettive legislative dell'Italia.

1. Il trattato di Prüm come strumento di cooperazione rafforzata in materia penale

La firma del Trattato di Prüm, avvenuta il 27 maggio 2005, da parte di sette Stati membri dell'Unione europea (Belgio, Lussemburgo, Paesi Bassi, Germania, Francia, Spagna e Austria) si pone quale pietra miliare del lungo e complesso *iter* volto a garantire un elevato livello di protezione ai cittadini nello spazio di libertà, sicurezza e giustizia delineato dall'art. 29 del TUE nell'ambito del c.d. terzo pilastro[1]. Le *guidelines* finalizzate alla realizzazione di questo obiettivo sono individuate, ai sensi del par. 2 dell'art. 29 TUE, nella duplice prospettiva, da leggersi in chiave di complementarità e di reciproca interazione, della progressiva armonizzazione degli ordinamenti statuali interni in materia penale, da un lato, e del rafforzamento della cooperazione tra le forze di polizia e le autorità giudiziarie degli Stati membri, dall'altro lato[2].

Collocandosi in questo secondo angolo visuale, il Trattato di Prüm si pone l'obiettivo di potenziare la cooperazione tra le autorità di *law enforcement* nei settori della lotta contro il terrorismo, della criminalità transnazionale e dell'immigrazione clandestina attraverso una serie di strumenti che possono utilmente ricondursi a due aree tematiche[3].

---

1 Per una lettura diacronica degli atti normativi adottati al fine di realizzare lo spazio comune di libertà sicurezza e giustizia proclamato dai Trattati di Amsterdam e di Nizza e ribadito nelle conclusioni prese in seno al Consiglio europeo di Tampere, si vedano, fra gli altri: E. Aprile, *Diritto processuale penale europeo e internazionale*, Padova, Cedam, 2007, *passim*; M Chiavario, *Cooperazione giudiziaria e di polizia in materia penale a livello europeo*, in "Rivista italiana di diritto e procedura penale", 2005, p. 974; L. Salazar, "Le fonti tipiche dell'Unione Europea", in *Rogatorie penali e cooperazione giudiziaria e internazionale*, a cura di G. L. Greca e M. R. Marchetti, Torino, Giappichelli, 2003, pp. 57 sgg. Per un'analisi delle iniziative volte al superamento della architettura dell'*aquis* U.E. fondata su tre pilastri (Comunità europea, PESC, cioè politica estera e sicurezza comune, e GAI, cioè giustizia e affari interni), ad opera prima del Trattato che adotta una Costituzione per l'Europa, sottoscritto a Roma il 12 gennaio 2005, e poi del Trattato di Lisbona del 13 dicembre 2007, si vedano: M. Bargis, *Costituzione per l'Europa e cooperazione giudiziaria in materia penale*, in "Rivista italiana di diritto e procedura penale", 2005, p. 144; G. De Amicis - G. Uzzolino, *Lo spazio di libertà, sicurezza e giustizia nelle disposizioni penali del Trattato che istituisce una Costituzione per l'Europa*, in "Cassazione penale", 2004, p. 3067; T. Rafaraci, "Lo spazio di libertà, sicurezza e giustizia nel crogiuolo della costruzione europea", in *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, a cura di T. Rafaraci, Milano, Giuffré, 2007, pp. 3 sgg.

2 Sottolineano l'esistenza di un rapporto biunivoco tra cooperazione giudiziaria e armonizzazione penale: E. Bernardi, *Strategie per l'armonizzazione dei sistemi penali europei*, in "Rivista trimestrale di diritto penale dell'economia", 2002, p. 789; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale. Verso un sistema integrato di forme e strumenti di collaborazione tra le autorità giudiziarie*, Milano, Giuffrè, 2007, p. 290.

3 Onde individuare l'ambito di applicazione del Trattato con riferimento alle tipologie di reati, qualche indicazione può trarsi dall'elenco di fattispecie delittuose contemplato dall'art. 2 della decisione quadro 2002/584/GAI del Consiglio in materia di mandato d'arresto europeo, pubblicata in *GUUE*, L 190, 18 luglio 2002, p. 1.

La prima, più caratterizzante, si articola in due ulteriori sottosistemi, l'uno attinente alla semplificazione dello scambio di informazioni tra le autorità degli Stati membri come presupposto indispensabile del rafforzamento della cooperazione, l'altro, quale necessario *pendant*, riguardante la predisposizione di adeguate garanzie in materia di tutela dei dati, in tal modo circolanti. In questo settore, il Trattato di Prüm mostra di recepire, con alcuni limiti, le enunciazioni di principio contenute nel Programma dell'Aia adottato dal Consiglio Europeo il 4 novembre 2004[4], ed in particolare l'affermazione secondo cui il potenziamento della cooperazione di polizia e giudiziaria in materia penale richiede «un approccio innovativo» nei confronti dello scambio di informazioni fra le autorità competenti degli Stati membri, le quali dovrebbero informarsi al cd. principio di disponibilità enunciato in seno al Programma.

In sede di prima approssimazione, l'attuazione da parte del Trattato di Prüm del principio di disponibilità – nei termini di accesso, reciproco e diretto, di informazioni contenute nei *databases* di uno Stato membro da parte di un'autorità di altro Stato membro – si caratterizza in quanto si allontana dai precedenti strumenti di informazione, fra i quali quelli previsti dalle Convenzioni di applicazione Schengen ed Europol, basati sul meccanismo della mediazione della richiesta ad un servizio centrale cui sono collegate le banche dati nazionali[5].

La seconda linea tematica, di carattere residuale, comprende una serie di istituti, di matrice prettamente operativa, che configurano altrettante forme di intervento diretto o congiunto delle forze di polizia di uno Stato membro nel territorio e nello spazio aereo di altro Stato con finalità di prevenzione di atti terroristici e di altre attività criminali transfrontaliere, tra i quali la previsione di scorte di sicurezza armata sui voli aerei (art. 17), le misure relative alla lotta contro l'immigrazione illegale (artt. 20 sg.), le forme di intervento congiunto nel territorio di uno Stato membro (art. 24), le operazioni di polizia transfrontaliera in caso di pericolo imminente (art. 25) e la cooperazione su richiesta (art. 27).

Appare opportuno sottolineare come la suddetta distinzione non rileva solo ai fini di una classificazione squisitamente dogmatica, ma anche nell'ottica della futura ricezione delle disposizioni del Trattato in seno all'Unione Europea.

Giova, a tal fine, premettere alcune considerazioni intorno alla natura giuridica del Trattato di Prüm (di seguito denominato Trattato).

Il testo appartiene al *genus* del diritto internazionale pattizio, esulando, per contro, dal diritto comunitario in quanto negoziato da alcuni soltanto degli Stati membri dell'Unione – ma aperto all'adesione di tutti gli altri Stati membri dell'Unione – e concluso al di fuori dello spazio giuridico europeo, senza avva-

---

4 Pubblicato in *GUUE*, C 53, 3 marzo 2005, p. 1.

5 Per un approfondimento sui meccanismi di funzionamento delle banche dati tradizionalmente operanti nell'*aquis* UE, si veda *supra*, F. Decli - G. Marando, "Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia".

lersi degli strumenti preordinati *ad hoc* dal TUE, per le ipotesi di cooperazione rafforzata.

I sette Stati firmatari si proponevano, infatti, di addivenire ad una più stretta collaborazione nel settore della criminalità transnazionale senza pregiudicare le sorti del TUE e lasciando, al contempo, aperta la prospettiva della futura ricezione dell'accordo da parte dell'Unione, sulla base di uno schema analogo a quello a suo tempo seguìto per gli accordi di Schengen.

L'iniziativa protesa alla realizzazione di una cooperazione rafforzata tra alcuni Stati membri – al di fuori delle procedure previste dall'art. 43 TUE – ha sollevato, da una parte, alcune perplessità circa la legittimità delle modalità di adozione del testo[6], mentre, dall'altra parte, ha reso necessario dotare lo strumento *de quo* di alcune clausole di adattamento al fine di garantirne la compatibilità con le disposizioni contenute nel Trattato dell'Unione anche nell'ottica dell'integrazione di Prüm nell'*aquis* UE.

Così, l'art. 47, par. 1, del Trattato enuncia, *in primis*, il principio di prevalenza del diritto dell'Unione Europea sulle norme in esso contenute, qualora quest'ultime risultino incompatibili con le prime; in secondo luogo, l'art. 1, par. 4, prevede che entro tre anni dalla data della sua entrata in vigore dovrà essere avviata una iniziativa volta a consentirne l'integrazione nello spazio giuridico dell'Unione europea «sulla base di una valutazione dell'esperienza acquisita grazie all'attuazione del Trattato stesso».

A tale disposizione è stata data realizzazione, in seguito all'intenso dibattito avviato dalla Presidenza tedesca dell'Unione durante la riunione dei ministri svoltasi a Dresda il 15-16 gennaio 2007, con una prima proposta, sottoscritta da tredici Stati membri, volta a consentire l'ingresso nel diritto dell'Unione delle principali disposizioni del Trattato, cui è seguita una seconda iniziativa, di poco successiva, di analogo tenore ma proveniente da quindici Stati membri[7].

Successivamente durante il Consiglio GAI del 15 febbraio 2007[8] è stato raggiunto un accordo per la trasposizione delle «parti essenziali» del Trattato mediante lo strumento della decisione del "terzo pilastro"[9]. A questo ha fatto seguito

---

6 Sul punto, il Garante europeo ha messo in luce che il procedimento adottato potrebbe configurare una violazione della procedura di cooperazione rafforzata prevista dall'art. 40 TUE nell'ambito del "terzo pilastro", in quanto gli Stati aderenti a Prüm avrebbero conseguito, mediante l'adozione di tale strumento giuridico, il fine di evitare l'*iter* legislativo previsto in ambito GAI, che subordina l'adozione delle decisioni al requisito dell'unanimità (il testo del Parere è pubblicato in *GUUE*, C 169, 21 luglio 2007, p. 2). Cfr. anche *supra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea", § 8.

7 Il testo dell'iniziativa è pubblicato in *GUUE*, C 71, 28 marzo 2007, p. 35.

8 Si veda il Comunicato stampa, 2781ª sessione del Consiglio "Giustizia e affari interni", Bruxelles, 15 febbraio 2007.

9 Sul punto, alcuni dubbi sono stati sollevati con riferimento alla base giuridica della decisione di cui all'art. 34, par. 2, lett. *c*), del Trattato UE e si è ritenuta, per contro, più adeguata la base giuridica della decisione quadro di cui all'art. 34, par. 2, lett. *b*), caratterizzata da una maggiore

una Risoluzione del Parlamento Europeo (7 giugno 2007) che si è espressa in senso favorevole all'adesione della proposta di decisione da parte del Consiglio.

L'iniziativa ha, infine, trovato definitiva consacrazione nella recente decisione 2008/615/GAI, del 23 giugno 2008, la quale, come premesso, si propone, tra l'altro, di incorporare la sostanza delle disposizioni in seno al quadro giuridico europeo.

Mantenendo, per il momento, fermo lo sguardo sul tenore normativo del Trattato è necessario operare un *distinguo* tra due settori tematici: da un lato, si collocano le disposizioni afferenti allo scambio di dati tra le autorità degli Stati membri e alla correlativa tutela delle informazioni, in relazione alle quali, trattandosi di materie attinenti al "terzo pilastro", si prevede l'integrale inserimento in ambito europeo; dall'altro lato, si situano gli istituti che coinvolgono materie nelle quali esiste una competenza comunitaria, come le indicate disposizioni relative agli agenti di sicurezza a bordo degli aerei (cd. *air marshals*, *ex* art. 17), le misure volte a combattere l'immigrazione clandestina (artt. 20 sg.), quelle concernenti le operazioni di polizia transfrontaliera in caso di pericolo imminente (art. 25) e la cooperazione su richiesta (art. 27).

2. Lo scambio di informazioni nel Trattato di Prüm: un'attuazione del principio di disponibilità con alcuni limiti e una zona d'ombra

È opinione condivisa in dottrina che la dimensione transnazionale delle nuove forme di criminalità organizzata, unitamente al carattere dinamico che ne consente la dislocazione su vasta scala all'interno del territorio dell'Unione europea e all'impiego di tecniche criminose che consentono di travalicare i confini dei singoli Stati, ha reso necessario potenziare il coordinamento tra le autorità nazionali assicurando la circolarità dei dati in possesso dei singoli Stati sia a fini preventivi che di indagine[10].

A tal riguardo, un vero e proprio spartiacque in tema di interscambio di informazioni è rappresentato, come già anticipato, dal Programma dell'Aia, adottato nel novembre del 2004 dal Consiglio Europeo a Bruxelles. Il Consiglio, coniando il cd. principio di disponibilità, ha previsto che, a far data dal 1° gennaio 2008, l'accesso e lo scambio di informazioni e di *intelligence* tra gli Stati membri dell'Unione debba avvenire in modo tale che un ufficiale di contrasto di uno Stato membro, che necessiti di informazioni in funzione preventiva e di repressione di determinati reati possa ottenerle direttamente da un altro Stato membro, alle

---

apertura alla consultazione del Parlamento, in quanto lo strumento da adottare perseguirebbe, sia pure indirettamente, il fine di armonizzare le legislazioni tra gli Stati membri.

10 Per la definizione di "reato transnazionale", in seguito all'entrata in vigore della Convenzione di Palermo, si veda E. Rosi, "Il reato transnazionale", in *Criminalità organizzata transnazionale e sistema penale italiano. La Convenzione ONU di Palermo*, a cura di E. Rosi, Milano, Ipsoa, 2007, pp. 67 sgg.

stesse condizioni previste per le autorità interne. Superando le precedenti impostazioni in materia, il principio *de quo* mira a realizzare la condivisione dei dati (*information sharing*) in possesso di un singolo Stato con le autorità di *law enforcement* degli altri Stati, preludendo, per tale via, alla creazione di uno spazio di libera circolazione delle informazioni, nel rispetto delle norme di garanzia sulla protezione dei dati raccolti[11].

Per un verso, infatti, l'enunciazione del principio di disponibilità in materia di scambio di informazioni rappresenta una netta innovazione rispetto agli assetti dei circuiti informativi tradizionalmente operanti su scala europea – quali SIS (Sistema Informativo Schengen), E-TECS di Europol, EPOC-III di Eurojust – il cui funzionamento, informandosi al principio di base che i dati appartengono a chi li detiene, si fonda sulla mediazione di una unità centrale attivabile a richiesta delle sezioni nazionali e degli Stati membri, i quali stabiliscono limiti e condizioni di accesso ai propri databases[12].

Per altro verso, l'obiettivo posto dal Programma dell'Aia si pone quale lineaguida degli strumenti giuridici volti a realizzare il rafforzamento della cooperazione giudiziaria mediante l'interscambio diretto delle informazioni in possesso dei singoli Stati[13].

La materia dello scambio di informazioni sulla base del principio di disponibilità trova compiuta ed autonoma trattazione negli artt. 2-15 del Capitolo II del Trattato, recante la disciplina delle modalità con cui avviene l'*information sharing* (artt. 2-12) e la previsione della trasmissione di dati in occasione di grandi eventi (artt. 13-15), cui deve aggiungersi, per contiguità di contenuto, la menzione specifica dello scambio di dati in funzione di contrasto al terrorismo (art. 16), benché attratta nell'orbita del Capitolo III, dedicato alle misure di prevenzione di attacchi terroristici[14].

Sotto tale profilo, deve evidenziarsi che il merito della prospettiva coltivata dal Trattato è non solo quella di consentire che le informazioni confluiscano in un unico *network* di banche dati direttamente consultabile dalle autorità interne

---

11 Per un approfondimento del principio di disponibilità nel quadro del Programma dell'Aia, si rinvia, ancora, a S. Ciampi, *op. cit*.

12 Al riguardo, si veda *supra*, F. Decli - G. Marando, *op. cit*.

13 Tra gli strumenti giuridici che attuano il principio di disponibilità enunciato dal Programma in ambito UE si annoverano: la proposta di decisione quadro della Commissione n. 490 del 2005 sullo scambio di informazioni in virtù del principio di disponibilità; la decisione del Consiglio n. 671 del 2005 concernente lo scambio di informazioni e la cooperazione in materia di reati terroristici, 2005/671/GAI del 20 settembre 2005 (in *GUUE*, L 253, 29 settembre 2005, p. 22); la decisione del Consiglio n. 960 del 18 dicembre 2006 sull'applicazione del principio di disponibilità allo scambio di informazioni tra i Paesi UE al fine del rafforzamento della cooperazione di polizia (in *GUUE*, L 386, 29 dicembre 2006, p. 89). Per un approfondimento, si veda, *amplius*, S. Ciampi, *op. cit*.

14 Per un' analisi testuale del Trattato, si veda F. Gandini, *Il trattato di Prüm articolo per articolo. Ecco le nuove frontiere per la sicurezza. Banche dati antiterrorismo e interventi congiunti in 7 Stati Ue*, in "Diritto e giustizia", 2006, n. 37, pp. 57 sgg.

degli Stati membri, ma anche quella di realizzare, attraverso gli impegni assunti dalle Parti contraenti a livello internazionale, e, sia pure indirettamente, una armonizzazione degli ordinamenti interni dei singoli Stati[15].

Orbene, il potenziamento della cooperazione transfrontaliera che il testo *de quo* consente, anche e, soprattutto, nell'ottica della lotta al terrorismo e alla criminalità transfrontaliera, soddisfacendo pienamente i requisiti sostanziali del Programma dell'Aia, ha, come si è detto, indotto il Consiglio dell'Unione europea a fare proprie le disposizioni del Trattato attraverso la decisione 2008/615/GAI[16].

L'atto europeo mutua e recepisce quelle disposizioni che vengono, quindi, ad inserirsi, a pieno titolo, all'interno della cornice legislativa europea determinando, del pari, l'accelerazione dell'operatività dei meccanismi di fruizione "diretta" dei dati di *intelligence* di cui dispongono i singoli Stati, in ossequio alle direttive del Programma[17], rendendo, fra l'altro, superflua la predisposizione di uno schedario unico "europeo" che avrebbe comportato costi e tempi indubbiamente più ampi.

By-passando la singola adesione degli Stati che ne avevano assunto l'iniziativa e estendendone la valenza agli altri Stati membri dell'Unione, la decisione del 2008 ricalca in larghissima parte, infatti, il contenuto e la sostanza del Trattato: essa contiene disposizioni riguardanti il trasferimento automatizzato di profili DNA; dati in materia di impronte digitali (*fingerprints*) e dati relativi ai veicoli iscritti nei pubblici registri e, più in generale, dei dati in relazione a eventi di rilievo a dimensione transfrontaliera, nell'intento univoco di prevenire reati terroristici e potenziare la cooperazione di polizia sovranazionale.

Al fine di realizzare la condivisione di informazioni, gli Stati membri si impegnano, infatti, a istituire e conservare tre banche dati nazionali accessibili online e contenenti profili di DNA, dati in materia di impronte digitali (*fingerprints*) e dati relativi ai veicoli iscritti nei pubblici registri. A differenza di quest'ultima banca dati, che permette di accedere immediatamente ai dati relativi al proprietario a partire dal numero di immatricolazione, gli archivi con profili DNA e quelli dattiloscopici non consentono di pervenire direttamente ad una identificazione della persona cui si riferiscono, ma sono soggetti ad un procedimento comune di consultazione che si articola in due fasi (cd. doppio binario).

---

15 Configura l'armonizzazione come una tecnica normativa che persegue il ravvicinamento di diversi ordinamenti, il quale può presentarsi in forma spontanea o indotta, S. Allegrezza, "Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo", in *L'area di libertà sicurezza e giustizia*, cit., p. 702.

16 Pubblicata in *GUUE*, L 210, 6 agosto 2008, p. 1. Va poi segnalata la contestuale decisione 2008/616/GAI, volta a stabilire le disposizioni amministrative e tecniche necessarie all'attuazione della decisione 2008/615/GAI (in *GUUE*, L 210, 6 agosto 2008, p. 12).

17 In ambito UE, il principio di disponibilità nell'ottica del Programma dell'Aia era stato recepito nella proposta di decisione quadro COM (2005) 490 def., del 12 ottobre 2005. Cfr., *supra*, S. Ciampi, *op. cit.*, § 4. In argomento, si veda anche la decisione 2005/671/GAI del 20 settembre 2005 (in *GUUE*, L 253, 29 settembre 2005, p. 22).

La prima fase disciplina l'accesso automatizzato on-line alle informazioni contenute all'interno delle banche dati. Come si è anticipato, essa non consente l'accesso diretto ai dati che permettono di risalire all'identità della persona interessata, ma, più semplicemente, rende disponibili i soli indici di consultazione. Pertanto, mediante la procedura di accesso automatizzato (cd. sistema *hit/no hit*) l'autorità richiedente potrà attingere unicamente ad un indice di consultazione anonimo e ad un numero di riferimento (*reference index*) al fine di verificare la presenza del dato nell'archivio.

La procedura di accesso, a seconda del tipo di informazione in possesso della parte richiedente, si articola in due differenti modalità di ricerca.

Sotto tale aspetto, il Trattato, prima, e la decisione europea, poi, prevedono che, ove l'autorità compulsante disponga di un profilo DNA riferibile ad una persona identificata, questa può avviare una procedura di consultazione automatizzata (*automated searching*) al fine di verificare se il dato immesso nel sistema trovi una concordanza all'interno del complesso di informazioni registrate nell'archivio. Lo scopo della consultazione è, pertanto, quello di accertare se la banca dati contenga un profilo corrispondente a quello trasmesso. Al termine della ricerca automatizzata, la parte compulsante è raggiunta da una informazione che comunica, in caso di esito positivo, il solo *reference index*, attestante la sussistenza in banca dati del profilo richiesto, e, in caso di esito negativo, l'impossibilità di registrare una concordanza tra i dati immessi e quelli registrati.

Ove, per contro, la parte richiedente disponga di un profilo DNA che non sia attribuibile a persona determinata o determinabile (cd. *open record*), viene dato avvio ad un procedimento di comparazione (*automated comparison*). La procedura di comparazione viene attivata mediante la trasmissione del profilo anonimo al fine di saggiarne la corrispondenza con tutti i dati contenuti in archivio, siano o meno riferibili a persona determinata.

Le due forme di accesso alla banca dati, pertanto, si distinguono principalmente in ragione della fonte di compulsazione, costituita, nel primo caso, da un profilo identificato, e, nel secondo caso, da una traccia aperta, mentre la procedura di ricerca avviene in forma automatizzata, con modalità analoghe.

Un ulteriore elemento di differenziazione è dato dalla comunicazione relativa agli esiti della ricerca alla Parte compulsante: l'inoltro avviene, in forma non automatizzata, a cura dell'autorità richiesta e solo nei casi in cui il sistema abbia permesso di registrare una concordanza.

Quando l'accesso automatizzato on-line mediante consultazione o comparazione abbia dato esito positivo, si apre, infatti, la seconda fase del procedimento che riguarda la trasmissione delle informazioni ricollegabili ai dati di indice all'autorità richiedente. Sotto tale profilo, la disciplina appare, invero, piuttosto scarna: la normativa internazionale si limita, infatti, a prevedere la necessità di una richiesta esplicita da parte dell'autorità interessata ad ottenere le ulteriori informazioni ricollegabili all'indice di consultazione, e rinviando, per i profili procedurali, alle norme di diritto interno dello Stato membro e alle Convenzioni sull'assistenza giudiziaria *ivi* vigenti.

Il Trattato lascia impregiudicata la centrale questione se in capo alla Parte richiesta debba configurarsi un obbligo, un onere o una mera facoltà di trasmettere l'informazione all'autorità richiedente. Esula, parimenti, dalla disciplina pattizia, la specificazione dei modi e dei tempi del procedimento informativo. Sul punto, il Trattato si limita, infatti, ad operare un generico rinvio alle pregresse Convenzioni regolanti i rapporti di assistenza giudiziaria tra gli Stati dell'Unione europea (artt. 5 e 10)[18].

La materia, com'è noto, è regolata dalla Convenzione europea di Strasburgo del 20 aprile 1959[19], nonché dalla Convenzione sull'assistenza giudiziaria adottata dal Consiglio dell'Unione europea il 29 maggio 2000[20]. Il rinvio a tali atti normativi parrebbe configurare, a carico dei soli Stati che abbiano ratificato gli accordi *de quibus*[21], un dovere dell'autorità interna di dare seguito alla richiesta di trasmissioni di informazioni collegate al *reference index*. Il rifiuto di adempiere potrebbe essere opposto solo nei casi espressamente previsti e, in ogni caso, dovrebbe essere corredato di motivazione[22].

La smagliatura normativa è lasciata indenne nel testo della decisione 2008/615/GAI, che conferma il richiamo alla normativa interna.

Verosimilmente, la questione potrebbe essere risolta ricorrendo alle decisioni-quadro 2006/960/GAI e 2008/977/GAI che configurano una sorta di "mutua

---

18 Diversamente, la proposta di decisione quadro in tema di principio di disponibilità configurava *expressis verbis* un obbligo in capo all'autorità richiesta di fornire le informazioni richieste entro termini prestabiliti, potendo opporre un rifiuto solo in casi tassativi.

19 Ai sensi della Convenzione di Strasburgo, l'assistenza giudiziaria deve essere concessa dalle Parti contraenti secondo le modalità stabilite dallo Stato richiesto, e può essere rifiutata solo in casi tassativamente indicati (art. 2) e con atto motivato (art. 19); il testo specifica, poi, i casi nei quali la comunicazione può avvenire in via diretta tra le autorità dei singoli Stati (art. 15).

20 La Convenzione di mutua assistenza del 29 maggio 2000 modifica il precedente quadro normativo spostando il baricentro del coordinamento tra gli Stati e specificando le modalità e i termini che scandiscono il procedimento di trasmissione degli atti e delle informazioni. In particolare, l'accordo pone a carico dello Stato richiesto l'obbligo formale di fornire l'assistenza nel rispetto delle modalità (par. 1) e dei termini (par. 2) indicati dall'Autorità richiedente, anziché dalla Parte richiesta, prevedendo, in caso di inottemperanza, che quest'ultima sia tenuta a darne pronta informazione.

21 La Convenzione sull'assistenza giudiziaria del 2000 non è stata ratificata dall'Italia, e, pertanto, non è entrata in vigore nel nostro ordinamento: in argomento, si veda E. Aprile, *op. cit.*, p. 48; E. Zanetti, "Le convenzioni vigenti", in *Rogatorie penali e cooperazione giudiziaria internazionale*, cit., pp. 79 sgg.

22 Cfr. la decisione n. 960 del 2006, che, dando piena attuazione al principio di disponibilità, prevede il diritto della parte richiedente, con correlativo obbligo di attivazione in capo all'autorità richiesta, di ottenere i dati alle medesime, o più favorevoli condizioni previste per gli organi competenti sul piano nazionale. A tal fine, la parte interessata deve inoltrare una richiesta motivata che fa sorgere a carico dell'interlocutore un dovere di fornire le informazioni e i dati di *intelligence* entro otto ore, prorogabile fino a tre giorni, nel caso in cui la richiesta sia contrassegnata dal requisito dell'urgenza, ed entro una settimana nei casi non urgenti. Per un approfondimento, si rinvia a S. Ciampi, *op. cit.*, § 9.

circolarità" delle informazioni, rafforzandosi, così, l'idea della reciproca complementarietà dei più recenti strumenti normativi sopranazionali[23].

In ogni caso, qualora venga riscontrata una concordanza, al punto di contatto nazionale dello Stato richiedente sono notificati, per via automatizzata, i dati indicizzati; in forma automatizzata avviene altresì la comunicazione negativa.

Il Trattato non chiarisce, peraltro, se le richieste ai punti di contatto nazionali possano provenire solo dall'autorità di polizia o anche dall'autorità giudiziaria.

Sul punto, a favore della soluzione di una creazione e gestione dei rapporti tra "punti di contatto" e , dunque, della soluzione meno ampia si è espressa la dottrina[24]. La conclusione merita condivisione anche alla luce di quanto stabilisce il testo adottato dal Consiglio europeo che polarizza il suo campo di applicazione nel settore delle attività preventive del crimine, di competenza esclusiva delle autorità di *intelligence*[25], senza peraltro, che possa trascurarsi il fatto che il corredo degli strumenti indicati è creato ai fini dello scambio di informazioni, vale a dire al duplice obiettivo della prevenzione e del perseguimento dei reati.

Più precisamente, l'accesso alla banca dati DNA appare riservato esclusivamente alle attività di investigazione, come attesta l'*incipit* degli artt. 3 e 4 della decisione 2008/615/GAI («per le indagini penali»), mentre gli archivi relativi ai dati *fingerprints* e di immatricolazione dei veicoli sono compulsabili solo in casi concreti e, quanto al primo, sia per finalità preventive che di indagine (art. 8), e quanto al secondo, in ulteriore aggiunta, anche per altri illeciti che rientrino nella competenza dei tribunali e delle procure e per il mantenimento della sicurezza e all'ordine pubblico (art. 12). Se così è, appare preferibile che il testo del 2008 abbia voluto riferirsi alle autorità a cui gli ordinamenti dei singoli Stati attribuiscano una "competenza specifica" nei settori menzionati.

In conclusione, nel tessuto normativo in esame il principio di disponibilità riceve un'attuazione equilibrata, sotto il profilo sia quantitativo, sia procedimentale: da un lato, l'accesso è limitato a determinate categorie di informazioni, quali i profili di DNA, le impronte digitali e i dati relativi ai veicoli. In questa prospettiva, rispetto al Trattato, i confini di operatività del meccanismo che governa lo scambio dei dati vengono ampliati unicamente sotto l'aspetto quantitativo, fermo restando che entrambi i testi ne circoscrivono l'applicazione rispetto ad una parte soltanto delle informazioni rilevanti sul fronte della prevenzione e della repressione dei reati[26].

---

23 Si veda, *amplius*, S. Ciampi, *op. cit.*

24 V., per l'esegesi più restrittiva anche rispetto al Trattato, F. Gandini, *op. cit.*, p. 67.

25 Sul distinguo tra attività di *intelligence* e attività di indagine, si veda M. L. Di Bitonto, "Raccolta di informazioni e attività di *intelligence*", in *Contrasto al terrorismo interno e internazionale*, a cura di R. E. Kostoris e R. Orlandi, Torino, Giappichelli, 2006, p. 253.

26 Da questo punto di vista, le categorie di informazioni compulsabili sono più limitate rispetto a quanto previsto nella proposta di decisione quadro del 12 ottobre 2005, nella proposta

Dall'altro lato, l'accesso on-line agli archivi DNA e *fingerprints* mediante il sistema *hit/no hit* consente di accertare unicamente se il dato oggetto della ricerca è contenuto nella banca dati di riferimento, essendo invece precluso l'accesso diretto ad ogni altra informazione ad esso riconducibile.

Il considerando n. 18 della decisione 2008/615/GAI identifica, infatti, nel «sistema '*hit/no hit*' la struttura più idonea di raffronto dei profili anonimi, in quanto i dati supplementari a carattere personale sono scambiati solo dopo una risposta positiva; in quanto la loro trasmissione e la loro ricezione sono disciplinati dalla legislazione nazionale, fra le quali quelle relative all'assistenza giudiziaria. In tal modo si garantisce un sistema adeguato di protezione dei dati, essendo inteso che la trasmissione di dati personali ad un altro Stato membro richiede un livello adeguato di protezione dei dati da parte degli Stati riceventi».

Il principio di disponibilità risulta, invece, attuato *in toto* con riferimento ai veicoli registrati, in quanto la consultazione on-line della relativa banca dati consente di accedere, a partire dal numero di identificazione del veicolo o dal numero di targa, direttamente ai dati relativi al proprietario. Si assiste, pertanto, ad una graduazione del principio di disponibilità sulla scorta del grado di invasività dei dati oggetto di trasmissione.

3. (Segue): L'istituzione e la conservazione delle banche dati

Uno dei tratti più caratterizzanti del sistema di scambio di informazioni prefigurato dal Trattato, prima, e dall'atto del Consiglio, poi, concerne, come si è detto, l'istituzione di tre archivi centralizzati, contenenti rispettivamente i dati degli schedari nazionali di analisi DNA, i profili dattiloscopici (AFIS) e i dati contenuti nei registri nazionali dei veicoli. Deve, tuttavia, evidenziarsi come l'obbligo di costituzione e mantenimento (art. 2) è configurato a carico degli Stati dell'Unione solo con riferimento alla banca dati DNA, mentre gli archivi sulle impronte digitali (art. 8) e sui veicoli registrati (art. 12), generalmente già istituiti dagli Stati firmatari, sono oggetto di un mero dovere di conservazione e di accesso.

Il profilo istitutivo va, dunque, circoscritto alla creazione di una banca dati nazionale di analisi DNA.

La sua costituzione viene assunta quale *condicio sine qua non* di adesione al Trattato (artt. 2, parr. 3 e 42), ma il presupposto, com'è intuibile, è superato dalla decisione europea.

Peraltro, si è già chiarito come il sistema del doppio binario informativo obblighi ciascuno Stato a rendere accessibili alla consultazione diretta unicamente gli indici di riferimento, senza che sia possibile pervenire immediatamente

---

di decisione quadro del Regno di Svezia, e, infine, nella decisione quadro n. 960 del 2006. Sul punto, si veda, *supra*, S. Ciampi, *op. cit.*, § 8.

all'identificazione della persona cui i dati si riferiscono (artt. 2, par. 2 e 3, par. 2). In questa sede, occorre aggiungere che il *reference index* è costituito da un numero e da un profilo ricavato dalla parte non codificante del DNA (cd. *junk DNA*)[27].

Gli Stati, in altri termini, devono limitare la trasmissione dei risultati delle analisi DNA alle zone cromosomiche prive di espressione genetica, escludendo quei segmenti dai quali siano desumibili informazioni su specifiche caratteristiche ereditarie o sullo stato di salute. La previsione si inserisce, invero, nel solco della posizione già adottata dall'Unione Europea in materia di scambio dei risultati di analisi del DNA con due successive Risoluzioni del Consiglio, rese in data 9 giugno 1997 e 25 giugno 2001[28], in cui gli Stati membri vengono esortati a circoscrivere il materiale di scambio ai dati concernenti il profilo non codificante della molecola DNA. Nella medesima prospettiva, trattandosi di una scienza *in fieri*, il Consiglio ha stabilito che, qualora l'evoluzione scientifica consentisse di trarre informazioni su specifiche caratteristiche ereditarie dai marcatori DNA, gli Stati membri sarebbero tenuti a precluderne la disponibilità allo scambio e a distruggere i risultati delle analisi DNA da essi ricevuti e contenenti tali informazioni.

Gli elementi di alimentazione della banca dati sono rappresentati da due *species* di dati: da un lato, si pongono i profili che consentono l'identificazione della persona interessata e dall'altro le cd. tracce aperte, ovvero non attribuibili ad alcuno[29]. Il testo della decisione 2008/615/GAI – al pari, peraltro, del Trattato – nulla dispone in merito al procedimento di estrazione e tipizzazione del profilo, né in relazione alle categorie di persone che possono essere sottoposte ai prelievi, né, infine, alle modalità tecniche di raccolta.

Quanto al profilo della conservazione degli archivi, ci si è chiesti se il generico obbligo di mantenimento includa anche quello di alimentazione della banca dati mediante la raccolta di dati e informazioni da parte dei singoli Stati. Sul punto, soccorre l'interpretazione sistematica con l'art. 7 della decisione 2008/615/GAI che, analogamente a quanto prevede il Trattato, stabilisce uno specifico obbligo di attivazione in capo ai singoli Stati nei casi in cui diviene necessario acquisire un profilo DNA di un soggetto che si trova nel territorio della Parte richiesta ed è indiziato di reato nell'ambito di un procedimento in corso nello Stato richiedente. In tale ipotesi, il Paese richiesto, cui venga presentata domanda motivata contenente l'indicazione dello scopo e del titolo giuridico dell'atto («mandato

---

27 L'art. 1-*bis* della proposta di decisione del Consiglio, emendata dal Parlamento, definisce le parti non codificanti del DNA come «le aree cromosomiche che non contengono alcuna espressione genetica, ovvero non note per fornire espressione genetica, ovvero non note per fornire informazioni su caratteristiche ereditarie specifiche», precisando che «senza pregiudizio di eventuali progressi scientifici, non verranno rivelate, né ora né in futuro, ulteriori informazioni sulla parte non codificante del DNA».

28 La seconda è pubblicata in *GUUE*, C 187, 3 luglio 2001, p. 1.

29 V., per ulteriori approfondimenti sulla struttura e proprietà del DNA, R. Dominici, "Prova del DNA", in *Digesto delle discipline penalistiche*, X, Torino, Utet, 2002, pp. 373 sgg.

o una dichiarazione di inchiesta dell'autorità competente, come richiesto dalla sua legislazione nazionale»), deve accordare l'assistenza giuridica allo Stato richiedente ai fini del prelevamento e analisi del profilo genetico del soggetto sottoposto ad indagini o un procedimento penale, nel rispetto del diritto interno dello Stato membro richiesto. Da tale dettagliata disciplina, pur regolante la richiesta di acquisizione del profilo DNA nel caso specifico in cui sia in corso un procedimento penale, pare doversi dedurre, sulla base dell'argomento interpretativo per cui *ubi lex voluit dixit, ubi noluit tacuit*, l'inesistenza di un obbligo generico di alimentazione delle banche dati in capo ai singoli Stati, dovendosi interpretare il dovere di mantenimento come un generico impegno di conservazione degli archivi nazionali, pur nella consapevolezza che l'obiettivo che si prefigge la decisione, qual è quella di realizzare un miglioramento della cooperazione giudiziaria e di polizia e una facilitazione dello scambio di informazioni per aprire una nuova dimensione nella lotta alla criminalità passa, fra l'altro, attraverso un suo "corretto" mantenimento.

4. (Segue): Le ipotesi particolari di trasmissione di informazioni

Gli artt. 13-15 del provvedimento del Consiglio d'Europa del 23 giugno 2008 regolano la trasmissione di dati di natura non personale (art. 13) e personale (art. 14) ai fini del mantenimento dell'ordine pubblico e della sicurezza, nonché della prevenzione di reati, in occasione di grandi eventi a carattere transfrontaliero, tra i quali vengono menzionati, in via esemplificativa, le manifestazioni a carattere sportivo e le riunioni del Consiglio europeo. Lo scambio di informazioni in siffatte occasioni rientra, nondimeno, nel novero degli strumenti predisposti in seno all'Unione europea al fine di rafforzare la cooperazione degli Stati membri, essendo oggetto di previsione specifica dell'Azione comune 97/339/GAI[30] e, successivamente, della Risoluzione del Consiglio adottata in data 29 aprile 2004[31] in relazione alla sicurezza delle riunioni del Consiglio europeo e di altri eventi di pari risonanza.

Il quadro normativo regolante il procedimento di trasmissione di informazioni contempla, in tal caso, due fattispecie procedurali che si differenziano in relazione al menzionato carattere personale o meno del dato oggetto di scambio[32].

---

30 L'Azione comune 97/339/GAI del 26 maggio 1997 è stata adottata dal Consiglio in base all'art. K.3 del Trattato UE in materia di cooperazione nel settore dell'ordine pubblico e della pubblica sicurezza, ed è pubblicata in *GUUE*, L 147, 5 giugno 1997, p. 1.

31 In *GUUE*, C 116, 20 aprile 2004, p. 18. Sul punto, si veda anche l'iniziativa del Regno dei Paesi Bassi in vista dell'adozione della Decisione del Consiglio concernente il rafforzamento della cooperazione di polizia in occasione di grandi eventi, pubblicata in *GUUE*, C 101, 27 aprile 2005, p. 36.

32 La sopravvenienza dell'atto europeo che fa proprio il contenuto sostanziale del Trattato consente di superare il nodo interpretativo legato alla definizione di «dato personale», non tanto perché la nozione sarebbe ivi ricavabile, quanto piuttosto per il fatto che utili indicazioni possono essere tratte dalla decisione–quadro del Consiglio 2008/977/GAI sulla protezione dei

In ambedue i *sub*-procedimenti si prevede che gli Stati europei interessati possano procedere allo scambio di informazioni, sia di propria iniziativa che a seguito di richiesta inoltrata da altra Parte contraente, con atto motivato che faccia menzione dello specifico evento. La trasmissione, sia spontanea che a richiesta, avviene per mezzo di punti di contatto nazionali designati *ad hoc* all'atto del deposito degli strumenti di ratifica (art. 15) e nel rispetto della legislazione nazionale dello Stato membro che li trasmette.

Comune ad entrambi è, peraltro, lo scopo della trasmissione, da identificarsi, come si è premesso, nella prevenzione di reati e nel mantenimento dell'ordine e della sicurezza pubblica in occasione dei già segnalati avvenimenti di natura transnazionale.

Parrebbero, invece, finalizzati a garantire un maggior grado di tutela dei dati a carattere personale gli elementi di differenziazione delle due fattispecie: così, da un lato, l'art. 14 prevede che la trasmissione, spontanea o a richiesta, dei dati a carattere personale debba trovare fondamento in una presunzione di pericolosità della persona interessata.

Sotto tale aspetto, deve segnalarsi che tale giudizio prognostico è ancorato a criteri non soddisfacenti quanto a determinatezza della fattispecie: la norma opera, infatti, un generico riferimento a «condanne definitive o altre circostanze facciano presupporre che le persone interessate commetteranno reati» – non meglio identificati – «in occasione di questi eventi o che costituiranno una minaccia per l'ordine e la sicurezza pubblici», rimettendo, dunque, alla totale discrezionalità dell'autorità competente la valutazione in ordine alla sua ricorrenza.

Dall'altro lato, si prevede un limite all'utilizzo e alla conservazione dei dati personali: le informazioni ottenute possono essere impiegate "esclusivamente" ai fini della prevenzione dei reati e del mantenimento dell'ordine pubblico, e solo nell'ambito dell'evento menzionato nell'atto di trasmissione. Non appena la conservazione del dato appare, dunque, infruttuosa perché l'obiettivo è stato raggiunto o non può più esserlo, i dati dovranno essere cancellati immediatamente. In ogni caso, l'art. 14, par. 2, prevede, con apposita norma di chiusura, che l'informazione non possa essere conservata per più di un anno.

Anche lo strumento della trasmissione di informazioni ai fini della prevenzione di attacchi terroristici – regolato all'art. 16 – costituisce parte integrante dell'*aquis* UE in quanto contemplata dalla decisione n. 2003/48/GAI del Consiglio della UE[33], sostituita dalla successiva decisione n. 2005/671/GAI adottata dal Consiglio il 20 settembre 2005 in relazione al rafforzamento della cooperazione investigativa nel settore dei reati di terrorismo[34].

---

dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. L'art. 2 del testo precisa, infatti, che per dato personale deve intendersi «qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata») [...]».

33 Pubblicata in *GUUE*, L 16, 22 gennaio 2003, p. 68.

34 Pubblicata in *GUUE*, L 253, 29 settembre 2005, p. 22. In merito, si veda, G. De Amicis,

L'art. 16 configura, invero, una facoltà, e non un obbligo, in capo ai singoli Stati di procedere allo scambio di dati personali e altre informazioni al fine di prevenire attacchi terroristici.

La disposizione contempla alcune norme di interpretazione autentica al fine di determinare il suo corretto ambito di applicazione: così, i reati di terrorismo, in relazione ai quali è prevista la facoltà di scambio di dati, si individuano sulla base della tipologia delle figure criminose elencate dagli artt. 1-3 della decisione quadro 2002/475/GAI adottata dal Consiglio dell'Unione il 13 giugno 2002 in relazione alla lotta contro il terrorismo[35]; inoltre, la trasmissione può avere ad oggetto dati personali, cioè le informazioni concernenti una persona fisica identificata o identificabile, comprensivi, ai sensi del par. 2 dell'art. 16, del nome, cognome, data e luogo di nascita e di una descrizione dei fatti che giustificano la presunzione di pericolosità posta alla base dell'inoltro.

Quanto ai profili procedurali, l'invio a fini preventivi può avvenire in relazione a casi concreti e quando vi siano «particolari circostanze» idonee a fondare una presunzione di pericolosità del soggetto interessato in relazione alla commissione dei reati *de quibus*[36]. Anche in tal caso, la norma in esame non fornisce alcun chiarimento sul punto, ma si limita ad ancorarne l'operatività alla sussistenza di specifiche circostanze e in relazione a casi concreti, per cui sarà l'autorità di *intelligence* ad operare un giudizio di prognosi a fronte di parametri del tutto insoddisfacenti sia dal punto di vista della tassatività, quanto della determinatezza.

5. Diritto alla sicurezza *vs* diritto alla riservatezza

Nella prospettiva volta alla realizzazione di «uno spazio comune di giustizia» attraverso il rafforzamento della cooperazione giudiziaria e di polizia, il Programma dell'Aia e il rispettivo Piano di attuazione focalizzano l'attenzione su due punti nevralgici destinati a condizionare le successive iniziative *in subiecta materia*: da un lato, il principio di disponibilità diviene criterio-guida della disciplina della trasmissione di informazioni tra le autorità di *intelligence* e giudiziarie degli Stati membri, dall'altro lato, la previsione di un sistema operativo che consenta l'accesso reciproco e diretto dei singoli Stati ai *databases* nazionali viene ancorata alla indispensabile predisposizione di adeguate garanzie per la tutela delle notizie a carattere personale.

Cooperazione giudiziaria e corruzione internazionale, cit., p. 288.

35 Pubblicata in *GUUE*, L 164, 22 giugno 2002, p. 3.

36 Si tratta di una trasmissione con finalità di prevenzione, differenziandosi, quindi, quanto ad ambito di applicazione, dalla decisione n. 671 del 2005 che prevede la trasmissione di informazioni ai fini investigativi.

La necessità di operare un bilanciamento tra cooperazione informativa e tutela del dato, in un'ottica di superamento della tradizionale contrapposizione tra esigenze di sicurezza e garanzie individuali, trova accoglimento, all'interno dell'Unione europea, inizialmente, nella predisposizione di due coeve proposte di decisione quadro del 2005, di cui una volta ad attuare il principio di disponibilità e l'altra, quale indispensabile *pendant*, afferente alla materia del trattamento delle informazioni personali[37]. Per lungo tempo sono state disattese le sollecitazioni volte ad accelerare l'attuazione della seconda proposta in via prioritaria rispetto agli strumenti deputati a regolare lo scambio di informazioni nell'ottica della disponibilità[38], creando una disciplina poco organica in seno al perimetro del cd. terzo pilastro[39].

Va, dunque, apprezzata l'adozione della decisione quadro 2008/977/GAI[40], diretta alla regolamentazione e protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, che sembrerebbe poter fornire qualche preziosa indicazione circa il regime da applicarsi anche ai dati in esame, benché debba evidenziarsi la sua natura puramente residuale in quanto il considerando n. 39 della decisione quadro precisa che «questa dovrebbe lasciare impregiudicata la pertinente serie di disposizioni sulla protezione dei dati» degli atti adottati a norma del titolo VI del trattato sull'Unione europea, che contengono norme specifiche riguardanti la protezione dei dati, fra cui le disposizioni di protezione dei dati che disciplinano il trasferimento automatizzato tra Stati membri di profili DNA, dati dattiloscopici e dati nazionali di immatricolazione dei veicoli.

Per tale via, *iuxta* l'impostazione adottata dal Consiglio, tuttavia, la protezione del dato personale, nella duplice dimensione di diritto soggettivo dell'interessato all'autodeterminazione informativa e alla riservatezza, da un lato, e di strumento di tutela oggettiva che consenta il controllo sulla genuinità del dato, dall'altro

---

37 V. *supra*, S. Ciampi, *op. cit.*, § 4-5.

38 Nel *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (COM (2005) 475 def.)*, 19 dicembre 2005, in *GUUE*, C 47, 25 febbraio 2006, p. 27, si era sottolineata la necessità che l'entrata in vigore dell'iniziativa *de qua* precedesse l'adozione delle decisioni relative allo scambio di informazioni e *intelligence* tra gli Stati membri.

39 In particolare, non si applicano al "terzo pilastro" la direttiva 95/46/CE e il Regolamento (CE) n. 45/2001, recanti i principi fondamentali in materia di tutela dei dati. Di conseguenza, i sistemi informativi operanti nel settore della cooperazione giudiziaria di polizia, non potendosi richiamare ad un quadro giuridico unitario in materia di protezione dei dati, risultano vincolanti esclusivamente agli atti esplicitamente richiamati. Così, la Convenzione di applicazione Schengen contiene un rinvio espresso, a tutela dei dati gravitanti all'interno del SIS (Sistema Informativo Schengen), ai principi stabiliti dalla Convenzione del Consiglio d'Europa n. 108/1981 e dalla Raccomandazione R 15(87); analogo richiamo è contenuto nella Convenzione istitutiva Europol. Per ulteriori considerazioni si rinvia a F. Decli - G. Marando, *op. cit.*

40 In *GUUE*, L 350, 30 dicembre 2008, p. 60.

lato, si candida ad assumere il ruolo primario di condizione necessaria all'attuazione del principio di disponibilità.

In ambito europeo, la decisione 2008/615/GAI, fa proprio, dunque, il disegno di reciproca compenetrazione tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati affiorante dal Piano di attuazione del Programma dell'Aia.

Le disposizioni inerenti alla protezione delle informazioni personali sono contenute, infatti, in un coacervo di norme (artt. 24 sg.) che trova collocazione successiva rispetto a tutte le fattispecie regolanti la trasmissione di dati contemplati dal provvedimento. La scelta di ordine sistematico conferma la conclusione, già ricavabile, fra l'altro, sul piano dell'esegesi interpretativa, secondo cui le norme in tema di tutela dei dati personali parrebbero applicabili a tutti gli scambi di informazioni, sia spontanei che a richiesta, normativamente previsti dalla decisione e, nell'ambito peculiare della trasmissione dei dati DNA, ad entrambe le fasi del sistema del doppio binario informativo disciplinato dagli artt. 2 sgg.[41].

In particolare, l'art. 25 si propone di assicurare l'osservanza del *corpus* normativo di tutela della riservatezza subordinando l'applicabilità dei meccanismi di scambio di informazioni a due condizioni cumulative: per un verso, si richiede che le legislazioni degli Stati membri rispettino gli *standard* di garanzia offerti dalle fonti di diritto internazionale vigenti in materia, e segnatamente la Convenzione del Consiglio d'Europa del 28 gennaio 1981 ed il relativo Protocollo addizionale dell'8 novembre 2001, nonché la Raccomandazione n° R (87) 15 del Comitato dei Ministri del Consiglio d'Europa; per altro verso, nell'ottica della disponibilità, condizione di legittimità dello scambio di informazioni è che i Paesi membri abbiano dato attuazione interna al complesso di norme sulla protezione dei dati contenute nel Capo VI della decisione, assegnando, così, una posizione prioritaria alle disposizioni concernenti la tutela della privacy rispetto all'attuazione dello scambio di informazioni, garantendone, parimenti, l'effettività[42].

Il quadro normativo di protezione del dato si sviluppa in due direzioni complementari.

---

41 Qualche dubbio si sarebbe potuto profilare in relazione alla trasmissione dell'indice di riferimento in esito alla prima fase del doppio binario. Tuttavia, qualora si accolga la nozione di «dato personale» fornita dalla direttiva 95/46/CE, recepita anche dall'art. 2 della proposta di decisione–quadro del Consiglio del 4 ottobre 2005, ai sensi della quale per dato personale si intende «qualsiasi informazione concernente una persona fisica identificata o identificabile [...]», diviene inevitabile concludere per la classificazione dell'indice di riferimento nell'alveo dei dati a carattere personale.

42 In base all'art. 25, par. 2, il rispetto delle condizioni *de quibus* è verificato dal Consiglio che decide all'unanimità. Va ricordato, peraltro, come il par. 3 preveda una deroga per gli Stati membri in cui la trasmissione di dati personali sia già stata avviata a norma del Trattato del 27 maggio 2005 fra il Regno di Belgio, la Repubblica Federale di Germania, il Regno di Spagna, la Repubblica Francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria.

Il primo profilo attiene alla tutela dell'autodeterminazione informativa – sia dello Stato che detiene il dato sia della persona fisica interessata – al fine di rendere possibile il controllo sulle fasi di trasmissione e utilizzo dell'informazione e garantirne, per questa via, la genuinità e l'attualità. Su tale versante, viene in gioco la dimensione oggettiva della protezione della qualità dell'elemento oggetto di scambio, nella raggiunta consapevolezza che la disponibilità on-line degli archivi nazionali potrà realizzare tanto più un effettivo rafforzamento della cooperazione di polizia quanto più i dati in essi contenuti siano veritieri e controllabili.

Così, si prevede che le informazioni possano venir impiegate solo per gli scopi per cui sono state trasmesse (art. 26) e solo dall'autorità, dagli organi e dai tribunali competenti a procedere per realizzare le finalità per le quali le informazioni sono rese disponibili (art. 27). Tuttavia, lo Stato membro che gestisce lo schedario può autorizzare il trattamento per scopi diversi o ammettere la comunicazione ad altre autorità, purché il trattamento sia consentito dal diritto interno (art. 26, par. 1). Il rispetto della legislazione nazionale vale, altresì, per il Paese destinatario.

Inoltre, gli Stati membri debbono osservare una serie di obblighi inerenti alla tutela della qualità e alla conservazione del dato.

Sotto tale aspetto, essi devono, in primo luogo, garantire la genuinità del dato sotto il profilo della sua esattezza e attualità (art. 28). Qualora, su segnalazione della persona interessata o d'ufficio, l'informazione dovesse, infatti, rivelarsi inesatta o non più aggiornata, o qualora sia stato trasmesso un dato che non poteva essere reso disponibile, gli Stati membri interessati devono essere informati e sono tenuti a procedere alla sua rettificazione o cancellazione (art. 28, par. 1). Nel caso in cui non sia possibile controllarne l'attendibilità, il dato deve essere contrassegnato[43]. L'apposizione dell'indicatore di validità, che avviene allorché l'esattezza del dato è contestato dalla persona interessata e quando non è possibile stabilire se siano corretti o inesatti, è disciplinato, con rinvio, in base al diritto nazionale del Paese membro. Deve sottolinearsi che l'informazione – ancorché di "dubbia attendibilità" – rimane, comunque, indicizzata, quindi, non limitata nel suo trattamento.

Proprio tale aspetto meriterebbe, forse, una maggiore attenzione da parte del legislatore europeo e quello nazionale, attese le implicazioni derivanti sul soggetto interessato dal lato impiego che le nuove forme di cooperazione e di circolazione consentono.

Peraltro, la sua rimozione potrà avvenire solo previo consenso dell'interessato o su decisione del Tribunale o dell'autorità competente in materia di controllo della protezione dei dati (art. 28, par. 2). Con apposita norma di chiusura, si prevede, poi,

---

43 Giova ricordare che la previsione *de qua* coincide con la "caratterizzazione", contenuta nella decisione quadro n. 977 del 2008, in tema di tutela di dati personali, e definita come il contrassegno dei dati personali memorizzati senza l'obiettivo di limitarne il trattamento in futuro (art. 2): sul punto, si veda, ancora, S. Ciampi, *op. cit.*, § 5.

il dovere dello Stato di provvedere alla cancellazione delle informazioni allorquando esse non risultino più necessarie ai fini per cui sono state richieste o, in ogni caso, allo scadere del termine massimo previsto dal diritto interno (art. 28, par. 3).

La decisione 2008/615/GAI annovera, poi, una nuova tipologia di dati: le informazioni cd. «bloccate», caratterizzate dal fatto che il dato non può essere cancellato, in quanto tale attività pregiudicherebbe gli interessi della persona interessa. Merita osservare come tale tipologia di dati possa, comunque, venir utilizzata e trasmessa, anche se per le sole finalità che ne hanno impedito la cancellazione.

In secondo luogo, gli Stati devono tutelare la protezione e la sicurezza dei dati da ogni forma di distruzione, perdita o divulgazione non autorizzata (art. 29).

In terzo luogo, i Paesi dell'Unione devono garantire un adeguato controllo del percorso di trasmissione, ricezione e utilizzo del dato, sia nei casi in cui il trasferimento venga reso in forma non automatizzata, sia nel caso in cui la consultazione avvenga on-line (art. 30). Nel primo caso, l'invio e la ricezione del dato devono essere documentati con atto che contenga l'indicazione dell'oggetto dell'informazione, della data dell'accesso, del motivo della trasmissione e dell'autorità richiedente. Nel secondo caso, si prevede che l'accesso on-line possa essere effettuato solo dai funzionari dei punti di contatto predisposti *ad hoc* e sia debitamente registrato. La registrazione indica, infatti, il contenuto dell'informazione, la data e l'ora dell'accesso, l'indicazione dell'autorità richiedente e dell'autorità che gestisce i dati. Comune a entrambe le previsioni è la norma di garanzia che stabilisce un onere di registrazione di tali dati sia in capo alla Parte richiedente che in capo alla Parte ricevente, al fine di renderne possibile il successivo controllo riservato alle autorità nazionali competenti in materia di protezione dei dati, sulla sussistenza dei presupposti di legittimità delle trasmissioni. Il procedimento di controllo è, in ogni caso, attivato su domanda della persona interessata o d'ufficio, da parte dell'autorità nazionale competente, sulla base dei *dossier* relativi ai dati oggetto di trasmissione (art. 30, par. 5).

Il secondo profilo della disciplina relativa alla protezione dei dati si propone di garantire il diritto soggettivo della persona interessata alla tutela delle informazioni personali, sia nella prospettiva – di segno positivo – della "autodeterminazione" informativa, assicurando al soggetto la possibilità di controllare la veridicità, l'aggiornamento, la circolazione e l'uso delle informazioni che lo riguardano, sia nella componente – di segno negativo – della riservatezza, prescrivendo l'esclusione di alcuni dati dalla categoria delle informazioni accessibili e assicurando il riconoscimento del cd. diritto alla cancellazione del dato[44].

---

44 I due aspetti fondamentali compresi nell'alveo del diritto alla protezione dei dati personali sono evidenziati, fra gli altri, da: A. Baldassarre, "Diritti inviolabili", in *Enciclopedia Giuridica Treccani*, XI, Roma, Istituto dell'Enciclopedia Italiana, 1989, p. 20; S. Rodotà, "Tecnologie dell'informazione e frontiere del sistema socio-politico", in *Banche dati, telematica e diritti della persona*, a cura di G. Alpa e M. Bessone, Padova, Cedam, 1984, p. 93; *adde*, più di recente, C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un diritto comune europeo*, in "Diritto penale e processo", 2007, p. 385.

Così, l'art. 31 della decisione stila un catalogo di diritti di informativa e di impulso all'autorità competente, che si aggiungono alla facoltà del soggetto, prevista dall'art. 28, di richiedere allo Stato di verificare la correttezza e l'aggiornamento dei dati oggetto di trasmissione, al fine di operarne la rettifica, la cancellazione o l'apposizione del contrassegno, nonché alla possibilità di adire, ai sensi dell'art. 39, l'autorità nazionale al fine di attivare il procedimento di controllo sulla legittimità delle trasmissioni.

In particolare, l'art. 31 garantisce alla persona coinvolta specifici diritti di conoscenza riguardo le notizie a lui relative, sulla loro origine, i destinatari, la base giuridica e proclama *expressis verbis* il diritto di ottenere la rettifica e la correzione dei dati errati o trattati illecitamente. In caso di violazione dei diritti di protezione, il soggetto interessato potrà adire congiuntamente un Tribunale indipendente e imparziale, come previsto dall'art. 6 Convenzione europea dei diritti dell'uomo, e un'autorità indipendente di controllo ai sensi dell'art. 28 della direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché la loro libera circolazione, e potrà ottenere una riparazione in forma specifica o un risarcimento per equivalente. La procedura viene regolata con rinvio al diritto nazionale.

Ad una prima analisi, la disciplina sulla tutela dei dati trasmessi nel quadro dello scambio fra gli Stati dell'Unione fin qui analizzata non sembrerebbe pienamente conforme ai parametri regolanti lo scambio di informazioni richiamati dall'art. 34, par. 1, del Trattato dell'Unione[45] e, più in generale, dei diritti fondamentali previsti dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, la regola in base alla quale il dato può essere trasmesso solo per uno scopo determinato (cd. il principio di finalità del trattamento[46]) stabilita all'art. 26 parrebbe trovare un'attuazione solo parziale non appena si ponga mente al fatto che, a tale proclamazione formale, segue la previsione, nel secondo periodo del primo paragrafo, della sua derogabilità da parte del legislatore interno, senza, peraltro, che l'operatività della deroga venga circoscritta a casi e modi tassativi. Come si comprende, dunque, la discrezionalità degli Stati, seppur vincolata al requisito dell'autorizzazione da parte dello Stato emittente e al rispetto della legislazione dello Stato ricevente, consente che la "circolarità" del dato, in quanto del tutto discrezionale, venga, di fatto, lasciata sostanzialmente intatta.

Inoltre, il testo del 23 giugno 2008 dedica, *sub* art. 28, un'ampia previsione normativa al tema della tutela della genuinità del dato, ma la qualità dell'infor-

---

45 Anche l'art. 34 del Trattato vincola gli Stati aderenti ad assicurare un livello di protezione dei dati che corrisponda a quello previsto dalla Convenzione del Consiglio d'Europa n. 108 del 1981, dal Protocollo dell'8 novembre 2001 e dalla Raccomandazione del Comitato dei ministri del Consiglio d'Europa n. R (87) 15.

46 Sul principio di scopo quale criterio guida cui deve informarsi il trattamento dei dati personali, si vedano, fra gli altri, i contributi di C. Fanuele, *op. cit.*, p. 392; P. Felicioni, *Accertamenti sulla persona e processo penale*, Milano, Ipsoa, 2007, p. 184.

mazione viene misurata esclusivamente in rapporto ai parametri della esattezza e dell'aggiornamento, senza che vengano menzionate le caratteristiche dell'adeguatezza, pertinenza e non eccessività, espressamente considerate, invece, dalla Convenzione n. 108 del 1981. La medesima disposizione prevede, inoltre, un sistema di controllo, da effettuarsi solo *ex post*, sulla correttezza e l'aggiornamento del dato trasmesso, con esclusione di qualsiasi previsione volta a consentire una verifica in via preventiva circa la sussistenza dei presupposti di legittimità della trasmissione che avrebbe consentito di realizzare un maggior grado di tutela dell'informazione di carattere personale e sensibile.

6. Le prospettive legislative dell'Italia

Volgendo lo sguardo alle modalità di attivazione dei meccanismi fin qui illustrati ed al compendio di norme di cui il nostro Paese dispone, si constata come in Italia non esiste ancora una (ufficiale) banca dati di analisi del DNA.

L'unica struttura simile a quella richiesta per il test del DNA è legata all'identificazione mediante l'impronta digitale, per cui le autorità italiane muovendosi sulla linea prospettica imposta dal Trattato, e sulla scorta degli approdi maturati in seno ai precedenti progetti legislativi miranti all'istituzione di una banca dati nazionale[47], nel luglio del 2008 hanno depositato al Senato il disegno di legge n. 905[48], volto a consentire l'adesione dello Stato italiano al Trattato.

Premesso che l'avvenuta emanazione della decisione 2008/615/GAI, rende più pressante provvedere, per questa via, alla creazione e alla conservazione di archivi nazionali on-line destinati a confluire in un unico *network* di banche dati direttamente consultabile dalle autorità interne degli Stati membri, non pare inopportuno esaminare – sommariamente e limitatamente agli aspetti contemplati nel presente lavoro[49] – il citato disegno di legge[50].

---

47 Tra i progetti legislativi particolare attenzione merita la Proposta di schema di disegno di legge recante "Norme per la istituzione dell'archivio centrale dei profili del DNA e del Comitato tecnico-scientifico di vigilanza", approvato dal Comitato Nazionale per la Biotecnologia e la Biosicurezza (CNBB) il 14 aprile 2005, pubblicato in P. Felicioni, *op. cit.*, pp. 219 sgg.

48 Il testo della proposta, presentata dai Ministri degli affari esteri, dell'interno e della giustizia, è consultabile all'indirizzo <http://www.senato.it/loc/link.asp?tipodoc=DDLPRES&leg=16&id=307774>.

49 Per un commento alle modifiche al codice di rito, cfr., anche per le più ampie indicazioni bibliografiche, C. Fanuele, *op. cit.*, p. 390; P. Felicioni, *op. cit.*, pp. 207 sgg; A. Santosuosso-G. Gennari, *Il prelievo coattivo di campioni biologici e i terzi*, in "Diritto penale e processo", 2007, pp. 395 sgg.

50 L'art. 36 della decisione 2008/615/GAI prevede (al par. 1) che «gli Stati membri adottano le misure necessarie per conformarsi alle disposizioni della presente decisione entro un anno dalla decorrenza degli effetti della presente decisione, fatta eccezione per le disposizioni del capo 2, per le quali le relative misure necessarie sono adottate entro tre anni dalla decorrenza degli effetti della presente decisione e della decisione del Consiglio relativa all'attuazione della

Tralasciando il Capo I, relativo alle disposizioni di autorizzazione all'adesione al Trattato, il Capo II focalizza l'attenzione sulla necessità di istituire un archivio genetico nazionale al fine di garantire alle autorità di *law enforcement* l'accesso diretto on-line ai dati in esso registrati, e, per tale via, di realizzare la condivisione delle informazioni (cd. *information sharing*) quale necessario presupposto di una più efficace cooperazione di polizia e giudiziaria, anche interna.

In particolare, sotto tale aspetto, viene prevista, su un primo versante, la creazione di due organismi paralleli all'interno dei quali si articolano e si suddividono le attività di trattamento dei dati genetici: in particolare, l'art. 5, comma 1, del disegno di legge istituisce la banca dati nazionale DNA, a carattere interforze, presso il Dipartimento della pubblica sicurezza del Ministero dell'Interno, mentre il successivo comma 2 prevede la creazione del Laboratorio centrale della banca dati DNA in seno al Dipartimento dell'amministrazione penitenziaria, presso il Ministero della giustizia.

La previsione di due strutture operative eterogenee consente di tenere distinte le attività di raccolta e comparazione dei profili DNA, riservate alla banca dati (art. 7), dalle operazioni di estrazione dei profili e di conservazione dei campioni biologici, di competenza esclusiva del Laboratorio (art. 8). La condivisibile scelta di operare un *distinguo* tra la sede delle attività di estrazione dei profili DNA dai campioni biologici, da un lato, e il luogo di raccolta e raffronto dei dati, dall'altro lato, risponde alla finalità di tutelare la genuinità dei dati raccolti e di evitare contaminazioni tra le diverse *species* di informazioni trattate.

In linea con le indicazioni precedentemente formulate, l'analisi dei campioni genetici, quale attività necessariamente prodromica rispetto alla registrazione dei profili all'interno della banca dati ai fini consultivi, deve essere condotta nel rispetto delle garanzie di cui all'art. 11, comma 3: la norma prevede che l'attività di analisi ed estrazione del profilo, da effettuarsi unicamente nei laboratori certificati, possa essere svolta esclusivamente sui segmenti non codificanti del genoma umano, da cui non siano, pertanto, desumibili informazioni sul soggetto analizzato, quali, ad esempio, le patologie genetiche e le caratteristiche ereditarie.

La medesima *ratio* di garanzia informa la disciplina della successiva attività di consultazione della banca dati. Disciplinata all'art. 12, comma 1, la regola del trattamento dei dati, l'accesso e la tracciabilità dei campioni è informata al principio del doppio binario informativo, vale a dire dell'accesso di "secondo livello".

All'evidente fine di garantire che l'accesso all'archivio on-line non consenta di pervenire direttamente ai dati identificativi della persona interessata, ma solo ai dati di indice relativi alla sussistenza del profilo all'interno della banca dati, si dispone *expressis verbis* che i profili DNA ed i relativi campioni non permettono

---

presente decisione». La deroga si riferisce, appunto, alle norme che disciplinano l'«accesso in linea e seguito delle richieste» relative ai profili del DNA, dato dattiloscopici, dati di immatricolazione dei veicoli.

l'identificazione diretta del soggetto cui si riferiscono, nel pieno rispetto dell'art. 2 del Trattato, inerente al carattere anonimo dei profili inseriti all'interno della banca dati.

In pratica, la polizia giudiziaria ovvero l'autorità giudiziaria dovranno prima richiedere di effettuare il confronto e, solo se questo è positivo, potranno essere autorizzati a conoscere il nominativo del soggetto cui appartiene il profilo, garantendo, parallelamente, le esigenze di tutela e privacy, che anche la decisione europea intende soddisfare, e la fruizione delle informazioni.

Su un altro versante, il disegno di legge si preoccupa di fornire una risposta alle questioni esegetiche che riguardano l'individuazione dei soggetti deputati ad attingere alle informazioni contenute all'interno degli archivi.

In particolare, premesso che la trasmissione delle informazioni avverrà per il tramite dei punti di contatto nazionali, l'art. 12, comma 2, del testo identifica le autorità autorizzate a compulsare la banca dati, di cui si prevede la costante tracciabilità, stabilendo, fra l'altro, che le richieste potranno pervenire unicamente dalle Forze di polizia, dall' autorità giudiziaria – da intendersi, in ragione della natura dell'attività, comprensiva tanto del pubblico ministero quanto del giudice – e, nei limiti della legislazione, dai difensori (artt. 391-*bis* sgg. c.p.p.), mentre l'accesso al laboratorio, in ragione della maggiore delicatezza delle attività svolte, è consentito alla polizia giudiziaria solo previa autorizzazione del magistrato. In entrambi i casi, la consultazione avviene esclusivamente per finalità di identificazione personale nonché per finalità di collaborazione internazionale di polizia. La precisazione consente, pertanto, di riferire tali operazioni all'ambito delle attività preprocedimentali di polizia e procedimentali in senso stretto.

Un secondo profilo concerne gli elementi di alimentazione della banca dati: come premesso, il punto non è stato direttamente affrontato dalla decisione 2008/615/GAI, che si limita a distinguere i profili riferibili ad un soggetto determinato dalle cd. tracce aperte, ovvero insuscettibili di identificazione, nulla disponendo in merito alle modalità di raccolta ed estrazione degli stessi. A tal proposito, il disegno di legge stila, invece, un catalogo di fonti, da cui è possibile ricavare il materiale biologico ai fini della tipizzazione dei relativi profili DNA e del loro inserimento negli archivi, in relazione a ciascuna delle quali sono stabilite specifiche modalità di acquisizione procedimentale.

In primo luogo, è prevista la possibilità di prelevare i campioni biologici da determinate categorie di soggetti, selezionati in base al denominatore comune di essere stati sottoposti a misure privative della libertà personale. Il potere di comprimere la libertà di soggetti indiziati o imputati nel corso del procedimento penale si dilaterebbe fino a comprendere, nell'ottica del legislatore, la facoltà del prelievo coattivo del campione biologico[51]. In particolare, ai sensi dell'art. 9, com-

51 Tuttavia, come sottolineato anche dal Garante europeo per la protezione dei dati, il prelievo di sostanze biologiche è misura di maggiore afflittività rispetto alle altre limitazioni della

ma 2, del disegno di legge, possono essere sottoposti al prelievo, volontario o coattivo, di sostanze biologiche i soggetti sottoposti a misure cautelari, precautelari e a misure di sicurezza detentive, e i soggetti cui sia stata applicata la detenzione, l'internamento, o una misura alternativa della detenzione a seguito di sentenza irrevocabile di condanna per un delitto non colposo.

A giustificare tale soluzione induce la considerazione, peraltro, poco conforme al sistema, che lo stato di restrizione più ampio – quello della libertà – dovrebbe comportare quella minore, che consiste nel prelievo coattivo del piccolo saggio di saliva.

Alcune limitazioni sono previste, tuttavia, in base alle categorie di reato per cui si procede. In ogni caso, deve trattarsi di procedimenti per delitti non colposi, per i quali sia consentito l'arresto in flagranza, con esclusione di un elenco di reati regolato per *nomen iuris* dall'art. 9, comma 2, e che contempla, per sommi capi, i delitti che non contengano tra i loro elementi costitutivi la violenza o la minaccia, i delitti contro la pubblica amministrazione, i delitti di falso, i reati fallimentari.

Una riduzione del potere di prelievo coattivo riconosciuto alla polizia giudiziaria è, poi, previsto dal comma 3, ai sensi del quale, in caso di arresto in flagranza o di fermo, l'estrazione del materiale biologico è consentita solo in seguito alla convalida da parte del giudice. S'introdurrebbe, così, una sorta di "autorizzazione" per lo svolgimento di atti invasivi della libertà personale, per loro natura "postumi".

Il procedimento di acquisizione dei campioni biologici dei soggetti privati della libertà personale trova, infatti, specifica disciplina nei commi 3 e 4 dell'art. 9, in cui si prevede che il prelievo venga effettuato dalle forze di polizia giudiziaria, anche mediante ausiliari, nel rispetto della dignità e della riservatezza del soggetto interessato. I campioni prelevati all'esito delle operazioni, di cui deve essere redatto apposito verbale, devono essere inviati a cura della polizia giudiziaria procedente al laboratorio centrale, per la tipizzazione e il successivo inserimento in banca dati.

In secondo luogo, viene in rilievo la possibilità di estrarre i profili dai reperti biologici, cioè dai materiali acquisiti dalla polizia giudiziaria sul luogo del reato o su cose pertinenti al reato, tipicamente all'esito delle attività di perquisizione o sequestro.

A tal fine, il legislatore, da un lato, pone a carico dell'autorità procedente che abbia richiesto – mediante accertamento tecnico, consulenza o perizia – la tipizzazione dei campioni biologici raccolti, il dovere di disporre la trasmissione dei profili alla banca dati DNA. Tale obbligo, per contro, non riguarda i campioni biologici

---

libertà personale previste dal codice di rito penale. Inoltre, la previsione è di dubbia conformità rispetto al canone di proporzionalità che, *in unum* con il principio di scopo, informa la materia del trattamento dei dati e implica che possano essere sottoposti a prelievo di materiale genetico solo i soggetti imputati o gravemente indiziati di delitti a particolare allarme sociale, quali quelli contro la pubblica incolumità. In merito, si veda, C. Fanuele, *op. cit.*, p. 393; R. E. Kostoris, "Prelievi biologici coattivi", in *Contrasto al terrorismo interno e internazionale*, cit., p. 329.

prelevati in seguito ad attività di ispezioni corporali volontarie o coattive. Dall'altro lato, a seguito del passaggio in giudicato della sentenza, il pubblico ministero legittimato ai sensi dell'art. 655, comma 1, c.p.p. ha la mera facoltà di richiedere al giudice dell'esecuzione di disporre l'attività di tipizzazione e trasmissione dei reperti, che non siano mai stati analizzati nel corso del procedimento (art. 10).

In terzo luogo, è consentito il prelievo di materiale biologico sui cadaveri non attribuiti ad alcuno, al fine di consentirne l'identificazione: in tal caso, il procedimento di acquisizione dei profili ricalca quello delineato per il prelievo dai reperti biologici, in linea con quanto pretende, allo stato dell'arte, la legislazione sovranazionale.

Sul diverso fronte della tutela dei dati, il progetto prevede un *corpus* di norme volte a tutelare sia il profilo positivo del diritto alla privacy, inerente all'autodeterminazione informativa e al controllo sulla circolazione del dato, sia il profilo negativo della riservatezza del soggetto interessato, cui attiene la problematica afferente alla conservazione e alla cancellazione dei dati.

Per quanto attiene al primo profilo, l'art. 12, comma 3, – come si è anticipato – prevede che il trattamento e l'accesso alle informazioni contenute negli archivi possa essere effettuato dal personale a ciò autorizzato, in modo tale da garantire la verifica «costante» del dato, assicurando sia l'identificazione dell'operatore sia la registrazione delle attività concernenti i profili e i campioni, in linea con quanto stabilisce l'art. 30 della decisione 2008/615/GAI che impone la tracciabilità «oggettiva» dell'invio (il motivo della trasmissione; i dati trasmessi; la data della trasmissione) e quella «soggettiva» (la denominazione o il codice di riferimento dell'autorità che effettua la consultazione e dell'autorità che gestisce lo schedario).

Per quanto riguarda l'aspetto legato alla conservazione dei dati, il disegno di legge opera un bilanciamento tra il buon funzionamento della banca dati – la cui efficienza, fisiologicamente collegata al fenomeno della recidiva, dipende dal fatto che quanto più il dato viene conservato in archivio tanto più aumentano le probabilità di identificazione delle tracce aperte – e l'opposta *ratio* di garanzia della riservatezza della persona interessata.

L'art. 13, comma 4, prevede, con apposita norma di chiusura, che i termini massimi di conservazione dei profili DNA e dei relativi campioni, da determinarsi in concreto con apposito regolamento attuativo, non possano superare, rispettivamente, i quaranta e i venti anni dall'ultima circostanza che ne ha determinato l'acquisizione.

Sebbene la scelta temporale regga – come si è anticipato – sul rilievo che le continue evoluzioni delle tecniche di tipizzazione e confronto possono rendere necessaria la sua disponibilità onde effettuare delle nuove analisi ogniqualvolta si rendesse disponibile una innovazione in tal senso, va evidenziato che se il *dies a quo* appare eccessivamente generico, è lecito chiedersi, per quanto attiene il *dies ad quem*, se un termine così ampio possa dirsi conforme al principio di proporzionalità, espresso all'art. 5 della decisione quadro 2008/977/GAI, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di

polizia in materia penale – a mente del quale «sono previsti adeguati termini per la cancellazione dei dati personali o per un esame periodico della necessità della memorizzazione dei dati» – e recepito a livello nazionale dal d.lgs. 30 giugno 2003, n. 196, secondo cui i dati possono essere conservati per il tempo necessario al raggiungimento dello scopo perseguito.

Dovrà provvedersi alla cancellazione in ogni caso, anche d'ufficio, prima della scadenza dei termini massimi, dei profili e dei campioni prelevati dai soggetti *ex* art. 9 a seguito di sentenza definitiva di assoluzione nel merito con formula liberatoria (art. 13, comma 1) e dei profili di cui all'art. 7, lett. *c*), a seguito di ritrovamento di persona scomparsa o di identificazione del cadavere, essendo raggiunto lo scopo a cui tende la loro conservazione.

Parrebbe rispondere, invece, ad una logica sanzionatoria, la cancellazione del profilo DNA e la distruzione del relativo campione stabilita all'art. 13, comma 3, ogniqualvolta risulti che le operazioni di prelievo siano state eseguite in violazione del protocollo indicato all'art. 9.

Gli organi preposti al controllo della banca dati e del laboratorio sono, infine, individuati, rispettivamente, nel Garante per la protezione dei dati, che esercita tale funzione nell'ambito delle attribuzioni previste dal d. lgs. n. 196 del 2003, e nel Comitato nazionale per la biosicurezza e le biotecnologie (art. 15): la scelta normativa merita piena condivisione, trattandosi di due istituzioni capaci di offrire la tutela, la più ampia, d'imparzialità nell'espletamento del ruolo di garanzia circa l'osservanza delle norme di sicurezza, in quanto esse si pongono, fra l'altro, come autonome ed estranee rispetto all'attività di raccolta dei dati prefigurata dal disegno di legge e, quindi, conformi a quanto pretende, sul punto, l'art. 30, par. 4, della decisione GAI n. 615 del 2008.

Nel Capo III del provvedimento italiano si dà, poi, attuazione alle forme di cooperazione di polizia ulteriori e residuali, che impongono la condivisione di informazioni on-line tra gli Stati aderenti all'Unione e che la decisione europea contempla agli artt. 17 e 18, in termini di «operazioni congiunte, assistenza in occasioni di assembramenti, catastrofi e incidenti gravi» per le quali è ammesso «uso di armi, munizioni e attrezzature» (art. 19).

In conclusione, com'è emerso, il testo sommariamente esaminato, salvo piccole discrasie, si pone prevalentemente in linea con il quadro tratteggiato a livello europeo, per cui sembra ormai opportuna ed improrogabile la sua adozione. A sollecitare in tal senso, induce, sul versante interno, la constatazione dell'assoluta rilevanza che i dati in esame paiono acquisire ormai non solo ai fini dell'accertamento giudiziale, ma anche in quanto elementi fondamentali per la stessa instaurazione dei processi.

Il casellario giudiziario europeo: una frontiera dell'integrazione in materia penale

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

SOMMARIO: 1. La genesi dell'idea nell'ambito del Consiglio d'Europa. – 2. Il dibattito sul casellario giudiziario europeo nel contesto dell'Unione europea. – 3. L'inefficienza dei tradizionali meccanismi di assistenza giudiziaria. – 4. Il Libro bianco del 2005: modelli di casellario europeo e utilizzazione delle informazioni sulle condanne all'estero. – 5. Una razionalizzazione dell'esistente: la decisione n. 876 del 2005. – 6. Il progetto pilota di interconnessione dei casellari giudiziari. – 7. La decisione quadro relativa all'organizzazione e al contenuto degli scambi di informazioni estratte dal casellario giudiziario. – 8. La decisione istitutiva del sistema europeo di informazione sui casellari giudiziari (ECRIS). – 9. Lo studio di fattibilità di uno schedario di condannati cittadini di paesi terzi. – 10. La decisione quadro sulla considerazione delle pronunce di condanna in occasione di un nuovo procedimento penale. – 11. Riflessioni conclusive.

1. La genesi dell'idea nell'ambito del Consiglio d'Europa

Lo scambio tra Stati di informazioni estratte dal casellario giudiziale viene tradizionalmente considerato una forma di mutua assistenza in materia penale. Diverse sono, infatti, le Convenzioni che prevedono meccanismi di trasferimento dei dati relativi al curriculum criminale: tanto a livello mondiale – si pensi solo alla Convenzione sulla soppressione del traffico di persone e lo sfruttamento della prostituzione oppure alla Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale[1] –, quanto a livello regionale. Per quel che riguarda l'Europa, la fonte primaria in materia è costituita senza dubbio dalla Convenzione europea di assistenza giudiziaria in materia penale, predisposta nell'ambito del Consiglio d'Europa e firmata nel 1959.

Essa contempla due diversi meccanismi vòlti a garantire la conoscenza dei precedenti penali anche in un ordinamento diverso da quello in cui il soggetto è stato condannato. Da un lato, l'art. 22 – così come modificato dall'art. 4 del Protocollo addizionale del 1978 – prevede lo strumento della notifica a iniziativa dello Stato di condanna: almeno una volta all'anno, questo invia allo Stato di cittadinanza le informazioni relative alle «sentenze penali e [alle misure posteriori che concernono i cittadini di questa Parte e che sono state iscritte nel casellario giudiziale». Dall'altro lato, l'art. 13 disciplina la comunicazione su richiesta: statuisce, infatti, che «la Parte richiesta trasmetterà, nella misura in cui le sue autorità giudiziarie potranno ottenerli esse stesse in un caso simile, gli estratti del casellario giudiziale e tutte le informazioni relative al medesimo che le saranno chieste dalle autorità giudiziarie di una Parte Contraente per i bisogni di un affare penale».

Non è un caso, allora, che l'idea di un "casellario giudiziario europeo" si sia affacciata, agli inizi degli anni ottanta, proprio nell'ambito del Consiglio d'Europa. Più precisamente, nel 1978, il Comitato europeo per i problemi penali creò un Comitato ristretto sul casellario giudiziale e la riabilitazione dei condannati, in vista delle giornate organizzate dalla *Fondation Internationale Pénale et Pénitentiaire* sullo stesso tema[2]: il Comitato fu incaricato (tra l'altro) di «examiner les problèmes liés à l'utilisation des ordinateurs en matière de casier judiciaire» e «l'opportunité d'élaborer un modèle de casier judiciaire européen uniforme»[3]. Il

---

1 Per una compiuta rassegna delle Convenzioni internazionali che dedicano un qualche spazio allo scambio di estratti del casellario, v. M. Plachta, *Criminal Records in an Era of Globalization: Identifying Problems and Conceptualizing Solutions within the European Union*, in "International Criminal Law Review", 2007, pp. 427 sgg. Interessanti spunti storici si trovano in M. Pisani, *Per un casellario giudiziario su dimensioni internazionali*, in "Rivista italiana di diritto e procedura penale", 2006, p. 1152.

2 Gli atti di tali giornate di studio sono pubblicati nel volume *Casier judiciaire et rehabilitation: actes des Journees de Neuchatel* (Neuchatel, 30 aout-1er september 1979), Neuchatel, Editions Ides et calendes, 1982.

3 V. *Rapport final d'activité. Le casier judiciaire et la rehabilitation de condamnés*, Strasburgo, 8 maggio 1984, p. 3.

Comitato prese in considerazione due possibilità. Anzitutto, quella consistente nella creazione di un vero e proprio «casier judiciaire européen» in seno al Consiglio d'Europa o a un altro organismo indipendente: una soluzione giudicata «la plus efficace pour la centralisation des informations et la communication rapide de celles-ci aux autorités intéressées»[4]. In secondo luogo, valutò la prospettiva dell'«intercommunication des casiers judiciaires informatisés des Etats membres». Entrambe le strade furono, però, ritenute impraticabili: la prima presentava ostacoli insormontabili dal punto di vista metodologico (dipendenti dalle differenze di definizione dei reati, dall'eterogeneità linguistica) e finanziario, mentre la seconda venne giudicata prematura, in quanto l'informatizzazione dei casellari nazionali era ancora agli albori[5].

Se i tempi non erano ancora maturi per la realizzazione del progetto, neanche nella sua versione meno ambiziosa, il Comitato presentò nell'aprile del 1984 un progetto di raccomandazione, che poi venne recepito dal Comitato dei Ministri. Il 21 giugno 1984 fu infatti adottata la *Recommandation R(84)10 sur le casier judiciaire et la réhabilitation des condamnés*, la quale perseguiva due obiettivi precisi.

Il primo era quello di fissare alcune garanzie fondamentali circa la disciplina in materia, sulla scorta della considerazione che «l'institution du casier judiciaire vise principalement à informer les autorités responsables du système de justice pénale sur les antécédents du justiciable en vue de faciliter l'individualisation de la décision à prendre» e che «tout autre usage du casier judiciaire peut compromettre les chances de réinsertion sociale du condamné».

Il secondo obiettivo consisteva invece proprio nella riaffermazione della «necessité de promouvoir une collaboration étroite entre les Etats membres du Conseil de l'Europe». Esattamente in quest'ottica, la Raccomandazione R(84)10 invitava i Governi «à appliquer en fait strictement les obligations prévues aux articles 13 et 22 de la convention [européenne d'entraide judiciaire]» e a «examiner la possibilité de retirer les réserves formulées par rapport aux mêmes articles 13 et 22 de la convention» (punto 14). Inoltre, in una nota pubblicata successivamente alla Raccomandazione e relativa ai lavori del Comitato ristretto, venivano indicati i vantaggi derivanti dal casellario europeo e si configurava la sua creazione quale *condicio sine qua non* per la realizzazione – a livello di Consiglio d'Europa – di quell'ambizioso progetto – nato nell'ambito dell'Europa dei nove – dell'*espace judiciaire européen*[6].

---

4 V. ancora *Rapport final d'activité*, cit., p. 33.

5 Cfr. *Rapport final d'activité*, cit., pp. 33-34. Sulla genesi dell'idea del casellario giudiziario europeo nei lavori del Comitato ristretto, cfr. A. Spielmann, *Un casier judiciaire européen?*, in "Revue de science criminelle et de droit pénal comparé", 1984, pp. 633 sgg.

6 V., ancora, A. Spielmann, *op. cit.*, p. 649, secondo il quale, «s'il est vrai que l'idée d'un casier judiciaire européen ne dat pas d'hier, sa réalisation ne sera pas pour demain». Sulla genesi del concetto di "spazio giudiziario europeo", cfr., da ultimo, A. Weyembergh, *L'harmonisation des législations: condition de l'espace pénal européen et révélateur de ses tensions*, Bruxelles, Editions de l'Université de Bruxelles, 2004, p. 13.

2. Il dibattito sul casellario giudiziario europeo nel contesto dell'Unione europea

A distanza di meno di vent'anni, l'idea del casellario giudiziale europeo è stata ripresa proprio nel contesto della rinnovata Unione europea. Con il superamento dei confini e l'affermazione del principio fondamentale della libera circolazione delle persone, si è posto con forza il tema della circolazione delle informazioni riguardanti la storia criminale degli individui: se una persona può liberamente spostarsi da un Paese all'altro e delinquere in qualsiasi Stato membro, è logico che «son passé judiciaire doit pouvoir être connu de l'ensemble de juridictions des Etats concernés, afin que la justice répressive soit la plus efficace possible et joue pleinement son rôle de prévention d'un retour à la délinquance»[7]. In effetti, il rafforzamento della circolazione tra gli Stati membri delle informazioni relative alle condanne e alle interdizioni è divenuto uno dei cardini della cooperazione giudiziaria nello spazio di libertà, sicurezza e giustizia, delineato dal Trattato di Amsterdam.

Fin dalla fine degli anni novanta, la riflessione sul casellario europeo si è sviluppata seguendo due diverse direttrici.

La prima è quella rappresentata dalla lotta alla criminalità organizzata e al terrorismo. In due ricerche multidisciplinari effettuate nel 1999 e nel 2000 emergeva chiaramente l'importanza decisiva dello scambio di informazioni estratte dagli archivi nazionali ai fini della prevenzione e della repressione dei reati di criminalità organizzata[8]. Tali studi mettevano in luce l'inefficienza degli strumenti tradizionali di assistenza giudiziaria e suggerivano l'adozione di un vero e proprio *European Criminal Record* (ECR). Non a caso, nel documento che – all'inizio del nuovo secolo – disegnava la strategia dell'Unione europea sulla prevenzione e sul controllo della criminalità organizzata, si riprendeva l'invito a valutare «la

---

7 Queste le parole di B. Lapérou-Scheneider, "La mémoire de la justice: Interconnexion des casiers judiciaires et récidive à l'echelle européenne", in *Le nouveau droit de la récidive*, a cura di B. Lapérou-Scheneider, Parigi, L'Harmattan, 2008, p. 68.

8 Si allude, in particolare, allo studio realizzato nell'ambito del FALCONE Project JHA/1999/FAL/197, intitolato *The use of criminal records as a means of preventing organised crime in the areas of money laundering and public procurement: the need for Europe-wide collaboration* (lo studio è reperibile all'indirizzo <http://ials.sas.ac.uk/postgrad/docs/Falcone%20CR%20Vol1.pdf> ed è pubblicato in *Financial Crime in the EU. Criminal Records as Effective Tools or Missed Opportunities?*, a cura di C. Stefanou e H. Xanthaki, L'Aia, Kluwer Law International, 2005), e finalizzato all'analisi comparatistica in ordine all'esistenza, all'utilizzo dei casellari nazionali e alla loro accessibilità per finalità di verifica dei requisiti per l'assunzione nelle cosiddette *vulnerable professions* (cfr. H. Xanthaki, "Introduction: National Criminal Records as a Means of Combating Organised Crime", in *Financial Crime in the EU*, cit., pp. 1 sgg.). In secondo luogo, va segnalata la ricerca compiuta in seno al FALCONE Project JHA/2000/FAL/168, dedicato al tema "*A European Criminal Record as a means of combating organised crime*".

possibilità di ampliare e possibilmente formalizzare lo scambio di informazioni sui casellari giudiziali»[9].

La seconda direttrice è quella legata alla valorizzazione del canone del reciproco riconoscimento delle decisioni giudiziarie[10]. Com'è noto, dopo essere stato consacrato in materia civile e commerciale, esso è stato affermato per la prima volta in materia penale nel Consiglio europeo di Cardiff del 1998 ed è stato eletto ad asse portante della cooperazione giudiziaria in materia penale nelle conclusioni del Consiglio europeo di Tampere del 1999 (§ 33)[11]. Non sfuggirà come la precondizione fondamentale per riconoscere una decisione adottata in un altro Stato membro sia proprio quella di essere a conoscenza della decisione stessa. Proprio per questo, nell'ambito della Comunicazione sui progressi compiuti nella creazione di uno spazio di libertà, sicurezza e giustizia del 24 marzo 2000, la Commissione ha prospettato l'esigenza di ampliare e migliorare lo scambio di informazioni sui casellari giudiziari[12]. Successivamente, nella Comunicazione al

---

9 V. il documento *Prevenzione e controllo della criminalità organizzata. Strategia dell'Unione europea all'inizio del nuovo millennio*, in *GUCE*, C 124, 3 maggio 2000, p. 24.

10 V. A. Marandola, *Verso un casellario giudiziario europeo (o una variante di minor portata)*, in "Diritto penale e processo", 2007, p. 1379.

11 Cfr. *Le conclusioni della Presidenza. Consiglio europeo di Tampere*, in "Cassazione penale", 2000, p. 307. Del canone del reciproco riconoscimento come «chiave di volta della costruzione dello spazio giudiziario europeo» si parla nella *Comunicazione della Commissione al Consiglio e al Parlamento europeo sul reciproco riconoscimento delle decisioni giudiziarie in materia penale* (COM (2005) 195 def.), in "Rivista italiana di diritto e procedura penale", 2006, p. 378. Inoltre, quello che dovrebbe divenire – per effetto dell'entrata in vigore del Trattato di Lisbona – l'art. 69A del Trattato sull'Unione europea stabilisce che «la cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e include il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri». Sul principio del mutuo riconoscimento, v. almeno C. Amalfitano, "Spazio giudiziario europeo e libera circolazione delle decisioni penali", in *Cooperazione giudiziaria civile e penale nel diritto dell'Unione europea*, a cura di S.M. Carbone e M. Chiavario, Torino, Giappichelli, 2008, pp. 1 sgg.; G. De Amicis - G. Iuzzolino, *Guida al mandato d'arresto europeo*, Milano, Giuffrè, 2008, pp. 3 sgg.; D. Fiore, "Réflexions sur l'idée de la «confiance mutuelle»", in *Sécurité et justice: enjeu de la politique extérieure de l'Union européenne*, a cura di G. De Kerchove e A. Weyembergh, Bruxelles, Université de Bruxelles, 2003, p. 133; L. Moreillon – A. Willi-Jayet, *Coopération judiciaire pénale dans l'Union européenne*, Monaco, Bruxelles, Parigi, Helbing&Lichtenhahn, Bruylant, L.G.D.J., 2005, pp. 301 sgg.; A. Pasquero, *Mutuo riconoscimento delle decisioni penali: prove di federalismo. Modello europeo e statunitense a confronto*, Milano, Giuffrè, 2007, pp. 53 sgg.; B. Piattoli, *Cooperazione giudiziaria e pubblico ministero europeo*, Milano, Giuffrè, 2002, pp. 94 sgg.; *La confiance mutuelle dans l'espace pénal européen*, a cura di G. De Kerchove e A. Weyembergh, Bruxelles, Université de Bruxelles, 2005; nonché, *L'espace pénal européen: enjeux et perspectives*, a cura di G. De Kerchove e A. Weyembergh, Bruxelles, Université de Bruxelles, 2002; H. Satzger – F. Zimmermann, "From traditionalmodels of judicial assistance to the principle of mutual recognition: New developments of the actual paradigm of the European Cooperation in Penal Matters", in *European cooperation in penal matters: issues and perspectives*, a cura di M. Cherif Bassiouni, V. Militello, H. Satzger, Padova, Cedam, 2008, pp. 337 sgg.

12 In tal senso, la *Comunicazione della Commissione al Consiglio e al Parlamento europeo sul quadro di controllo per l'esame dei progressi compiuti nella creazione di uno spazio di "libertà, sicurezza e*

Consiglio e al Parlamento europeo sul riconoscimento reciproco delle decisioni definitive in materia penale, ha affermato che, non essendo disponibile alcun casellario giudiziale europeo, «sarebbe molto utile istituire tale registro europeo di sentenze penali definitive, nonché di procedimenti pendenti davanti ad autorità che decideranno sul merito della fattispecie»[13].

Ancora, nel Programma di misure per l'attuazione del principio del reciproco riconoscimento, la Commissione accordava un alto grado di priorità alla misura n. 2 consistente nell'«adozione di uno o più strumenti volti ad introdurre il principio secondo cui il giudice di uno Stato membro deve essere in grado di tener conto delle decisioni penali definitive rese negli altri Stati membri per valutare i precedenti penali del delinquente, prendere in considerazione la recidiva e determinare la natura delle pene e le modalità di esecuzione applicabili». In secondo luogo, auspicava la predisposizione di «un modello uniforme di richiesta di precedenti giudiziari tradotto nelle diverse lingue dell'Unione, basandosi sul modello elaborato in ambito Schengen» (misura n. 3). Infine, prevedeva la realizzazione di due studi di fattibilità vòlti a determinare il modo migliore per pervenire, tenendo pienamente conto delle esigenze in materia di libertà individuali e di protezione dei dati, all'informazione delle autorità competenti dell'Unione europea in merito: da un lato, «alle condanne penali pronunciate nei confronti di una persona» (misura n. 4); dall'altro «ai provvedimenti di decadenza, divieto e incapacità pronunciati negli Stati membri» (misura n. 21). In particolare, la Commissione demandava a tali studi il compito di «individuare il migliore tra i seguenti metodi: a) agevolazione degli scambi bilaterali d'informazioni; b) collegamento in rete degli archivi nazionali; c) costituzione di un vero e proprio archivio centrale europeo»[14].

Nello spazio tracciato da queste due direttrici, il dibattito si è sviluppato nei primi anni duemila. Da una parte, sono stati realizzati importanti studi sulla fattibilità, sia di un casellario europeo delle condanne[15], sia di una banca dati delle

---

giustizia" nell'Unione europea (COM (2000) 167 def.), 24 marzo 2000, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0167:FIN:IT:PDF>, p. 18.

13 Così, la *Comunicazione della Commissione al Consiglio e al Parlamento europeo. Riconoscimento reciproco delle decisioni definitive in materia penale* (*COM (2000) 495 def.)*, 26 luglio 2000, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0495:FIN:IT:PDF>, p. 7.

14 Cfr. *Programma di misure per l'attuazione del principio del reciproco riconoscimento delle decisioni penali*, in *GUCE*, C 12, 15 gennaio 2001, p. 16.

15 Cfr., in particolare, lo studio realizzato dall'*Institute for International Research on Criminal Policy* e confluito nel volume *Blueprint for an EU criminal records database: Legal, politico-institutional & practical feasibility*, a cura di E. De Busser, A. Dormaels, T. Vander Beken, G. Vermeulen, Anversa, Maklu, 2002; nonché la ricerca affidata dalla Commissione all'*Institute of Advanced Legal Studies*, intitolata *Comparative study into Member States' measures to prevent the penetration of legal entities by organised crime and terrorist groups* (DG.JAI-B2/2003/01) (il *Final Report*, realizzato da C. Stefanou e H. Xanthaki, è disponibile in rete all'indirizzo <http://ials.sas.ac.uk/postgrad/AGIS-035/Materials/StefanouXanthaki/ILE.pdf>; si v., in particolare, la raccomandazione n. 7).

investigazioni e dei procedimenti pendenti[16]; dall'altra, la Commissione si è fatta carico della necessità di migliorare gli strumenti di conoscenza dei precedenti penali non nazionali degli imputati, inserendo un'apposita disciplina nell'ambito della proposta di decisione quadro relativa al mandato europeo di ricerca delle prove (COM (2003) 688 def.)[17]. In tale progetto, la Commissione intendeva perseguire lo scopo di aumentare l'efficienza dei meccanismi di scambio delle informazioni sul curriculum criminale inquadrando la richiesta di precedenti penali nel mandato di ricerca della prova e richiedendo specificamente l'individuazione – da parte degli Stati membri – di un'autorità centrale del casellario incaricata di dare seguito ai mandati europei di richiesta di estratti del casellario giudiziario (art. 8).

Nondimeno, una forte accelerazione nell'attività normativa sul tema del casellario giudiziale europeo si è avuta solo a seguito di due tragici eventi[18].

Sul versante della lotta al terrorismo, un forte impulso è venuto dagli attentati di Madrid dell'11 marzo 2004. Prova ne sia che, nella Dichiarazione contro il terrorismo, adottata dal Consiglio Europeo a neanche due settimane di distanza dai fatti, si invitava espressamente il Consiglio a semplificare lo scambio di informazioni e di *intelligence* e a esaminare la misura consistente nella creazione di un registro europeo delle condanne e delle interdizioni (punto 5)[19]. Qualche giorno dopo, la Commissione indicava, tra le misure fondamentali da adottare nella lotta contro il terrorismo, proprio la creazione di un casellario giudiziario europeo e si impegnava a effettuare una proposta legislativa entro la fine del 2004[20].

Sul fronte del reciproco riconoscimento, una molla decisiva è giunta da un gravissimo fatto di cronaca accaduto nello stesso anno: ossia l'"*affaire* Fourniret". Si trattava di un soggetto che, dopo essere stato ripetutamente condannato in Francia per violenza sessuale nei confronti di minori, era stato assunto da una

---

16 Si tratta, in particolare, del *Feasibility study on the creation of a database on investigations and prosecutions* (AGIS Project JAI/2003/AGIS/002), coordinato da C. Stefanou e H. Xanthaki e disponibile all'indirizzo <http://ials.sas.ac.uk/postgrad/JAI__AGIS/pdf%20volume%201/AGIS%20 2003%20Vol%201.pdf>.

17 La proposta è pubblicata in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM :2003:0688:FIN:IT:PDF>.

18 Cfr. V. Havv, *Le casier judiciaire européen: vers une première décision*, in "Cahiers de droit europeen", 2005, p. 157.

19 Si legga il *Documento del Consiglio n. 7906/04*, 29 marzo 2004, <http://register.consilium. europa.eu/pdf/it/04/st07/st07906.it04.pdf>, p. 5.

20 V. *Comunicazione della Commissione al Consiglio e al Parlamento europeo relativa a talune azioni da intraprendere nel settore della lotta contro il terrorismo e altre forme gravi di criminalità, in particolare per migliorare gli scambi di informazioni (COM (2004) 221 def.)*, 29 marzo 2004, <http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0221:FIN:IT:PDF>, pp. 12 sgg. Cfr. anche la decisione 2005/671/GAI (adottata dal Consiglio nel settembre del 2005 e pubblicata in *GUUE*, L 253, 29 settembre 2005, p. 22), ove si riconosce che la complessità del fenomeno terroristico postula un rafforzamento dello scambio delle informazioni anche relative alle condanne (considerando n. 4 e art. 2, par. 3).

scuola in Belgio, nell'assoluta ignoranza della sua storia criminale[21]: questo caso – oltre a quello di Marc Dutroux – sconvolse l'opinione pubblica belga ed europea, e indusse a reclamare un tempestivo rafforzamento dello scambio di informazioni tra i Paesi membri[22].

Fu così che, nell'autunno del 2004, vennero presentate diverse iniziative. Nella sessione del Consiglio "Giustizia e affari interni" del 25 e 26 ottobre 2004, la Commissione avanzò una proposta di decisione relativa allo scambio di informazioni estratte dal casellario giudiziario (COM (2004) 664 def.)[23]; nemmeno due settimane più tardi, il Regno del Belgio depositò una proposta di decisione quadro relativa al riconoscimento e all'esecuzione nell'Unione europea dei divieti risultanti da condanne per reati sessuali ai danni di bambini, con lo scopo dichiarato di completare, nel settore specifico, la proposta di decisione del Consiglio[24]. In quest'ultimo progetto si prevedevano, infatti, da un lato, alcuni vincoli diretti a garantire la conoscenza dell'interdizione anche nello Stato diverso da quello della condanna[25] e, dall'altro, un meccanismo vòlto a dare esecuzione all'estero all'interdizione.

Nel frattempo, il Consiglio europeo del 4 e 5 novembre approvava il Programma dell'Aia. Un documento dal quale emerge chiaramente la consapevolezza che il rafforzamento della libertà, della sicurezza e della giustizia richiede «un approccio innovativo nei confronti dello scambio transfrontaliero di informazioni in materia di applicazione della legge», tanto che, secondo il Consiglio europeo, «il fatto che le informazioni attraversino le frontiere non dovrebbe più, di per sé, essere rilevante» (§ 2.1). In forza di tale premessa, sul versante del consolidamento della sicurezza, il Programma conia il principio di disponibilità delle informazioni[26]; mentre nella parte dedicata specificamente al rafforzamento della giustizia (e al reciproco riconoscimento), invita la Commissione a presentare «proposte per intensificare lo scambio di informazioni, sulla base degli estratti

---

21 Cfr. L. Salazar, "La costruzione di uno spazio penale comune europeo", in *Lezioni di diritto penale europeo*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2007, p. 421.

22 Cfr. R. Reichstein, *Eu Rules Out central Criminal Register*, <http://www.dw-world.de/dw/article/0,1433,1262357,00.html>; nonché, J. Dymond, *Widening the EU's criminal justice net*, <http://news.bbc.co.uk/2/hi/europe/5410518.stm>.

23 Cfr. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0664:FIN:IT:PDF>.

24 V. il *Documento del Consiglio n. 14207/04*, 5 novembre 2004, <http://register.consilium.europa.eu/pdf/it/04/st14/st14207.it04.pdf>. Va ricordato che il Regno di Danimarca, già nel 2002, aveva presentato una proposta volta all'adozione di una *Decisione del Consiglio sul rafforzamento della cooperazione tra gli Stati membri dell'Unione europea in materia di decadenza da diritti*, in *GUCE*, C 223, 19 settembre 2002, p. 17.

25 Due le norme rilevanti in tal senso: anzitutto, quella che prevedeva l'obbligo di iscrizione della decadenza nel casellario nazionale (art. 3); in secondo luogo, quella che imponeva allo Stato di condanna di trasmettere l'iscrizione dell'interdizione allo Stato richiedente (art. 4).

26 Su tale canone, cfr. ampiamente, *supra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea".

dei casellari giudiziari nazionali, in particolare per quanto riguarda le persone perseguite per reati sessuali» e per istituire «un sistema informatizzato di scambio di informazioni» (§ 3.3.1)[27].

3. L'inefficienza dei tradizionali meccanismi di assistenza giudiziaria

Come si è notato, la riflessione sul casellario giudiziale europeo ha preso le mosse da alcune ricerche interdisciplinari, le quali hanno avuto il merito di mettere a fuoco i due principali profili problematici nella materia dello scambio di informazioni sul passato penale dei cittadini degli Stati membri: da un lato, la notevole disomogeneità della disciplina adottata in tema di archivi delle condanne da parte degli Stati membri; dall'altro, l'inefficienza dei meccanismi tradizionali di circolazione delle informazioni. Questa duplice fotografia è stata ripresa dalla Commissione e posta a fondamento della parte ricognitiva di quel documento basilare che è il Libro bianco relativo allo scambio di informazioni sulle condanne penali e sull'effetto di queste ultime nell'Unione europea (COM (2005) 10 def.)[28].

Sotto il primo profilo, è stato posto in rilievo come gli Stati membri tengano registri nazionali, generalmente informatizzati e centralizzati. Il problema è che si registrano rilevanti divergenze, per quanto riguarda: *a.* il servizio responsabile della conservazione dei casellari giudiziali; *b.* il loro contenuto; *c.* i termini di cancellazione; *d.* le norme che disciplinano l'accesso ai dati.

L'autorità presso la quale sono conservati gli archivi varia: in Austria, Irlanda, Svezia e Gran Bretagna, i registri sono tenuti dalle autorità di polizia[29]; in Belgio, Danimarca, Finlandia, Francia, Germania, Grecia, Italia, Olanda, Repubblica Ceca, Slovenia, Spagna, Ungheria, la competenza è del Ministero della giustizia[30], men-

---

27 Cfr. *Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea*, in *GUUE*, C 53, 3 marzo 2005, p. 12.

28 Il *Libro bianco relativo allo scambio di informazioni sulle condanne penali e sull'effetto di queste ultime nell'Unione europea* è stato presentato dalla Commissione il 25 gennaio 2005 ed è disponibile all'indirizzo <http://eur-lex.europa.eu/LexUriServ/site/it/com/2005/com2005_0010it01.pdf>.

29 Al riguardo, cfr., rispettivamente, R. Kert, "The European Criminal Record in Austria", in *Towards a European Criminal Record*, a cura di C. Stefanou e H. Xanthaki, New York, Cambridge University Press, 2008, pp. 108 sgg.; A. Kjellgren, "National Criminal Records and Organised Crime in Sweden", in *Financial Crime in the EU*, cit., pp. 311 sgg.; T. Thomas, *Criminal Records. A Database for Criminal Justice System and Beyond*, New York, Palgrave Macmillan, 2007, pp. 27 sgg.; L. Webley, "The European Criminal Record in England and Wales", in *Towards a European*, cit., p. 292.

30 V. rispettivamente J. Simon, "Criminal Records and Organised Crime in Belgium", in *Financial Crime in the EU*, cit., p. 103; K.B. Hansen, "National Criminal Records and Organised Crime in Denmark", *ibidem*, p. 119; K. Mäkelä, "Criminal Records and Organised Crime in Finland", *ibidem*, p. 149; F. Havard, "Criminal Records and Organised Crime in France", *ibidem*, p. 177; L. Boellinger, "Criminal Records in Germany: A Case of Leniency", *ibidem*, p. 207; O. Andritsou, "Criminal Records and Organised Crime in Greece", *ibidem*, p. 222; M. Gavouneli – P. Traianos, "The European Criminal Record in Greece", in *Towards a European*, cit., p. 170;

tre in Lussemburgo e in Slovacchia, il casellario è conservato presso la Procura generale[31]. Evidentemente, tale discrepanza rischia di rendere oltremodo difficile la creazione di canali di comunicazione tra i diversi Stati membri[32].

Per quel che concerne il contenuto degli archivi, è stato riscontrato che soltanto i casellari di Austria, Belgio, Cipro, Danimarca, Estonia, Finlandia, Francia, gran Bretagna, Irlanda, Lussemburgo, Olanda, Portogallo, Slovenia contengono la registrazione delle condanne a carico di persone giuridiche[33]. Ancora più marcate sono le discrepanze relative alla registrazione dei reati commessi da cittadini all'estero. Se tutti i casellari includono le informazioni relative alle condanne pronunciate nei confronti di stranieri sul territorio nazionale, in molti Paesi (Cipro, Repubblica Ceca, Gran Bretagna, Irlanda, Polonia) non vengono registrate le condanne emesse all'estero nei confronti di propri cittadini. Anche negli ordinamenti nei quali è contemplata la registrazione delle sentenze straniere, questa viene spesso subordinata a diverse condizioni[34]. Tra queste, viene in rilievo anzitutto la circostanza che la sentenza non sia contraria ai principi fondamentali sanciti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo (cfr., ad esempio, l'art. 733 c.p.p., il quale esclude il riconoscimento e, quindi, l'iscrizione della sentenza straniera, che «non è stata pronunciata da un giudice indipendente e imparziale»). Talvolta, lo Stato membro prevede l'iscrizione delle sentenze straniere solamente se si riferiscono a un reato riconosciuto anche al proprio interno (così accade in Austria, Danimarca, Germania, Italia, Lussemburgo, Svezia, Ungheria) oppure se riguardano un delitto grave (così avviene in Grecia).

Va rilevato, inoltre, che taluni registri contengono una sezione *ad hoc* per i procedimenti in corso e conservano alcune tipologie di sentenze di proscioglimento, in particolare quelle fondate sull'accertamento dell'incapacità di intendere e di volere (v. ad esempio l'Italia: art. 3, comma 1, lett. *f*, d.P.R. 14 novembre 2002, n. 313). In alcuni Stati membri, le decisioni trascritte provengono soltanto da giurisdizioni penali, mentre in altri, sono registrate pure decisioni di autorità amministrative o di giurisdizioni commerciali che applicano ad esempio san-

---

O. Jansen, "The Regulation of Criminal Records in the Netherlands", in *Financial Crime in the EU*, cit., pp. 267 sgg.; Id., "The European Criminal Record in the Netherlands", in *Towards a European*, cit., p. 215; J. Fenyk, "The European Criminal Record in the Czech Republic", *ibidem*, pp. 138 sgg.; K. Šugman – D. Petrovec, "The European Criminal Record in Slovenia", *ibidem*, p. 227; F.J. García Fernández, "National Criminal Records and Organised Crime in Spain", in *Financial Crime in the EU*, cit., p. 281; Id., "The European Criminal Record in Spain", in *Towards a European*, cit., p. 270; K. Ligeti, "The European Criminal Record in Hungary", *ibidem*, p. 182.

31 Cfr. A. Ondrejova, "The European Criminal Record in Slovakia", in *Towards a European*, cit., p. 245.

32 Cfr. *The use of criminal records as a means of preventing organised crime*, cit., I, p. 9.

33 Cfr. H. Xanthaki, "The European Criminal Record: Analysis", in *Towards a European*, cit., p. 28. Ai Paesi indicati va ora aggiunta anche l'Italia (v. art. 9 d.P.R. 14 novembre 2002, n. 313).

34 V., ancora, H. Xanthaki, "The European Criminal Record: Analysis", cit., pp. 30 sg., dalla quale sono desunti anche i dati riferiti agli ordinamenti stranieri citati nel testo.

zioni disciplinari o misure interdittive. Anche le informazioni sulle misure di esecuzione delle pene variano[35].

Con riferimento alla cancellazione dell'iscrizione dal casellario, occorre sottolineare che essa non è prevista in Irlanda, mentre è contemplata negli altri Paesi. Ciò che varia notevolmente, però, è l'arco temporale dopo il quale essa è disposta: si va dai dieci anni dopo la morte del soggetto della Lituania, ai dieci anni dal termine dell'esecuzione della pena della Danimarca, sino ai due anni dal termine dell'esecuzione in Spagna (almeno per le condanne a pena non superiore a un anno)[36].

Infine, per quel che concerne l'accesso ai registri nazionali, si è osservato che, mentre tutti i Paesi consentono il pieno accesso agli archivi alle autorità di polizia e giudiziarie, il panorama appare assai più variegato in relazione all'accesso da parte di altre autorità. Taluni ordinamenti consentono l'accesso – perfino diretto – alle autorità amministrative ai fini del compimento della loro funzione istituzionale, mentre in un numero limitato di Stati membri, il casellario giudiziario è accessibile pure ai terzi (datori di lavoro privati o associazioni professionali)[37].

Ebbene, è del tutto evidente che la riscontrata disomogeneità della disciplina del casellario giudiziale nei diversi ordinamenti ostacola alla radice una uniforme e completa conoscenza della storia personale del soggetto sul territorio dell'Unione europea. Ove anche funzionassero i meccanismi di trasmissione dei dati, le discrepanze sul contenuto dei casellari e sui termini di conservazione sono tali da rendere incerta e casuale l'attuazione del canone di disponibilità in senso lato dei dati[38].

Ad ogni modo, gli strumenti tradizionali di assistenza giudiziaria appaiono tutt'altro che efficienti. Già a metà degli anni Ottanta, si era messo in luce come «l'application pratique des dispositions prévues aux articles 13 et 22 de la Convention laisse a désirer»[39].

In particolare, tre sembrano essere le disfunzioni riscontrate: anzitutto, la difficoltà di identificare rapidamente gli Stati membri nei quali una persona è già stata destinataria di condanne; in secondo luogo, la difficoltà di ottenere l'informazione rapidamente e secondo una procedura semplice; infine, la difficoltà di comprendere le informazioni eventualmente trasmesse[40].

---

35 V. *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 3.

36 Cfr. H. Xanthaki, "The European Criminal Record: Analysis", cit., p. 28. Sulla brevità dei termini di conservazione del dato nel casellario spagnolo, derivante dalla necessità di facilitare la riabilitazione sociale del reo, v. F.J. García Fernández, *op. cit.*, pp. 267 sgg. (spec. p. 273).

37 V. la tabella pubblicata in *The use of criminal records as a means of preventing organised crime*, cit., I, pp. 43-44.

38 Sulla disponibilità in senso lato, cfr. *supra*, M. Gialuz, "La cooperazione informativa quale motore del sistema europeo di sicurezza", § 2.

39 Così, A. Spielmann, *op. cit.*, p. 652.

40 In tal senso, il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 4.

Sotto il primo profilo, il problema nasce dal mancato funzionamento in concreto del meccanismo di centralizzazione delle informazioni presso lo Stato di cittadinanza previsto dalla Convenzione del 1959. In linea teorica, l'obbligo di notifica disciplinato dall'art. 22 Conv. eur. ass. giud. dovrebbe consentire agli Stati membri di conoscere – e, quindi, di trascrivere – altresì le condanne riguardanti il proprio cittadino pronunciate in altro Stato membro. Senonché, non solo la trasmissione avviene generalmente una volta all'anno, ma lo Stato di cittadinanza non ha – come si è visto – l'obbligo di iscrivere il dato relativo alla condanna straniera nel proprio casellario e, quand'anche prevede la registrazione, normalmente la subordina a tutta una serie di condizioni. Di più: una volta effettuata la registrazione, generalmente il singolo ordinamento applicherà la propria disciplina relativamente alla cancellazione e all'accesso. Il risultato è che il casellario giudiziale dello Stato di nazionalità è spesso incompleto: pertanto, qualora un altro Stato si rivolga allo Stato di nazionalità per conoscere i precedenti penali di una persona rischierà di ottenere un'informazione parziale. Da questo punto di vista, appare sintomatico lo scandalo scoppiato in Inghilterra quando, a seguito dell'individuazione di un'autorità centrale del casellario, emerse che, nel periodo compreso tra il 1995 e il 2006, si erano accumulate presso l'*Home Office* circa ventimila notifiche di condanne di cittadini inglesi, inviate da autorità straniere[41]. Non molto diversa la situazione in Francia, ove si è notato che circa il quaranta per cento delle informazioni notificate dalla Germania non venivano registrate nel casellario nazionale[42].

Quanto alla difficoltà di ottenere informazioni in tempi brevi, viene in gioco il meccanismo della richiesta, contemplato dall'art. 13 Conv. eur. ass. giud. Dal Libro bianco della Commissione emerge come tale meccanismo sia inefficace. Anzitutto, l'art. 13 sembra generalizzare l'obbligo di risposta, ma, in realtà, tale disposizione è oggetto di diverse riserve da parte di alcuni Stati membri. In secondo luogo, trattandosi di un meccanismo di mutua assistenza, potrà essere neutralizzato facendo valere il requisito della doppia incriminabilità[43]. Infine, non è previsto alcun termine per la risposta, la quale potrebbe giungere in tempi incompatibili con quelli del

---

41 Se tra il 1991 e il 1995 le notifiche venivano trasmesse alla *Metropolitan Police*, dopo questa data esse vennero trattenute presso l'*Home Office*, in quanto vennero considerate «as having little or no operational value and were treated purely as a statistical return by officials in National Criminal Intelligence Service» (testualmente, D. Amroliwala, *Report of the Inquiry into the handling by Home Office officials of notifications, by other European countries, of criminal convictions for UK citizens*, <http://www.homeoffice.gov.uk/documents/inquiry-criminal-convictions?view=Binary>, p. 6). Per qualche indicazione al riguardo, cfr. anche T. Thomas, *op. cit.*, pp. 184 sg.; L. Webley, *op. cit.*, p. 296.

42 V. *Proposition de resolution sur le Livre blanc relatif à l'échange d'informations sur les condamnations pénales et à l'effet de celles-ci dans l'Union européenne*, presentata al Senato francese da P. Fauchon, nella seduta del 10 marzo 2005, <http://www.senat.fr/leg/ppr04-241.html>.

43 C. Stefanou – H. Xanthaki, "Introduction: How did the idea of a European Criminal Record come about?", in *Towards a European*, cit., p. 7.

procedimento penale[44]. Per tutte queste ragioni, le giurisdizioni nazionali spesso finiscono per considerare la procedura di cui all'art. 13 Conv. eur. ass. giud. troppo complessa e lunga, e, pertanto, per rinunciare alla richiesta.

In terzo luogo, quand'anche le informazioni relative alle condanne pronunciate all'estero vengano trasmesse, si riscontrano notevoli problemi di comprensione. Si tratta senz'altro di difficoltà di ordine linguistico[45], ma gli ostacoli di ordine giuridico sono perfino maggiori. Come si è osservato, esiste una grande diversità nelle informazioni che figurano nei casellari giudiziari nazionali, che riflette la disomogeneità dei diversi sistemi penali. Ciò rende spesso difficile l'impiego dei dati da parte delle autorità che le ricevono. Se possibile, ancora più incerta risulta la circolazione delle notizie relative alle decadenze e alle interdizioni, in quanto, vista la loro eterogeneità, non sempre figurano nel casellario nazionale[46].

Accanto ai meccanismi individuati dalla Convenzione del 1959, che costituiscono i canali più diffusi di collaborazione, se ne annoverano molti altri. Da un lato, vanno ricordate le convenzioni bilaterali, stipulate da diversi Paesi, e, dall'altro, non si può sottacere l'uso di Interpol, di Europol e del SIS, né si può omettere di rammentare la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea del 2000. L'art. 6 di tale Convenzione prevede, infatti, la possibilità di effettuare le richieste di assistenza giudiziaria e gli scambi di informazioni direttamente tra le autorità giudiziarie degli Stati membri.

Ora, è stato rilevato che nemmeno tali meccanismi garantiscono un'efficace circolazione delle informazioni, per diverse ragioni, che vanno dalla loro portata spesso limitata – ad esempio: le ricerche tramite Interpol, Europol e Schengen si riferiscono solo all'attività di polizia – alla circostanza che non tutti gli Stati membri partecipano a ciascuno strumento di trasmissione, dal fatto che mancano mezzi di esecuzione dell'obbligo, alla macchinosità e lentezza di tali strumenti[47].

4. Il Libro bianco del 2005: modelli di casellario europeo e utilizzazione delle informazioni sulle condanne all'estero

Di fronte a tale preoccupante panorama e alla crescente consapevolezza dell'importanza di disporre di notizie complete sulla storia criminale, tanto ai fini del processo penale, quanto per scopi diversi (tra i quali spicca quello relativo al vaglio dell'idoneità per l'assunzione), il Programma di misure sul reciproco rico-

---

44 Cfr. C. Tomboy, *Vers une meilleure connaissance des antécédents pénaux des personnes. Le casier judicaire*, in "International Review of Penal Law", 2006, p. 180.

45 Cfr. D. Amroliwala, *op. cit.*, p. 13.

46 V. il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 5-6.

47 V. H. Xanthaki, "The European Criminal Record: Analysis", cit., p. 40; M. Plachta, *op. cit.*, p. 432.

noscimento aveva prospettato – come si è visto[48] – tre possibili rimedi al fine di rendere davvero efficienti gli scambi di informazioni tra i casellari nazionali: anzitutto, l'agevolazione degli scambi bilaterali di informazioni; in secondo luogo, il collegamento in rete degli archivi nazionali; infine, la costituzione di un vero e proprio archivio centrale europeo.

Negli studi compiuti in seguito e nel Libro bianco presentato dalla Commissione nel gennaio del 2005, sono stati posti in luce i pregi e i difetti delle diverse soluzioni.

Le prime due sono inquadrabili, secondo la dottrina, in un approccio intergovernativo[49]. Il rafforzamento degli scambi bilaterali si colloca in tutto e per tutto nella prospettiva tradizionale, mentre l'interconnessione presuppone un legame inedito tra i casellari, che può essere più o meno immediato a seconda dei diversi assetti. Sembra, pertanto, che, con riguardo alla prima prospettiva, sia difficile parlare di "casellario giudiziario europeo"; mentre tale espressione pare possa essere impiegata – sia pure in un senso lato – con riferimento alla seconda soluzione.

Ad ogni modo, va notato che entrambe le ipotesi avrebbero il vantaggio di conservare le informazioni a livello nazionale, quello di evitare la duplicazione delle registrazioni e, infine, quello di non richiedere risorse aggiuntive (finanziarie, di personale e di infrastrutture). Per altro verso, esse presentano alcuni inconvenienti. Anzitutto, non risolvono minimamente il problema dell'identificazione dello Stato detentore delle informazioni. In secondo luogo, non permettono di fornire alle autorità richiedenti informazioni comprensibili e immediatamente utilizzabili, in quanto lasciano intatta l'eterogeneità linguistica e giuridica[50]. In terzo luogo, non contemplano la supervisione da parte di un'autorità dell'Unione, volta a garantire lo scambio anche nel caso di mancata cooperazione dei singoli Stati[51]. Infine, l'accesso ai dati e il loro impiego rimarrebbe regolato in modo diverso, così che non sarebbe agevole garantire uno *standard* minimo di protezione dei dati[52].

La terza opzione è quella che passa per la costruzione di un vero e proprio "casellario giudiziario europeo", ossia di un archivio centralizzato delle condanne pronunciate nei Paesi membri dell'Unione. Il progetto più importante al riguardo è quello dell'*European Criminal Record* (ECR), tratteggiato nelle ricerche effettuate dall'*Institute of Advanced Legal Studies* di Londra e dall'*Institute for International Re-*

---

48 Cfr. *supra*, § 2.

49 In tal senso, E. De Busser, "A European criminal records database: An integrated model", in *Towards a European*, cit., p. 338.

50 V. il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., pp. 6-7; nonché, C. Stefanou, "The European Criminal Record: Political parameters", in *Towards a European*, cit., p. 70.

51 Ancora, E. De Busser, *op. cit.*, p. 338

52 In tal senso, H. Xanthaki, "The European Criminal Record: Analysis", cit., p. 43.

search on Criminal Policy di Gand[53]. Secondo la definizione fornita dai suoi fautori, l'ECR si configurerebbe come un «centralised, Eurojust mantained, EU database with data on convictions for transnational crimes for all EU citizens»[54].

Sarebbe pertanto un archivio istituito a livello comunitario e gestito da Eurojust, che verrebbe preferito a Europol in quanto offre maggiori garanzie: non soltanto esso ha natura quasi giudiziaria, ma i rimedi esperibili avverso le sue decisioni si mostrano più efficienti; inoltre, appaiono più elevati i livelli di protezione dei dati[55].

Quanto ai dati raccolti in tale database, la maggior parte degli autori ritiene compatibile con il canone di proporzionalità la conservazione delle informazioni relative alle condanne per i soli reati per i quali l'ECR appare realmente indispensabile, ossia i reati transnazionali. In particolare, il catalogo di reati potrebbe essere quello individuato dall'art. 4 della decisione istitutiva di Eurojust o dall'art. 2 della decisione sul mandato d'arresto europeo[56]. Secondo questa proposta, si tratterebbe quindi di una sorta di «*casier judiciaire européen catégoriel*»[57].

Siffatto progetto consentirebbe di rimediare alle principali difficoltà che caratterizzano i primi due modelli: renderebbe, infatti, immediatamente disponibili le informazioni all'autorità giudiziaria di qualsiasi Stato membro (indipendentemente dal luogo della condanna) e garantirebbe regole comuni in tema di conservazione, sicurezza, cancellazione e aggiornamento dei dati, nonché con riguardo all'accesso e all'utilizzo degli stessi[58]. Peraltro, anche tale soluzione – soprattutto nella sua versione non limitata – presenta alcuni difetti, puntualmente segnalati dalla Commissione nel Libro bianco. Da un canto, essa si rivela «sproporzionata rispetto agli obiettivi perseguiti, poiché ne conseguirebbe che l'informazione contenuta negli archivi nazionali sia duplicata a livello europeo»; dall'altro, essa presupporrebbe la creazione di un costoso sistema di mantenimento e di accesso e la definizione di una normativa specifica per le informazioni contenute nel casellario europeo[59].

Proprio tenendo conto dei vantaggi e degli svantaggi delle diverse opzioni, la Commissione ha prospettato nel Libro bianco una soluzione mista, che potrebbe definirsi di "interconnessione centralizzata" dei casellari nazionali. Essa ruota

---

53 Cfr. *supra*, note 8 e 15.

54 C. Stefanou – H. Xanthaki, "Conclusions", in *Towards a European*, cit., p. 382.

55 Così, H. Xanthaki, "The European Criminal Record: Analysis", cit., pp. 44 sg.

56 Cfr., H. Xanthaki, "The European Criminal Record: Analysis", cit., p. 44; Ead., "The establishment of a European Criminal Record: Human rights considerations", in *Towards a European*, cit., p. 96.

57 L'espressione si legge nella *Proposition de resolution sur le Livre blanc*, cit.

58 In tal senso, per tutti, C. Stefanou, "The European Criminal Record: Political parameters", cit., p. 70.

59 V. il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 7.

intorno a due pilastri: la creazione di un indice europeo delle persone già condannate e l'elaborazione di un formato europeo standardizzato[60].

L'architettura complessiva del sistema sarebbe diversa rispetto a quella tradizionale: se questa riconosce centralità allo Stato di cittadinanza – si ricordi che le notifiche previste dall'art. 22 Conv. eur. ass. giud. hanno proprio questa funzione –, la proposta della Commissione si fonda sulla valorizzazione dello Stato di condanna, quale Stato naturalmente detentore delle informazioni sulla condanna. Ovviamente, tale scelta postula la predisposizione di uno schedario centralizzato, che permetta di individuare gli Stati che possiedono informazioni relative al curriculum penale di un cittadino europeo. Vista tale finalità limitata, l'archivio dovrebbe riportare soltanto gli elementi che permettono di identificare la persona (cognome, nome, luogo e data di nascita, cittadinanza, ecc.) e lo Stato membro nel quale la persona è già stata condannata. Non verrebbero, invece, conservate tutte le informazioni sul contenuto e sulla forma della pronuncia, le quali andrebbero richieste agli Stati membri individuati attraverso l'interrogazione dello schedario. Si tratterebbe dunque di un sistema di accesso mediato alle informazioni di un altro Stato membro, che ricalca per certi versi il modello del SIS o dell'Eurodac[61]. Peraltro, la stessa Commissione riconosce espressamente la possibilità di utilizzare le infrastrutture già esistenti.

Accanto a tale indice, che garantirebbe l'individuabilità del dato, la Commissione suggerisce la creazione di un sistema informatizzato di scambi basato su un formato standardizzato, che dovrebbe garantire la piena accessibilità e utilità dell'informazione. Una volta individuato lo Stato della condanna, questo dovrebbe rispondere alla richiesta, fornendo le informazioni concernenti: la persona oggetto della decisione; la forma del provvedimento; i fatti che hanno dato luogo alla pronuncia; il contenuto della sentenza.

Peraltro, il Libro bianco non si ferma al piano dello scambio di informazioni estratte dal casellario. Una delle novità più significative è rappresentata infatti dall'allargamento della prospettiva al livello – strettamente connesso – relativo all'utilizzazione delle informazioni circa la condanna pronunciata all'estero. Al fondo, vi è la consapevolezza che «il miglioramento della qualità dello scambio di informazioni sulle condanne penali ha senso soltanto nella misura in cui queste ultime possano essere utilizzate»[62] e, viceversa, che il pieno riconoscimento della condanna nell'ordinamento straniero incentiva lo scambio delle informazioni.

È chiaro che gli effetti della condanna in un ordinamento straniero sono assai eterogenei, come lo sono all'interno del medesimo ordinamento nazionale. La

---

60 Cfr., ancora, il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 7.

61 Sul Sistema di informazione Schengen, cfr. *supra*, F. Decli - G. Marando, "Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia", § 2. Per quel che riguarda Eurodac, si legga *supra*, M. Gialuz, "Principio di accessibilità e banche dati di 'primo pilastro'", § 2.

62 V. il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 9.

condanna può infatti assumere rilievo ai fini del *ne bis in idem* e dell'esecuzione, ma può incidere altresì sull'applicazione delle norme processuali, sulla qualifica del reato e sulla scelta della pena (si pensi, ad esempio, alla recidiva o all'impossibilità di applicare la sospensione condizionale), nonché sul regime di esecuzione della stessa (vengono in mente le preclusioni all'applicabilità delle misure alternative alla detenzione).

Anche da questo punto di vista, il panorama a livello europeo appare alquanto disomogeneo. Alcuni Stati membri subordinano gli effetti delle condanne penali straniere a precise condizioni previste dalla legge – si pensi all'ordinamento italiano, ove è richiesto il riconoscimento[63] –, mentre in altri la valutazione del precedente viene lasciata alla valutazione discrezionale del giudice. In ogni caso, si è verificato che la possibilità di tener conto delle condanne pronunciate negli altri Stati membri è spesso limitata e, appunto per questo, la Commissione si è impegnata a depositare «un progetto di decisione quadro sulla presa in considerazione delle decisioni di condanna»[64].

5. Una razionalizzazione dell'esistente: la decisione n. 876 del 2005

La prima proposta normativa elaborata dalla Commissione in materia di scambio di informazioni estratte dal casellario precede il Libro bianco e si colloca sul piano meno ambizioso tra i tre prospettati da quest'ultimo: ossia quello del semplice miglioramento dello scambio bilaterale.

Si tratta della già citata proposta di decisione del Consiglio relativa allo scambio di informazioni estratte dal casellario giudiziario (COM(2004)664 def.), presentata nell'ottobre del 2004, quale risposta immediata a quel clima emergenziale che si era determinato in quell'anno. È anche per questo suo *imprinting* che essa

---

63 Dopo l'entrata in vigore del nuovo codice si tende a ritenere che prima del riconoscimento le sentenze straniere siano prive di qualsiasi rilevanza: lo si desume dalla scelta di escludere la possibilità di iscrivere la sentenza nel casellario prima del suo riconoscimento (art. 686, comma 2, c.p.p., ora art. 3, lett. a, d.P.R. 313 del 2002). Pertanto, solo attraverso il riconoscimento acquisirebbero valenza anche soltanto come fatti storico-giuridici (R. Fois, "Riconoscimento di sentenze straniere", in *Rapporti intergiurisdizionali*, a cura di M.G. Aimonetto, Torino, Utet, 2002, p. 312; M.R. Marchetti, "Valore ed effetti della sentenza penale straniera", in *Digesto delle discipline penalistiche*, XV, Torino, Utet, 1999, p. 179; P. Pittaro, "Commento all'art. 730 c.p.p.", in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, VI, Torino, Utet, 1991, p. 817; nonché, sotto la vigenza del codice Rocco, A. Gaito, *Dei rapporti giurisdizionali con autorità straniere*, Padova, Cedam, 1985, p. 179). Ne consegue che la precedente condanna emessa all'estero e desumibile dall'estratto tempestivamente trasmesso non potrebbe – a rigore – essere considerata come elemento informativo sulla persona dell'imputato ai fini del giudizio prognostico di cui all'art. 274, comma 1, lett. *c* c.p.p. o dell'applicazione degli artt. 62-*bis* e 133 c.p. In tal senso, peraltro, depone lo stesso art. 236 c.p.p., che consente di acquisire, ai fini del giudizio sulla personalità dell'imputato, la sola sentenza straniera "riconosciuta".

64 V. il *Libro Bianco relativo allo relativo allo scambio di informazioni*, cit., p. 10.

ha – come emerge dalla stessa relazione – un obiettivo limitato: appunto quello di razionalizzare i meccanismi esistenti; mentre la realizzazione di un più ambizioso sistema informatizzato di scambio di informazioni delle condanne penali tra gli Stati membri viene demandato a un progetto successivo. D'altronde, la stessa scelta dello strumento della decisione è indicativa della prospettiva circoscritta nella quale si colloca la proposta: a detta della Commissione, tale fonte, che non comporta un processo di ravvicinamento delle disposizioni legislative nazionali, costituiva il mezzo più rapido per pervenire a un rapido miglioramento delle pratiche tradizionali.

Ciò premesso, il progetto di decisione ruotava intorno a due obiettivi: da un lato, quello di migliorare il sistema delle notificazioni di cui all'art. 22 Conv. eur. ass. giud. e, dall'altro, quello di garantire l'effettività del meccanismo della richiesta di cui all'art. 13 Conv. eur. ass. giud.

Sotto il primo profilo, si richiedeva la designazione di un'autorità centrale, competente in materia di casellario (art. 2) e l'obbligo per quest'ultima di effettuare la notificazione non soltanto una volta all'anno, ma immediatamente dopo la registrazione della condanna (art. 3). Peraltro, nella relazione al progetto, si poneva in luce la circostanza che la decisione «non modifica la natura degli obblighi imposti agli Stati membri e non prevede, in particolare, alcuna obbligazione a carico dello Stato di condanna di informare anche lo Stato di residenza, il che sarebbe stato ipotizzabile per i cittadini non comunitari o per i cittadini comunitari che risiedono in uno Stato diverso da quello di cui posseggono la nazionalità»[65].

Con riguardo al secondo fine, la proposta predisponeva anzitutto un formulario modello al fine di agevolare lo scambio delle informazioni[66]. Inoltre, essa contemplava la fissazione di un termine di cinque giorni entro il quale l'autorità centrale dello Stato richiesto doveva trasmettere le informazioni. Veniva inoltre fatta salva la possibilità, per l'autorità giudiziaria, di avvalersi del canale di comunicazione diretta riconosciuto dall'art. 6, par. 1, della Convenzione relativa all'assistenza giudiziaria tra gli Stati dell'Unione europea del 2000.

La proposta prevedeva inoltre la definizione, tanto del concetto di "casellario giudiziario", quanto di quello di "condanna" (art. 1). Quest'ultima veniva intesa come «ogni decisione definitiva di una giurisdizione penale o di un'autorità amministrativa la cui decisione può dar luogo ad un ricorso dinanzi ad una giurisdizione competente in particolare in materia penale, che stabilisca la colpevolezza di una persona per un reato penale o per un atto punibile secondo il diritto na-

---

65 Testualmente, la *Relazione alla Proposta di decisione del Consiglio relativa allo scambio di informazioni estratte dal casellario giudiziario (COM (2004) 664 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0664:FIN:IT:PDF>, p. 2. Qualche perplessità sull'esclusione dell'obbligo di informare lo Stato di residenza, soprattutto con riferimento ai non cittadini, viene espressa da M. Plachta, *op. cit.*, p. 433.

66 V. A. Marandola, *op. cit.*, p. 1383; N. Plastina – G. Iuzzolino, *Casellario giudiziale, via al modello UE. Agevolato lo scambio di dati fra Stati*, in "Diritto e giustizia", 2006, n. 1, p. 104.

zionale in quanto lesivo di norme di diritto». Si trattava di definizione modellata sulla nozione di reato risultante dall'applicazione dell'art. 51 della Convenzione di applicazione dell'accordo di Schengen del 1990, poi ripresa nell'art. 3 della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea del 29 maggio 2000[67]. Il casellario veniva invece designato come «il registro nazionale o i registri nazionali che riportano le condanne conformemente al diritto nazionale».

Ancora, il progetto si preoccupava di tutelare il diritto alla protezione dei dati, valorizzando il principio di finalità limitata: l'art. 5 consentiva, infatti, allo Stato richiedente di utilizzare le informazioni solo nell'ambito di procedimenti penali oppure per un fine diverso, ma soltanto nei limiti specificati dallo Stato richiesto e dal diritto nazionale dello Stato richiedente.

Sulla proposta si sono espressi, tanto il Parlamento europeo, quanto il Garante europeo per la protezione dei dati personali. Se il Parlamento ha adottato un parere favorevole, sia pure subordinato all'accoglimento di otto emendamenti vòlti a rafforzare la tutela della privacy[68], il Garante ha avuto un approccio più critico. Intervenuto di propria iniziativa – in quanto la Commissione non l'aveva interpellato –, ha posto in rilievo alcune lacune della decisione, proprio sotto il profilo delle garanzie in materia di protezione dei dati. Anzitutto, ha lamentato l'assenza di qualsivoglia assicurazione circa l'operatività delle tutele contemplate dal diritto nazionale per la trasmissione di informazioni estratte dal casellario giudiziario. In secondo luogo, il Garante ha censurato l'omessa delimitazione dell'accesso ai dati personali a persone con funzioni specifiche e nella misura necessaria per la sicurezza dei cittadini. Infine, ha criticato la proposta nella parte in cui metteva in dubbio il diritto della persona cui si riferiscono i dati di essere informata della comunicazione (la consegna alla stessa del formulario era prevista infatti come facoltativa). Sulla scorta di tali rilievi, il Garante europeo ha raccomandato, da un lato, di «limitare la proposta di decisione alle informazioni relative alle condanne pronunciate per determinati reati gravi» e, dall'altro, di «specificare le garanzie della persona cui si riferiscono i dati, in modo da essere conforme al vigente quadro giuridico in materia di protezione dei dati»[69].

In realtà, il Consiglio non ha accolto né gli emendamenti del Parlamento, né le raccomandazioni del Garante, ed ha approvato la decisione in tempi assai brevi. L'accordo politico è stato raggiunto già nel febbraio del 2005 e, nel novembre dello stesso anno, il testo è stato adottato con lievi modifiche.

---

67 Cfr. la *Relazione alla Proposta di decisione del Consiglio relativa allo scambio*, cit., p. 3.

68 V. la *Relazione della Commissione per le libertà civili, la giustizia e gli affari interni presentata da Antonio Di Pietro (doc. A-0020/2005)*, 3 febbraio 2005, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0020+0+DOC+PDF+V0//IT>.

69 Così, il *Parere del garante europeo della protezione dei dati sulla proposta di decisione del Consiglio relativa allo scambio di informazioni estratte dal casellario giudiziario (COM (2004) 664 def.)*, in *GUUE*, C 58, 8 marzo 2005, p. 6.

Rispetto alla versione iniziale, la decisione 2005/876/GAI ha eliminato le definizioni, sia di "casellario giudiziario", sia di "condanna". Inoltre, ha consentito agli Stati membri di individuare anche più autorità responsabili delle notificazioni e legittimate a rispondere alla richiesta di informazioni (art. 1, par. 2): ciò, in quanto vi sono Paesi dotati di una pluralità di archivi[70]. Per quel che riguarda il termine per la risposta, esso è stato portato da cinque a dieci giorni. Infine, relativamente al meccanismo delle notifiche, si è chiarito che la decisione «non comporta per gli Stati membri alcun obbligo di iscrivere nei propri casellari giudiziari condanne o informazioni in materia penale diverse da quelle che sono tenuti a iscrivere in forza del diritto nazionale» (considerando n. 12) e che rimangono impregiudicate le riserve avanzate relativamente all'art. 22 Conv. eur. ass. giud. (art. 6, par. 2).

6. Il progetto pilota di interconnessione dei casellari giudiziari

Se la via meno ambiziosa indicata nel Libro bianco per rafforzare gli scambi di informazioni estratte dal casellario è stata agevolmente percorsa con la decisione 876 del 2005, in quanto fondata su un modello strettamente intergovernativo, la strada più ambiziosa che passa per la creazione di un vero e proprio casellario centralizzato a livello europeo è stata sin da subito scartata. Questo per diverse ragioni. Anzitutto, il progetto del casellario giudiziale europeo ha il difetto intrinseco – già segnalato dalla Commissione – di comportare la duplicazione delle informazioni[71]. Altro ostacolo decisivo viene dai maggiori rischi che la creazione di archivi centralizzati determina sotto il profilo della protezione dei dati[72]. Infine, si è rilevato come vi sia una diffusa resistenza verso la creazione di nuovi database sul piano più strettamente politico, viste le esperienze del passato (non troppo remoto) di molti Stati europei[73].

Per la verità, la Commissione si era fatta carico di tali perplessità, nel momento in cui aveva prospettato la soluzione mista dell'"interconnessione centralizzata": questa, infatti, consentiva di conservare i vantaggi del casellario centralizzato, eliminandone però i difetti. Sta di fatto che, pure sulla proposta della

---

70 In tal senso, V. Havy, *op. cit.*, p. 165.

71 V. H. Leniston, *What prospects are there for the European Criminal Record?*, <http://www.europeens.org/question__europe.php?num=qe-19>. Cfr. *supra*, § 4.

72 Non a caso, il *Programma dell'Aia*, cit., p. 20, stabilisce che «nuove basi di dati centralizzate a livello europeo dovrebbero essere create soltanto sulla base di studi che ne dimostrino il valore aggiunto».

73 Secondo C. Stefanou, "The European Criminal Record: Political parameters", cit., p. 69, «especially for the Left in Europe and for citizens of the new Member States [...] keeping files on citizens conjures up images of a totalitarian Europe with dictators, secret police forces and informers keeping files on citizens' actions and political/religious beliefs».

Commissione, si è subito manifestata l'opposizione di alcuni Stati membri. Se nella riunione informale del Consiglio del 28 e 29 gennaio 2005, la maggior parte delle delegazioni appoggiò le proposizioni del Libro bianco, i ministri della giustizia di alcuni Paesi – in particolare Francia, Germania e Regno Unito – espressero forti perplessità sul progetto di indice delle condanne europee. Le riserve furono avanzate, in particolare, con riguardo alla previsione dell'automaticità della consultazione e, soprattutto, con riferimento alla centralizzazione delle informazioni[74]. Quest'ultima, infatti, è stata vista dai Paesi indicati «comme une 'porte ouverte', un préalable à l'installation à terme d'un grand casier judiciaire européen, qui porterait atteinte à la protection de la vie privée»[75].

Nella successiva riunione del Consiglio GAI 14 aprile 2005, la Francia e la Germania – insieme a Spagna e Belgio – insistettero nella richiesta di perseguire la seconda via indicata nel Libro bianco: ossia quella dell'interconnessione dei casellari nazionali[76].

Il che non sorprende affatto. Solo pochi giorni prima, questi quattro Paesi avevano lanciato una cooperazione intergovernativa al di fuori del quadro giuridico dell'Unione: avevano, infatti, promosso un progetto di interconnessione dei loro casellari (*Network of Judicial Registers*)[77]. Per la verità, il progetto aveva preso le mosse tra Francia e Germania già all'inizio del 2003, con una dichiarazione congiunta espressa in occasione del quarantesimo anniversario del Trattato dell'Eliseo; in seguito, erano entrati la Spagna (nel novembre del 2003) e il Belgio (nel novembre del 2004, a seguito del caso Fourniret). Negli anni successivi, il progetto è stato notevolmente allargato: nel 2006, vi hanno aderito Repubblica Ceca e Lussemburgo; nel 2007, sono entrati Slovenia, Regno Unito[78] e Bulgaria (presentati dalla Germania), nonché, Slovacchia, Polonia e Italia (presentati dal-

---

74 Cfr. V. Havy, *op. cit.*, p. 174.

75 Testualmente, V. Havy, *op. cit.*, p. 174.

76 Cfr. il documento del Committee on Civil Liberties, Justice and Home Affairs del Parlamento europeo, intitolato *Freedom, security and justice: an agenda for Europe*, <http://www.europarl.europa.eu/comparl/libe/elsj/zoom_in/12_en.htm>.

77 V. il documento intitolato *L'interconnexion des casiers judiciaires. Dominique Perben lance le projet d'interconnexion des casiers judiciaires avec ses homologues allemand, belge et espagnol (Mars 2005)*, <http://www.presse.justice.gouv.fr/art_pix/conf040405.pdf>. Di «une sorte de 'coopération renforcée'» si parla nella *Proposition de resolution sur le Livre blanc*, cit., nella quale si invita peraltro a sostenere il progetto della Commissione di realizzare un indice europeo delle condanne: secondo il senatore P. Fauchon, infatti, «il n'y a pas véritablement d'incompatibilité entre la mise en réseau des casiers judiciaires de ces pays et le projet de la Commission de créer un 'index européen des personnes ayant déjà fait l'objet de condamnations', puisque les deux démarches sont complémentaires et qu'elles vont dans le même sens».

78 Cfr. *House of Commons. Home Affairs - Third Report*, <http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhaff/76/7606.htm>, ove, non solo si garantisce il pieno supporto all'intenzione del Governo «to sign up without delay to the pilot project on interoperability of criminal records data», ma si riconosce che «it is very regrettable that the UK missed the opportunity to be one of the original pilot participants, and thus influence the project from the start».

la Francia); nel 2008, si sono aggiunti il Portogallo (presentato dalla Spagna) e i Paesi Bassi (presentati dal Belgio). Inoltre, Svezia, Romania e Austria sono stati ammessi come osservatori[79].

Sotto il profilo strettamente giuridico, il progetto non si discosta dalla decisione 876 del 2005: invero, la base giuridica è costituita dagli artt. 13 e 22 Conv. eur. ass. giud. Nondimeno, esso prevede due significative innovazioni. La prima riguarda le modalità di comunicazione; l'interconnessione si fonda infatti sull'utilizzo dell'infrastruttura TESTA (*Trans-European Services for Telematics between Administrations*), che permette la trasmissione delle informazioni in via telematica. Ciò garantisce l'invio davvero immediato delle notificazioni e la risposta in tempo reale alle richieste di informazioni sulle condanne (da un tempo minimo di pochi minuti a un periodo medio di tre ore)[80]. Di più: il sistema TESTA procede automaticamente alla memorizzazione delle informazioni inviate nella sua banca dati, in modo tale da garantire un ulteriore risparmio di tempo nel caso di ulteriore richiesta concernente la medesima persona da parte di altri Paesi[81].

La seconda importante novità è data dalla predisposizione di una tavola di corrispondenze tra le principali categorie di informazioni. Al fine di garantire una certa automaticità nella traduzione linguistica e giuridica, i quattro Paesi promotori hanno individuato una tabella relativa ai reati, che consta di quarantaquattro categorie e centosettantasei sottocategorie, alle quali è stato assegnato un codice identificativo[82]. Essa è stata elaborata partendo dalle infrazioni relative al mandato d'arresto e da quelle più registrate in ciascun casellario nazionale[83].

Il sistema è divenuto operativo nel marzo del 2006 e ha funzionato davvero bene, come emerge chiaramente dalle rilevazioni statistiche disponibili. Basti pensare che, nel primo mese di funzionamento, Francia e Germania hanno scambiato più informazioni che nei dieci anni precedenti[84]: tra il marzo del 2006 e il settembre del 2008, la Francia ha infatti risposto a 12.609 richieste di infor-

---

79 Queste informazioni si desumono da *Interconnexion des casiers judiciaires européens – ICJ*, <http://www.justice.gouv.fr/index.php?rubrique=10045&ssrubrique=10281&article=13884>.

80 Cfr. W. Bernhardt, *Network of Judicial Registers*, <http://www.mj.gov.pt/sections/o-ministerio/instituto-das/anexos/sebastian-von-levetzon/downloadFile/file/NJR__Presentation__Lisbon.pdf>, p. 15.

81 Il rilievo è di B. Lapérou-Scheneider, *op. cit.*, p. 77.

82 V. W. Bernhardt, *op. cit.*, p. 13, il quale riferisce come sia in cantiere anche un indice delle decisioni, comprendente diverse tipologie di sanzioni e di altre misure; J.B. Jacobs-D. Blitsa, *Major "Minor" Progress Under the Third Pillar: EU Institution Building in the Sharing of Criminal Record Information*, in "Chicago-Kent Journal of International and Comparative Law", 2008, p. 120, 136; C. Tomboy, *Vers une meilleure connaissance*, cit., p. 181.

83 Così, *L'interconnexion des casiers judiciaires*, cit., p. 9.

84 Cfr. *Comunicazione della Commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo. Verso una strategia europea in materia di giustizia elettronica (COM (2008) 329 def.)*, 30 maggio 2008, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0329:FIN:IT:PDF>, p. 8, nota 21.

mazioni e ha ricevuto 6.218 risposte a proprie richieste; quanto alle notificazioni, nello stesso periodo, la Francia ne ha emesse 7.782 e ne ha ricevute ben 19.371 dagli altri Paesi[85]. Con riferimento alla Germania, tra il primo gennaio e il 31 luglio del 2007, sono state emesse 327 richieste ad altri Paesi (con 84 risposte positive) e sono state fornite risposte a ben 1028 istanze provenienti dall'estero (con esito positivo in 201 casi); nello stesso scorcio temporale, sono state trasmesse 2884 notificazioni agli altri casellari e l'autorità centrale tedesca ne ha ricevute 1320[86].

7. La decisione quadro relativa all'organizzazione e al contenuto degli scambi di informazioni estratte dal casellario giudiziario

Preso atto dell'assenza delle condizioni per attuare il proprio modello centralizzato di interconnessione, la stessa Commissione ha deciso di assecondare la volontà dei principali Stati membri e di sostenere quindi la realizzazione di quello che si potrebbe definire – per distinguerlo dal primo – progetto di "interconnessione diffusa", già iniziato da alcuni di essi. Resasi conto che tale progetto non riusciva di per sé a rimediare alle carenze enucleate dal Libro bianco, ad appena un mese di distanza dall'adozione della decisione 876 del 2005, la Commissione ha presentato una proposta di decisione quadro relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def., 22 dicembre 2005).

Dopo un *iter* durato poco più di tre anni, la proposta è stata adottata dal Consiglio il 26 febbraio 2009: nell'ordinamento giuridico dell'Unione ha fatto così il suo ingresso la decisione quadro 2009/315/GAI[87], che è entrata in vigore il 27 aprile 2009 e dovrà essere recepita dagli Stati membri entro il 27 aprile 2012 (art. 13). Essa rappresenta oggi la fonte principale di disciplina dello scambio di informazioni estratte dal casellario giudiziale in quanto, per un verso, prevede espressamente che la sua disciplina sostituisce – ovviamente nei rapporti tra gli Stati membri che l'abbiano attuata – l'art. 22 Conv. eur. ass. giud. e, per l'altro, decreta l'abrogazione della decisione n. 876 del 2005 (art. 12, par. 3 e 4).

Come emerge dai lavori preparatori, la decisione quadro – che avrebbe consentito, ove adottata tempestivamente, di fornire sin dall'inizio una più solida base legale al progetto pilota di interconnessione[88] – ha due obiettivi. Da una par-

---

85 Le statistiche sono pubblicate nel documento *Interconnexion des casiers judiciaires européens – ICJ*, cit. I dati riferiti assumono maggiore valenza se si pensa che, nel 2002, la Francia aveva rivolto solo otto domande di informazioni alla Germania (l'informazione si trova in B. Lapérou-Scheneider, *op. cit.*, p. 70).

86 I dati sono riportati da W. Bernhardt, *op. cit.*, p. 15.

87 In *GUUE*, L 93, 7 aprile 2009, p. 23.

88 V. *Programme of the Federal Ministry of Justice for the German EU Council Presidency 2007/1*,

te, quello di perfezionare il meccanismo di scambio fondato sulla centralità dello Stato membro di nazionalità; dall'altra, quello di definire «il quadro che permetterà di costruire e sviluppare un sistema computerizzato di scambi d'informazioni sulle condanne penali, basato sull'uso di un 'formato europeo standardizzato' che permetta di scambiare queste informazioni in una forma omogenea computerizzata»[89].

Con riguardo al primo profilo, la decisione mira a porre lo Stato di cittadinanza nelle condizioni di fornire una risposta esauriente e puntuale alle richieste provenienti dagli altri Stati in merito agli antecedenti giudiziari di suoi cittadini. A tal fine, essa completa il lavoro di razionalizzazione iniziato con la decisione n. 876 del 2005.

In primis, ribadisce l'obbligo dello Stato di condanna di notificare immediatamente l'informazione concernente l'iscrizione all'autorità centrale dello Stato di cittadinanza e aggiunge il dovere di trasmettere – su richiesta di quest'ultima – copia delle sentenze e dei conseguenti provvedimenti, nonché qualsiasi altra informazione pertinente, ove ciò sia richiesto dall'autorità dello Stato di cittadinanza (art. 4, par. 5). La decisione specifica, inoltre, la tipologia di dati che lo Stato di condanna deve trasmettere, distinguendo nell'art. 11 tra informazioni obbligatorie (ossia quelle relative alle generalità della persona condannata, alla natura della condanna, al reato e al contenuto della sentenza), informazioni facoltative (ossia quelle che devono essere trasmesse se iscritte nel casellario, come ad esempio il nome dei genitori del condannato o il luogo del reato) e informazioni supplementari (ossia quelle che vanno trasmesse, se sono a disposizione dell'autorità centrale, come il tipo e numero del documento di identificazione della persona condannata, le impronte digitali prese a questa persona e i suoi eventuali pseudonimi). Degno di nota appare l'inserimento tra le informazioni facoltative delle interdizioni derivanti dalla condanna: tale norma deriva, infatti, dall'assorbimento nella proposta n. 690 del 2005 dell'iniziativa del Regno del Belgio del 2004[90].

Ma ancor più significativa è la previsione dell'obbligo, per lo Stato di cittadinanza, di conservare integralmente le informazioni trasmesse dallo Stato di con-

---

<http://bundesjustizministerium.com/files/-/1540/BMJ-Pr%C3%A4sidentschaftsprogramm%20engl.pdf>, p. 12.

89 Testualmente, la *Relazione alla Proposta di decisione quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0690:FIN:IT:PDF>, p. 4.

90 A tale proposito, si legga il preambolo della proposta di decisione quadro, nonché i considerando n. 6 e 12. Va notato, peraltro, che il progetto presentato dal Regno del Belgio era più ambizioso, in quanto non si limitava, come il testo in esame, al piano della circolazione delle interdizioni, ma prevedeva all'art. 3 l'introduzione di un vero e proprio obbligo di iscrizione delle stesse nei casellari nazionali (v. J.B. Jacobs-D. Blitsa, *op. cit.*, p. 132, secondo i quali la proposta della Commissione riprenderebbe solo alcuni elementi dell'iniziativa belga).

danna, ai fini della ritrasmissione allo Stato richiedente (art. 5)[91]: in particolare, esso deve conservare tutte le informazioni obbligatorie e quelle facoltative, mentre ha facoltà di archiviare le informazioni supplementari (art. 11, par. 2). Come si è ricordato, proprio la mancanza di quest'obbligo di conservazione era una delle cause fondamentali del mancato funzionamento del tradizionale meccanismo contemplato dalla Convenzione del 1959. La sua esplicita fissazione dovrebbe pertanto consentire una maggiore efficienza del sistema di interconnessione diffusa avallato dal progetto in esame.

Peraltro, la decisione quadro non si ferma qui. Opportunamente, essa si preoccupa di disciplinare il rapporto tra Stato di condanna e Stato di cittadinanza, anche per quel che riguarda la fase successiva all'iscrizione. Consapevole della notevole divergenza della disciplina nazionale dei casellari, il legislatore europeo ha ragionevolmente optato per la fissazione di un criterio di soluzione dei conflitti: tra il regime dello Stato di condanna e quello dello Stato di cittadinanza finisce per prevalere il primo. L'art. 4, par. 3, prescrive all'autorità dello Stato di condanna di trasmettere immediatamente a quella dello Stato di cittadinanza «le informazioni relative alla successiva modifica o soppressione delle informazioni contenute nel casellario giudiziario». Simmetricamente, l'art. 5, par. 2 stabilisce che qualsiasi modifica o soppressione di informazioni trasmessa dallo Stato di condanna «dà luogo a un'identica modifica o soppressione, da parte dello Stato membro di cittadinanza, delle informazioni conservate». La preminenza dello Stato di condanna è evidente, tanto che, secondo il Garante europeo, «lo 'Stato di condanna' può essere considerato il titolare dei dati»: lo Stato di cittadinanza, infatti, «conserva i dati per conto di tale Stato membro»[92].

---

91 Secondo H. Leniston, *op. cit.*, quest'obbligo rappresentava la «grande nouveauté» della proposta e altrettanto si può dire oggi della decisione.

92 Così, *Parere del garante europeo della protezione dei dati sulla proposta di decisione-quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def.)*, cit., p. 31. Il Garante europeo, pur accogliendo positivamente il meccanismo, raccomanda peraltro di precisare «il concetto di 'titolarità'», al fine di tracciare «una più chiara ripartizione delle competenze» (*ivi*, p. 31). Nel medesimo senso, si è espresso il Parlamento europeo. Tanto nella prima, che nella seconda risoluzione sulla proposta n. 690 del 2005, il Parlamento ha infatti proposto di inserire un considerando vòlto a chiarire che «lo Stato membro di condanna deve considerarsi proprietario dell'informazione relativa alle condanne penali pronunciate, sul proprio territorio, contro cittadini di altri Stati membri» (v. *Risoluzione legislativa del Parlamento europeo del 17 giugno 2008 sulla proposta di decisione quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (5968/2008 – C6-0067/2008 – 2005/0267(CNS)*, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2008-0279&language=IT&ring=A6-2008-0207>; nonché, in precedenza, *Risoluzione legislativa del Parlamento europeo del 21 giugno 2007 sulla proposta di decisione quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM(2005)0690 – C6-0052/2006 – 2005/0267(CNS)*, <http://socialistgroup.org/sides/getDoc.do?type=TA&reference=P6-TA-2007-0279&language=IT&ring=A6-2007-0170>).

Per quel che concerne poi l'obbligo di risposta dello Stato di cittadinanza a una richiesta di informazioni sul passato criminale di un proprio cittadino, l'art. 7 della decisione n. 315 del 2009 distingue a seconda della circostanza che si tratti di domanda finalizzata all'impiego del dato in un procedimento penale oppure di un'istanza rivolta a fini diversi. Nel primo caso, lo Stato di cittadinanza dovrà trasmettere le informazioni relative: alle condanne pronunciate nello Stato membro di cittadinanza e iscritte nel casellario; alle condanne pronunciate da altri Stati membri che le siano state trasmesse dopo il 27 aprile 2012 (ossia tre anni dopo l'entrata in vigore della decisione quadro), in applicazione dell'art. 4, quali conservate ai sensi dell'art. 5; alle condanne pronunciate in altri Stati membri che le siano state trasmesse entro il 27 aprile 2012 e siano iscritte nel casellario giudiziario; alle condanne pronunciate in paesi terzi di cui abbia ricevuto notifica e che siano iscritte nel casellario giudiziario.

Laddove, invece, una richiesta di informazioni estratte dal casellario giudiziario venga rivolta all'autorità centrale dello Stato di cittadinanza a fini diversi da un procedimento penale, tale autorità centrale risponde «in conformità del diritto nazionale indicando le condanne pronunciate nello Stato membro di cittadinanza e quelle pronunciate in paesi terzi che le siano state notificate e siano iscritte nel suo casellario giudiziario» (art. 7, par. 2). Per quanto concerne le informazioni sulle condanne pronunciate in altro Stato membro e trasmesse allo Stato membro di cittadinanza, la decisione precisa che l'autorità centrale di quest'ultimo le trasmette «in conformità del diritto nazionale allo Stato membro richiedente»: nondimeno, prevede che, a monte, lo Stato di condanna, nel trasmettere le informazioni, possa comunicare allo Stato membro di cittadinanza che le informazioni relative alle condanne «non possono essere ritrasmesse per fini diversi da un procedimento penale»; in tal caso, l'autorità centrale dello Stato membro di cittadinanza dovrà comunicare allo Stato richiedente quale altro Stato aveva trasmesso tali informazioni, in modo da consentirgli di rivolgere una richiesta direttamente allo Stato membro di condanna[93]. Ancora una volta, dunque, è lo Stato di condanna a essere configurato come il reale proprietario delle informazioni.

Se il legislatore europeo ha deciso di non seguire la prospettiva dell'armonizzazione della disciplina del casellario giudiziario vigente nei diversi Paesi[94], nella decisione quadro si è prefissato quantomeno di fornire una definizione di "condanna", di "casellario giudiziario" e di "procedimento penale".

Quest'ultimo è inteso come riferibile alla fase precedente al processo penale, alla fase del processo penale stesso e a quella dell'esecuzione della condanna (art.

---

93 Il meccanismo appare complicato, in quanto si debbono coordinare le regole poste da tre diversi ordinamenti: al riguardo, cfr. *Parere del garante europeo della protezione dei dati sulla proposta di decisione-quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def.)*, cit., pp. 31-32 (§ 38, 39).

94 V. il considerando n. 16 della decisione quadro, ove si specifica che lo scopo della decisione «non è di armonizzare i sistemi nazionali dei casellari giudiziari degli Stati membri».

2, lett. *b*). Viene quindi recepita la nozione lata impiegata nella decisione quadro n. 675 del 2008[95].

Per quel che riguarda il concetto di "casellario giudiziario", il legislatore europeo rinvia in sostanza alle scelte effettuate dai singoli ordinamenti: esso va, infatti, inteso come «il registro nazionale o i registri nazionali in cui le condanne sono registrate conformemente al diritto nazionale».

Quanto al termine "condanna", si è assistito a un'evoluzione identica a quella che ha interessato la decisione quadro sulla considerazione delle sentenze di condanna: nella proposta iniziale si adottava una definizione lata – analoga a quella che compariva nella proposta di decisione del 2004 e che era poi scomparsa nella versione definitiva della decisione n. 876 del 2005[96] – ricomprendente, tanto la pronuncia di una giurisdizione penale, quanto quella di un'autorità amministrativa, emessa nei confronti della persona fisica o della persona giuridica. Nella versione recentemente approvata dal Consiglio, si fa invece riferimento a «ogni decisione *definitiva* di una giurisdizione penale nei confronti di una persona fisica in relazione ad un reato, nella misura in cui tali decisioni siano riportate nel casellario giudiziario dello Stato di condanna» (art. 2, lett. *a*). Anche in tale contesto, si è ragionevolmente deciso di circoscrivere la nozione alle sole decisioni pronunciate in ambito penale[97] e aventi carattere definitivo in base all'ordinamento nazionale[98], nonché di specificare che esse debbono riguardare una persona fisica: a seguito delle pressioni di alcuni Stati, però, il settimo considerando chiarisce che la limitazione dell'operatività del meccanismo tratteggiato dalla decisione «alla sola trasmissione di informazioni estratte dal casellario giudiziario relativamente alle persone fisiche non dovrebbe pregiudicare l'eventuale futura estensione dell'ambito di applicazione [...] allo scambio di informazioni relative alle persone giuridiche».

---

95 Cfr. *infra*, § 10.

96 Cfr. *supra*, § 5.

97 In tal senso, si era espresso il Parlamento europeo: v. emendamento 5 contenuto nella *Risoluzione legislativa del Parlamento europeo del 21 giugno 2007*, cit. Sulla disputa tra gli Stati membri in ordine alla latitudine del concetto di condanna, v. C. Stefanou – H. Xanthaki, "Conclusions", cit., pp. 379-380. Va notato, peraltro, che la definizione contenuta nella decisione differisce da quella fissata dall'art. 2 della decisione quadro n. 675 del 2008: l'art. 2, lett. a), fa riferimento infatti a «ogni decisione definitiva di una giurisdizione penale nei confronti di una persona fisica *in relazione ad un reato*, nella misura in cui tali decisioni siano riportate nel casellario giudiziario dello Stato di condanna». La definizione appare piuttosto ambigua nella parte in cui allude a decisioni pronunciate "in relazione ad un reato" ("in respect of a criminal offence" nella versione inglese): a rigor di logica, potrebbe rientrare in questa definizione anche una sentenza di proscioglimento. Pertanto, sarebbe stato forse preferibile riprendere la definizione contenuta nella decisione n. 675 del 2008 (sulla quale, cfr. *infra*, § 10), salva la precisazione relativa alle persone fisiche.

98 Si badi che non vi è una norma che miri a specificare – in chiave di armonizzazione – il concetto di definitività: tenendo conto della varietà delle regole operanti nei singoli ordinamenti, si potrebbero creare delle disparità, le quali potrebbero, in ultima analisi, frenare la circolazione delle informazioni.

Pur essendo stata ridotta la portata del termine "condanna" (e quindi il campo di operatività dello strumento normativo), la decisione quadro fa però riferimento a qualsiasi reato. Proprio da questo punto di vista, il Garante europeo – sia pure con una linea più sfumata rispetto all'opinione espressa in passato sulla proposta di decisione del 2004 – aveva lamentato il fatto che «il legislatore comunitario non spieghi, né nella motivazione, né in alcun altro documento ufficiale, perché mai la presente proposta sullo scambio di informazioni non si sia potuta limitare ai reati penali più gravi»[99].

Nel perfezionare il modello di casellario europeo a rete con snodo nello Stato di cittadinanza, la decisione quadro si sofferma ancora su un aspetto assai rilevante: quello delle condizioni di utilizzo dei dati personali. Nella logica di tutela del diritto alla protezione del dato, il legislatore europeo pone una disciplina che dovrà essere apprezzata quale *lex specialis* rispetto a quella prevista dalla decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[100]. Il perno intorno al quale ruota tale disciplina è il principio di finalità limitata: l'art. 9 stabilisce, infatti, che i dati personali trasmessi ai fini di un procedimento penale, «possono essere usati dallo Stato membro richiedente solo ai fini del procedimento penale per il quale sono stati richiesti» (par. 1); più stringenti, invece, i limiti all'utilizzo dei dati trasmessi per fini diversi da un procedimento penale: essi possono essere impiegati «dallo Stato membro richiedente, conformemente al suo diritto nazionale, solo per il fine per il quale sono stati richiesti e nei limiti specificati dallo Stato membro richiesto» (par. 2)[101]. Ad ogni modo, una deroga rispetto a tale regola è prevista nel caso in cui lo Stato membro richiedente debba utilizzare le informa-

---

99 Così, *Parere del garante europeo della protezione dei dati sulla proposta di decisione-quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def.)*, cit., p. 30 (§ 25).

100 V. *Parere del garante europeo della protezione dei dati sulla proposta di decisione-quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def.)*, cit., p. 33 (§ 46). Sulla decisione quadro in materia di protezione dei dati personali nel "terzo pilastro", v. *supra*, S. Ciampi, *op. cit.*, § 3.

101 Esprimono più di qualche perplessità sulla cautela con la quale la proposta disciplina lo scambio di informazioni per finalità diverse da quelle giudiziarie, J.B. Jacobs-D. Blitsa, *op. cit.*, pp. 130 sg.: gli Autori lamentano, in particolare, la mancata previsione esplicita – pur suggerita dallo studio effettuato dall'*Institute for International Research on Criminal Policy* (cfr. *supra*, nota 15) – della possibilità di effettuare richieste da parte di datori di lavoro, soprattutto nei casi di "*vulnerable profession*" (come, ad esempio, nel settore dell'educazione, in quello medico, finanziario, nei trasporti e nelle telecomunicazioni). Al riguardo, merita segnalare anche la *Relazione sulla proposta di decisione quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (5968/2008 – C6 0067/2008 – 2005/0267(CNS))*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0207+0+DOC+PDF+V0//IT>, ove si precisa che, in casi estremamente specifici quali quelli relativi agli istituti scolastici o di assistenza ai bambini, si dovrebbe poter scoprire se le persone che si intendono assumere abbiano precedenti penali.

zioni «per prevenire un pericolo grave e immediato per la pubblica sicurezza» (art. 9, par. 3)[102].

Quanto al secondo obiettivo della decisione quadro, consistente nella predisposizione di un formato standardizzato che consenta di scambiare le informazioni per via elettronica, va rilevato che essa contempla direttamente in allegato un modulo *standard* che andrà utilizzato per le richieste di informazioni e per le risposte da parte dello Stato di cittadinanza (art. 10)[103]. Inoltre, l'art. 11, par. 4 rinvia ad altra fonte – da adottare in conformità delle pertinenti procedure del trattato sull'Unione europea entro tre anni dall'entrata in vigore della decisione quadro – la predisposizione di un formato standardizzato e la definizione di ulteriori modalità per organizzare e agevolare gli scambi di informazioni[104].

8. La decisione istitutiva del sistema europeo di informazione sui casellari giudiziari (ECRIS)

Ancor prima dell'adozione definitiva, da parte del Consiglio, della decisione quadro relativa all'organizzazione e al contenuto degli scambi di informazioni estratte dal casellario giudiziario, la Commissione ha assunto un'autonoma iniziativa volta a dare esecuzione proprio all'art. 11, par. 4, di quella che sarà poi la decisione 2009/315/GAI. In attuazione di una delle previsioni della decisione che istituisce un programma specifico sulla giustizia penale per il periodo 2007-2013[105], nel maggio del 2008 ha presentato una proposta di decisione che istituisce il sistema europeo di informazione sui casellari giudiziari (*European Criminal Records Information System* - ECRIS), (COM (2008) 332 def.)[106].

---

102 A tale riguardo, il Garante europeo, pur condividendo che in tali eccezionali situazioni venga consentito l'utilizzo dei dati, auspica che sia previsto un controllo da parte delle autorità garanti (*Parere del garante europeo della protezione dei dati sulla proposta di decisione-quadro del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (COM (2005) 690 def.)*, cit., p. 33 (§ 47). D'altronde, analoga deroga al canone della finalità limitata è prevista dall'art. 8, par. 3, della decisione quadro n. 960 del 2006 (v. *supra*, S. Ciampi, *op. cit.*, § 9).

103 Nel compilare i formulari per richiedere le informazioni estratte dal casellario giudiziario o per rispondere alle istanze, le autorità competenti si avvalgono del Manuale di procedura: cfr., al riguardo, il *Documento del Consiglio n. 6397/3/06*, 12 luglio 2006, <http://register.consilium.europa.eu/pdf/it/06/st06/st06397-re03.it06.pdf>.

104 Cfr. *infra*, § 8.

105 Cfr. l'art. 3, lett. g, della *Decisione del Consiglio che istituisce per il periodo 2007-2013 il programma specifico «Giustizia penale», quale parte del programma generale su diritti fondamentali e giustizia*, in *GUUE*, L 58, p. 14. V. B. Piattoli, *Diritti fondamentali: obiettivi e programmi dell'Unione europea in materia di giustizia penale*, in "Diritto penale e processo", 2007, p. 549.

106 Il progetto è pubblicato all'indirizzo <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0332:FIN:IT:PDF>.

Si tratta di uno strumento diretto a costruire un sistema informatizzato di scambio di informazioni sulle condanne tra gli Stati membri, che dovrebbe consentire alle diverse autorità nazionali di comprendere senza difficoltà le informazioni che ricevono sulle condanne (considerando n. 6). A tal fine, la proposta di decisione si ispirava – come emerge dalla stessa relazione accompagnatoria e dalla parte motiva – in larga parte al progetto pilota concernente la rete dei casellari giudiziari (*Network of Judicial Registers*), varato da alcuni degli Stati membri[107]. Forse per questa ragione la proposta di decisione è stata accolta molto positivamente dalle delegazioni permanenti in Consiglio, le quali hanno espresso sin dall'inizio un sostegno generale: essa è stata, infatti, ritenuta indispensabile, sia per integrare la decisione quadro sull'organizzazione e il contenuto degli scambi sulle informazioni estratte dal casellario, sia per facilitare l'attuazione della decisione quadro relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale[108]. Nella stessa Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo, tradizionalmente assai attenta alle garanzie individuali, si è manifestato un orientamento sostanzialmente favorevole alla proposta, anche se con qualche riserva relativa soprattutto alla procedura di comitato contemplata per l'esecuzione della decisione[109].

È così che, a neanche un anno di distanza dalla proposizione e con poche modifiche, il progetto è stato adottato dal Consiglio, nella sessione del 6 aprile 2009, ossia subito dopo l'approvazione della decisione sull'organizzazione e il contenuto degli scambi di informazioni estratte dal casellario (n. 315 del 2009).

La decisione 2009/316/GAI[110] si muove lungo due direttrici: da un lato, definisce le linee dell'interconnessione elettronica degli archivi nazionali mediante la predisposizione del sistema europeo di informazione sui casellari giudiziari (ECRIS) (art. 3); dall'altro, prevede un formato standard di trasmissione delle informazioni (art. 4), diretto a garantire che lo scambio avvenga in modo omogeneo, informatizzato e facilmente traducibile con dispositivi automatizzati (considerando n. 6).

---

107 Cfr. *supra*, § 6.

108 Cfr. il *Documento del Consiglio n. 13586/08*, 29 settembre 2008, <http://register.consilium.europa.eu/pdf/en/08/st13/st13586.en08.pdf>, pp. 2-3. Va notato che anche il Parlamento inglese ha manifestato un certo gradimento per la proposta: cfr. *Select Committee on European Scrutiny. Thirtieth Report - European criminal records information system*, <http://www.parliament.the-stationery-office.co.uk/pa/cm200708/cmselect/cmeuleg/16-xxvii/1625.htm>.

109 V. la *Relazione sulla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2008/XX/GAI (COM (2008) 332 def. – C6-0216/2008 – 2008/0101(CNS))*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0360+0+DOC+PDF+V0//IT>, pp. 13 sg.

110 In *GUUE*, L 93, 7 aprile 2009, p. 33.

Sotto il primo profilo, va ricordato che l'interconnessione elettronica dei casellari giudiziari è parte del progetto "Giustizia elettronica" (*e-justice*), cui il Consiglio europeo ha più volte riconosciuto valore prioritario nel 2007 (considerando n. 4). Recentemente, la stessa Commissione, dopo aver ammesso che l'interconnessione dei casellari «è l'ambito nel quale i lavori in materia di giustizia elettronica hanno segnato maggiori progressi», ha confermato che la sua ulteriore implementazione rappresenta «la prima priorità in materia di giustizia elettronica»[111].

La scelta operata nella decisione è quella di creare «un sistema informatico decentrato basato sulle banche dati di casellari giudiziari di ciascuno Stato membro», che si compone di due elementi: *a*) un *software* di interconnessione; *b*) un'infrastruttura di comunicazione comune che forma una rete cifrata (art. 3, par. 1).

Si stabilisce espressamente che i tutti i dati estratti dai casellari giudiziari «sono conservati unicamente nelle banche dati gestite dagli Stati membri» e che, pertanto, la decisione «non si prefigge di istituire una banca dati centralizzata di casellari giudiziari» (art. 3, par. 2). Inoltre, si chiarisce che le autorità centrali degli Stati membri «non hanno un accesso diretto in linea alle banche dati di casellari giudiziari degli altri Stati membri» (art. 3, par. 3). L'opzione a favore di una rete paritaria di banche dati dotate di una certa autonomia – già evidente nella proposta della Commissione – è stata salutata con grande favore dal Garante europeo, il quale ha rilevato come essa consenta di scongiurare la duplicazione dei dati e conduca al contempo alla responsabilizzazione dello Stato membro[112]. Nondimeno, il Garante ha messo in guardia dai rischi che derivano dalla scelta di costituire una rete *peer to peer* per lo scambio di informazioni tra le banche dati nazionali: da un lato, ha richiamato l'attenzione sul fatto che, nella pratica, la suddivisione delle responsabilità tra le autorità centrali degli Stati membri non si produce da sola e risultano pertanto necessarie «misure supplementari, ad esempio per garantire l'aggiornamento e l'uguaglianza delle informazioni detenute dallo Stato membro che trasmette e da quello che riceve (stato di condanna e stato di nazionalità)»; dall'altro lato, tale architettura è fonte di grandi diversità nel modo in cui viene applicata dai vari Stati membri; diversità che risultano ancora più manifeste «in un contesto di grandi differenze tra le legislazioni nazionali (quale è il caso dei casellari giudiziari)». In quest'ottica, secondo il Garante

---

111 Così, la *Comunicazione della Commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo - Verso una strategia europea in materia di giustizia elettronica (COM (2008) 329 def.)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0329:FIN:IT:PDF>, pp. 7-8, ove si precisa l'importanza che gli scambi di informazione si estendano «oltre la cooperazione giudiziaria e integrino altri obiettivi (ad esempio controllare l'accesso a determinate professioni)».

112 V. *Parere del Garante europeo della protezione dei dati sulla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2008/.../GAI*, in *GUUE*, C 42, 20 febbraio 2009, p. 3.

saranno fondamentali le misure di esecuzione della decisione ai fini di garantire l'armonizzazione dell'uso della rete[113].

Per quel che riguarda l'infrastruttura di comunicazione comune, si propone di utilizzare la rete s-TESTA (art. 3, par. 5), almeno in una prima fase, salvo valutare in seguito l'opportunità di basarsi su una rete sicura alternativa gestita dalla Commissione. Pure sotto questo profilo, la scelta è apprezzata dal Garante, che sottolinea come si tratti di infrastruttura impiegata quale spina dorsale di altri sistemi europei (come il SIS): per di più, viene valutato positivamente il richiamo al ruolo ricoperto dalla Commissione – anche con riferimento ad altri sistemi, quali SIS, VIS ed Eurodac – di responsabile dell'efficienza e della sicurezza del *network* (art. 3, par. 5)[114].

Quanto, infine, al *software* per l'interconnessione, la decisione attribuisce la responsabilità agli Stati membri. Nondimeno, si riconosce alla Commissione la possibilità si fornire un *software* specifico per implementare il pacchetto comune di protocolli (considerando n. 17).

La seconda novità fondamentale introdotta dalla decisione è rappresentata dalla previsione dell'utilizzo di indicazioni numeriche per trasmettere le informazioni sulle condanne, al fine di agevolare la traduzione automatica e la reciproca comprensione delle informazioni stesse. Per quel che riguarda la denominazione o la qualificazione giuridica del reato, l'art. 4, par. 1, prescrive che «gli Stati membri menzionano il codice corrispondente a ciascuno dei reati menzionati nella trasmissione in base alla tavola dei reati di cui all'allegato A»; in ordine alle informazioni relative al contenuto della condanna (e segnatamente la pena), l'art. 4, par. 2, stabilisce che «gli Stati membri menzionano il codice corrispondente a ciascuna delle pene e misure menzionate nella trasmissione in base alla tavola delle pene e misure di cui all'allegato B».

Vengono, dunque, predisposte due tavole di riferimento alle quali le autorità debbono attingere per contrassegnare un'iscrizione: l'una è relativa alle categorie di reato (allegato A), l'altra è riferita invece alle categorie delle pene (allegato B)[115]. A ogni categoria di reato viene assegnato un codice, il quale viene poi parzialmente specificato con riguardo a ciascuna sottocategoria: solo per fare un esempio, alla categoria dei reati contro l'ambiente è assegnato il codice 0600 00, mentre la sottocategoria del danneggiamento o distruzione di specie animali o vegetali protette è contrassegnata con il codice 0601 00. Sono poi previsti tre parametri relativi al grado di realizzazione del reato (reato consumato e reato tentato), al

113 Ancora, *Parere del Garante europeo della protezione dei dati sulla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari*, cit., p. 3.

114 Cfr. *Parere del Garante europeo della protezione dei dati sulla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari*, cit., p. 4.

115 La tabella A prevede ventisei categorie di reati, che corrispondono anche alle categorie aperte alle quali si può ricorrere qualora non sia possibile ricondurre lo specifico reato a una sottocategoria (art. 4, par. 1).

grado di partecipazione allo stesso (autore principale, concorrente, istigatore) e all'esonero della responsabilità (infermità mentale o imputabilità diminuita), nonché l'indicazione della recidiva. Come risulta dall'ottavo considerando, nella definizione delle tabelle, il legislatore europeo ha tratto ampiamente spunto dalla categorizzazione usata nel progetto pilota e ha «tenuto conto anche delle definizioni comuni e armonizzate esistenti a livello europeo e internazionale, oltre che dei modelli di dati di Eurojust e Europol».

Ciò che viene specificato in termini molto precisi dal considerando n. 14 è che le tavole di riferimento delle categorie di reato e delle categorie delle pene e delle misure non sono volte in alcun modo «a stabilire equivalenze giuridiche tra i reati, le pene e le misure esistenti a livello nazionale». In altri termini, esse sono finalizzate unicamente ad aiutare il destinatario a comprendere meglio i fatti e i tipi di pene e misure contenuti nelle informazioni trasmesse, ferma restando la possibilità delle autorità competenti dello Stato ricevente di interpretare diversamente le informazioni stesse. Per parte sua, il Parlamento aveva auspicato l'inserimento di un'ulteriore precisazione volta a escludere che, attraverso le tavole di corrispondenza, la decisione intenda armonizzare la disciplina delle fattispecie penali e delle sanzioni[116]. Il Consiglio non ha ritenuto di aggiungere un tale chiarimento, che sembra desumersi pacificamente, tanto dalla *ratio* di fondo della decisione, quanto dal tessuto normativo.

In conclusione, si può affermare che, con le due decisioni 315 e 316 del 2009, è stato adottato a livello di Unione europea quel modello di casellario giudiziario europeo che è si è definito di "interconnessione diffusa" e che aveva rappresentato l'oggetto di una cooperazione "rafforzata" di un'avanguardia di Stati membri.

9. Lo studio di fattibilità di uno schedario di condannati cittadini di paesi terzi

Siffatto sistema di "interconnessione diffusa" – che ruota intorno allo Stato di cittadinanza – può funzionare per i cittadini dell'Unione, ma non evidentemente per le informazioni sulle condanne penali pronunciate nell'Unione europea nei confronti di cittadini di paesi terzi o di persone di cui non è nota la nazionalità. Per costoro avrebbe potuto funzionare il modello di "interconnessione centralizzata" proposto dal Libro bianco, ma, come s'è visto, questo non ha avuto fortuna.

È così che, su sollecitazione del Consiglio, la Commissione europea ha presentato – nel luglio del 2006 – un Documento sulla fattibilità di uno schedario di

116 Cfr. la *Risoluzione legislativa del Parlamento europeo del 9 ottobre 2008 sulla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2008/XX/GAI (COM(2008)0332 – C6-0216/2008 – 2008/0101(CNS))*, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2008-0465&language=IT&ring=A6-2008-0360>.

cittadini di paesi terzi condannati nell'Unione europea (COM (2006) 359 def.). In tale atto, quel modello centralizzato viene in sostanza ripreso per i soli cittadini di paesi terzi. Lo schedario centralizzato dovrebbe infatti avere un ruolo assai specifico: quello di «permettere a uno Stato membro che cerchi informazioni sul casellario giudiziale di una persona di ricevere la notifica immediata di quali altri Stati membri detengano informazioni al riguardo»[117]. Il che significa che lo Stato membro della condanna deve fornire allo schedario unicamente le informazioni necessarie per identificare i cittadini di paesi terzi (o le persone di cui non è nota la nazionalità) che abbiano subito una condanna. Alla richiesta del singolo Stato, fondata sui dati identificativi della persona, la banca dati centrale dovrebbe rispondere con un semplice *hit*, quando risulti presente una segnalazione: a questo punto, lo Stato interessato all'informazione potrà rivolgersi direttamente allo Stato detentore della stessa.

Non sfuggirà che il problema fondamentale di tale sistema è quello di garantire un certo grado di certezza dei dati di identificazione della persona. A tal fine, nel documento vengono prospettate, a livello teorico, tre ipotesi. La prima opzione è quella che passa attraverso la creazione di uno schedario contenente le sole informazioni alfanumeriche: in fondo, tranne Cipro e il Regno Unito, i casellari giudiziari degli altri Stati conservano soltanto questi dati. La seconda è quella di inserire dei dati biometrici e la terza è quella di includerli unicamente per i reati più gravi. Infine, la Commissione contempla la possibilità di non creare alcuno schedario, posto che la costruzione *ex novo* dell'archivio (sia pur limitato) è assai costosa e che il miglioramento dei tradizionali meccanismi di cooperazione giudiziaria o di polizia – con l'attuazione del principio di disponibilità, l'entrata in funzione del SIS II, lo sviluppo del sistema di informazione Europol e del VIS – potrebbe consentire allo Stato membro di ottenere attraverso questi canali le informazioni sul curriculum criminale del cittadino non comunitario o del soggetto la cui nazionalità è sconosciuta. Al riguardo, la Commissione ricorda come l'attuazione del principio di disponibilità potrà condurre a scambiare informazioni – quali profili del DNA e impronte digitali – assai utili proprio ai fini dell'identificazione dei soggetti interessati.

Al momento, quest'ultima sembra l'opzione prescelta, poiché allo studio di fattibilità non è seguita alcuna proposta normativa. Probabilmente, la Commissione si è resa conto che il progetto del registro europeo delle persone condannate aveva senso solo nella sua versione completa, ossia comprendente sia i cittadini europei che i cittadini di Paesi terzi. Quando la creazione dell'indice completo si è rivelata impossibile per l'opposizione degli Stati membri – o, meglio, di una parte importante di essi –, si è deciso di abbandonare anche il progetto relativo allo

---

117 Testualmente, *Documento sulla fattibilità di uno schedario di cittadini di paesi terzi condannati nell'Unione europea* (COM (2006) 359 def., 4 luglio 2006), <http://register.consilium.europa.eu/pdf/it/06/st11/st11453.it06.pdf>, p. 4.

schedario limitato. Ciò, sulla scorta di una valutazione molto semplice: lo schedario ristretto non costerebbe molto meno di quello completo (circa il quaranta per cento in meno) e, per gli extracomunitari o per i soggetti la cui nazionalità non è nota, l'individuazione dello Stato di condanna può avvenire con gli strumenti della cooperazione di polizia. In attuazione del Programma dell'Aia, si sta investendo molto sul miglioramento della loro efficienza e, quindi, la Commissione immagina che essi saranno tali da garantire la possibilità di identificare lo Stato o gli Stati di condanna. Una volta individuato il detentore dell'informazione, ad esso ci si potrà rivolgere mercé l'impiego dei canali agevolati della cooperazione giudiziaria.

10. La decisione quadro sulla considerazione delle pronunce di condanna in occasione di un nuovo procedimento penale

Nel Libro bianco, la Commissione aveva individuato due linee parallele di intervento: da un lato, quella relativa alle condizioni di circolazione delle informazioni sul curriculum criminale; dall'altro, quella riguardante le condizioni di utilizzazione delle informazioni sul passato penale negli Stati membri diversi da quello in cui è stata pronunciata la condanna. Anche sotto quest'ultimo profilo, il quadro emergente dall'analisi condotta nei Paesi europei era piuttosto sconfortante, in quanto risultava che le sentenze straniere – ivi comprese quelle emesse in altro Paese dell'Unione – non venivano affatto prese in considerazione, oppure venivano valutate in modo molto limitato.

Ciò, nonostante vi fosse in materia un apposito strumento normativo. Nell'ambito del Consiglio d'Europa era stata infatti adottata la Convenzione europea sulla validità internazionale dei giudizi repressivi (1970): l'art. 56 stabiliva che «ciascuno Stato contraente adotterà le misure legislative che riterrà appropriate per permettere ai suoi tribunali, al momento di emanare una sentenza, di prendere in considerazione qualsiasi precedente sentenza penale europea emanata per un altro reato, avendo udito l'imputato, al fine di aggiungere a tale sentenza tutti o alcuni degli effetti che le proprie leggi prevedono per sentenze emanate nel proprio territorio. Esso determinerà le condizioni in cui tale sentenza viene presa in considerazione». Tuttavia, solo quattro Stati membri avevano ratificato la Convenzione senza emettere riserve sull'applicazione dell'articolo 56 (Austria, Danimarca, Spagna e Svezia)[118]. Per parte sua, l'Italia, pur avendo approvato la l. 16 maggio 1977, n. 305, che disponeva la ratifica, non aveva mai deposi-

118 V. *Comunicazione della Commissione al Consiglio e al Parlamento europeo relativa a talune azioni da intraprendere nel settore della lotta contro il terrorismo e altre forme gravi di criminalità, in particolare per migliorare gli scambi di informazioni (COM (2004) 221 def.)*, 29 marzo 2004, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0221:FIN:IT:PDF>, p. 13.

tato il relativo strumento. Sicché, la Convenzione non è mai entrata in vigore nel nostro Paese[119].

Proprio tenendo conto della ridotta efficacia di tale fonte, nel Programma di misure per l'attuazione del principio del reciproco riconoscimento, la Commissione aveva assegnato assoluta priorità alla misura n. 2, consistente nell'adozione di strumenti volti ad attuare il principio secondo cui «il giudice di uno Stato membro deve essere in grado di tener conto delle decisioni penali definitive rese negli altri Stati membri» e, nel Libro bianco, si era impegnata ad avanzare una specifica proposta.

Pertanto, nel marzo del 2005, la Commissione ha presentato il progetto di decisione quadro del Consiglio relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale (COM (2005) 91 def.). Il punto di partenza del ragionamento della Commissione – esplicitato nella relazione accompagnatoria – è che l'impossibilità di attribuire a una decisione presa in un altro Stato membro effetti equivalenti a quella adottata sul territorio nazionale «è contraria al principio del reciproco riconoscimento e pone i cittadini in una situazione di disuguaglianza in occasione dell'apertura di eventuali nuovi procedimenti giudiziari, a seconda dei rispettivi luoghi di svolgimento dei primi procedimenti e di quelli dei successivi»[120].

La portata degli effetti che vengono in rilievo è limitata: non si tratta né dell'efficacia esecutiva, né del divieto di un secondo giudizio. La proposta, infatti, prende in considerazione la precedente condanna, non come comando imperativo suscettibile di essere eseguito, ma unicamente come un fatto storico. Per altro verso, si specifica che la sentenza deve riguardare un fatto diverso da quello per cui si procede. Ciò che interessa, insomma, è che essa venga valutata come un "mero" fatto storico – esattamente come la sentenza nazionale – prima, durante e dopo il processo penale instaurato nei confronti della stessa persona per un fatto diverso. Coerentemente, dunque, la proposta affida esplicitamente la disciplina dei profili legati al *ne bis in idem* a diversi testi normativi[121].

Circoscritto è anche l'obiettivo della proposta di decisione. Essa non è volta ad armonizzare la disciplina nazionale relativa agli effetti attribuiti alle condanne

---

119 Cfr. M. Pisani, *"Reinserimento" del condannato e cooperazione giudiziaria internazionale*, in "Rivista italiana di diritto e procedura penale", 2008, p. 524; Id., *Convenzione europea sulla validità internazionale dei giudizi repressivi: in tema di mancata ratifica*, in "Indice penale", 1984, p. 207.

120 Così, *Relazione alla Proposta di decisione quadro relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale (COM (2005) 18)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0091:FIN:IT:PDF>, p. 2.

121 V., ancora, la *Relazione alla Proposta di decisione quadro relativa alla considerazione delle decisioni di condanna*, cit., p. 3. Con riguardo al *ne bis in idem*, cfr. il *Libro verde sui conflitti di giurisdizione e il principio del ne bis in idem nei procedimenti penali*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0696:FIN:IT:PDF>.

precedenti, ma unicamente a statuire una piena equiparazione tra la decisione emessa in altro Stato dell'Unione e la decisione nazionale.

D'altra parte, sotto questo profilo, essa non rappresenta una novità assoluta. Il canone del pieno riconoscimento degli effetti della sentenza di condanna straniera era già stato affermato – sia pure ai fini specifici dell'applicazione della recidiva – dalla decisione quadro 2001/888/GAI[122]: nel novellare la decisione quadro 2000/383/GAI, relativa alla protezione dell'euro contro la falsificazione di monete, aveva previsto l'introduzione di un art. 9-*bis*, il quale stabiliva espressamente che «ciascuno Stato membro ammette il principio della recidiva alle condizioni esistenti nella sua legislazione nazionale e, a tali condizioni, riconosce quali *generatrici di siffatta recidiva le sentenze di condanna definitive pronunciate in un altro Stato membro* [corsivo nostro]».

È così che, dopo un accurato lavoro preparatorio da parte del *Working Party on Cooperation in Criminal Matters* e del comitato di coordinamento di cui all'art. 36 TUE, e dopo aver acquisito il parere del Parlamento europeo, il Consiglio ha approvato la decisione quadro 2008/876/GAI nella riunione del 24 luglio 2008[123]. Essa pertanto sostituisce l'art. 56 della Convenzione europea del 1970 ed è vincolante per gli Stati membri, che dovranno conformarvisi entro il 15 agosto 2010 (art. 5).

La decisione quadro traccia anzitutto il proprio spazio applicativo, adottando una definizione del concetto di "condanna". Si tratta di uno dei punti oggetto di un vivace confronto a livello di lavori preparatori. Riprendendo un'impostazione comune a quella alla base delle iniziative in materia di scambio di informazioni estratte dal casellario – tanto di quella del 2004, quanto a quella del 2005 –, la proposta faceva riferimento a una nozione lata di condanna, comprensiva delle decisioni amministrative. Di fronte all'opposizione di alcuni Stati membri e alla sollecitazione del Parlamento europeo[124], il Consiglio ha però ritenuto di adottare una nozione più puntuale di condanna, intesa come «decisione definitiva di una giurisdizione penale che stabilisca la colpevolezza di una persona per un reato» (art. 2). Peraltro, su richiesta di altri Stati, si è chiarito, nel terzo considerando, che quello previsto dalla decisione è un obbligo minimo: pertanto, «essa non dovrebbe impedire [...] agli Stati membri di prendere in considerazione, conformemente alle rispettive legislazioni ed allorché dispongono di informazioni pertinenti,

---

122 In *GUUE*, L 329, 14 dicembre 2001, p. 3. Sul carattere in qualche misura "pionieristico" di tale decisione ai fini dell'attuazione del canone del reciproco riconoscimento, cfr. *Comunicazione della Commissione al Consiglio e al Parlamento europeo sul reciproco riconoscimento delle decisioni giudiziarie in materia penale (COM (2005) 195 def.)*, cit., p. 380.

123 In *GUUE*, L 220, 15 agosto 2008, p. 32.

124 Cfr. l'emendamento n. 5 proposto dalla *Risoluzione legislativa del Parlamento europeo sulla proposta di decisione quadro del Consiglio relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione dell'apertura di un nuovo procedimento penale (COM(2005)0091 – C6-0235/2005 – 2005/0018(CNS))*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2006-0373+0+DOC+PDF+V0//IT>, p. 2.

ad esempio, le decisioni definitive di autorità amministrative le cui decisioni possono dar luogo a un ricorso dinanzi a una giurisdizione competente in materia penale, che stabilisca la colpevolezza di una persona per un reato o per un atto punibile in base al diritto nazionale perché configura una violazione di legge».

Ciò premesso, merita analizzare quello che è senza dubbio il nucleo della decisione quadro, ossia la disposizione dell'art. 3. Nel primo paragrafo, essa prescrive che «ciascuno Stato membro assicura che, nel corso di un procedimento penale nei confronti di una persona, le precedenti decisioni di condanna pronunciate in un altro Stato membro nei confronti della stessa persona per fatti diversi, riguardo alle quali sono state ottenute informazioni in virtù degli strumenti applicabili all'assistenza giudiziaria reciproca o allo scambio di informazioni estratte dai casellari giudiziari, siano prese in considerazione nella misura in cui sono a loro volta prese in considerazione precedenti condanne nazionali, e che sono attribuiti ad esse effetti giuridici equivalenti a quelli derivanti da precedenti condanne nazionali conformemente al diritto nazionale».

Si tratta di un testo piuttosto involuto, soprattutto se comparato a quello della proposta. Da esso traspare, anzitutto, la preoccupazione di chiarire che l'obiettivo non è affatto quello di imporre al singolo ordinamento di modificare la propria disciplina interna sugli effetti delle condanne: l'unica finalità è quella di equiparare le sentenze pronunciate in altro Stato dell'Unione a quelle interne, ove a queste sia attribuito dal diritto nazionale un qualche effetto[125]. In secondo luogo, non si può fare a meno di notare il riferimento – anch'esso inserito nel corso dei lavori preparatori – ai canali attraverso i quali l'autorità giudiziaria dello Stato deve avere avuto le informazioni sulla storia criminale dell'imputato. Questi non possono che coincidere con gli strumenti tradizionali dell'assistenza giudiziaria oppure con i meccanismi specifici di scambio delle informazioni estratte dai casellari. Evidentemente, la *ratio* di tale specificazione è quella di escludere l'operatività della norma laddove le informazioni siano ottenute attraverso strumenti meno garantiti, quali potrebbero essere quelli di cooperazione di polizia (come il SIS o Europol). Il che è confermato dalla circostanza che, nel considerando n. 6, è stata inserita la precisazione secondo la quale non è previsto alcun obbligo di

125 Va notato che il testo finale discende dall'accoglimento dell'emendamento n. 7 proposto nella *Risoluzione legislativa del Parlamento europeo sulla proposta di decisione quadro del Consiglio relativa alla considerazione delle decisioni di condanna*, cit., p. 3, e diretto proprio a chiarire che «il diritto nazionale è l'unico criterio per decidere se, e in quale misura, si debbano attribuire effetti giuridici alla condanna precedentemente emessa da un altro Stato» (così, la *Relazione della Commissione per le libertà civili, la giustizia e gli affari interni sulla proposta di decisione quadro del Consiglio relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione dell'apertura di un nuovo procedimento penale (COM(2005)0091 – C6-0235/2005 – 2005/0018(CNS))*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2006-0268+0+DOC+PDF+V0//IT>, p. 16).

prendere in considerazione le decisioni di condanna, qualora «le informazioni ottenute ai sensi degli strumenti applicabili non siano sufficienti»[126].

Il secondo paragrafo dell'art. 3 chiarisce l'ambito "spaziale" di applicazione della regola di equiparazione. Essa non opera soltanto nella fase strettamente processuale, ma anche in quella precedente al processo penale e in quella successiva allo stesso: il che significa che la locuzione "procedimento penale", inclusa nel titolo della decisione quadro, va intesa in senso davvero ampio. D'altra parte, già la relazione accompagnatoria alla proposta della Commissione lo aveva chiarito[127]. Si era infatti osservato che: durante la fase che precede il processo, l'esistenza di una condanna può influire, ad esempio, sulla scelta delle norme di procedura applicabili, sulla qualifica penale adottata per i fatti o sui provvedimenti relativi alla detenzione cautelare; nel corso del processo, invece, la presenza di condanne anteriori può avere conseguenze sul tipo di organo giurisdizionale competente e, ancor più spesso, sulla natura e sulla quantificazione della pena[128]; infine, nell'ipotesi in cui sia stata pronunciata una nuova condanna, la sussistenza di precedenti penali può assumere rilievo nella fase di esecuzione di quest'ultima, ostacolando, ad esempio, l'accesso ad alcuni istituti del diritto penitenziario.

A una prima lettura del testo, pare che la regola sull'equiparazione dell'efficacia "storica" della sentenza pronunciata in altro Stato dell'Unione sia destinata a operare senza alcuna eccezione. Gli unici due limiti che emergono dal testo sembrano essere: quello risultante dalla lettura congiunta dei parr. 3 e 4 dell'art. 3, in forza dei quali la sentenza straniera non può essere considerata se essa comporterebbe interferenze con la precedente decisione di condanna o con qualsiasi altra decisione relativa alla sua esecuzione; quello di ordine temporale, relativo alle condanne pronunciate o eseguite dopo il reato che è oggetto del secondo procedimento.

Ben diverso era l'approccio della proposta della Commissione, che prevedeva motivi obbligatori e facoltativi di non considerazione della precedente condanna. Secondo l'art. 4, le decisioni di condanna pronunciate da un altro Stato membro non avrebbero dovuto essere prese in considerazione in quattro casi: quando la decisione di condanna è contraria al principio del *ne bis in idem*; quando sarebbe intervenuta la prescrizione dell'azione penale secondo la legislazione nazionale al momento della condanna; quando il reato che ha dato luogo alla condanna

---

126 Cfr. *Documento del Consiglio 13101/06*, 26 settembre 2006, <http://register.consilium.europa.eu/pdf/it/06/st13/st13101.it06.pdf>, p. 4.

127 Cfr. la *Relazione alla Proposta di decisione quadro relativa alla considerazione delle decisioni di condanna*, cit., p. 5.

128 È significativo notare come la legge di riforma della recidiva, approvata in Francia nel dicembre del 2005 (l. n. 2005-1549 del 12 dicembre 2005), abbia previsto espressamente che «les condamnations prononcées par les juridictions pénales d'un Etat membre de l'Union européenne sont prises en compte au titre de la récidive» (art. 132-16-6 cod. pen.) (sul punto, v. B. Lapérou-Scheneider, *op. cit.*, p. 78, la quale, non a torto, mette in relazione le iniziative legate alla creazione di un casellario giudiziario europeo con la valorizzazione dell'istituto della recidiva).

rientra nell'ambito di un'amnistia e lo Stato membro aveva competenza a perseguire tale reato secondo la propria legge penale; quando la normativa nazionale che regola le iscrizioni nel casellario giudiziario nazionale avrebbe portato alla cancellazione della menzione della condanna. L'art. 5 della proposta consentiva, invece, di non tener conto della condanna nel caso di insussistenza del presupposto della doppia punibilità (salvo che si trattasse di una serie di reati specificamente indicati) e nell'ipotesi in cui il prendere in considerazione la condanna straniera avrebbe avuto come conseguenza un trattamento più sfavorevole per la persona rispetto all'ipotesi in cui la condanna fosse stata pronunciata da un giudice nazionale.

Ebbene, nonostante il parere contrario del Parlamento europeo[129], le due disposizioni sono state cancellate. Pertanto, il Consiglio sembrerebbe essere andato ben al di là della proposta della Commissione. In effetti, si è osservato in dottrina che, nel contesto di questo strumento normativo, gli Stati membri «should regard courts in other EU countries as 'sister courts' whose procedures and fact finding are fair and reliable»[130].

In realtà, da una lettura più attenta dell'intera decisione quadro emerge che alcuni limiti all'operatività della regola dell'equiparazione, inizialmente concepiti come motivi obbligatori o facoltativi di non considerazione, vengono spostati nella parte motiva. Il considerando n. 6 precisa, infatti, che la decisione quadro «non prevede alcun obbligo di prendere in considerazione decisioni di condanna precedenti, ad esempio qualora le informazioni ottenute ai sensi degli strumenti applicabili non siano sufficienti, qualora una decisione di condanna nazionale non sia stata possibile riguardo all'atto per cui la condanna precedente è stata emessa, o qualora la pena comminata in precedenza non sia contemplata dall'ordinamento giuridico nazionale». Tre quindi sono le eccezioni all'obbligo di equiparazione: la prima, come si è visto, risponde alla finalità di valorizzare i canali ordinari dello scambio di informazioni sui precedenti, che garantiscono una conoscenza completa degli stessi. Il riferimento all'"impossibilità della condanna" parrebbe comprensivo, tanto del richiamo all'amnistia e alla prescrizione, quanto di quello alla doppia incriminabilità. Se inteso in senso astratto – come pare indurre la versione inglese: «where a national conviction *would not have been possible*» – il considerando n. 6 indurrebbe a configurare la doppia incriminabilità come un requisito di operatività dell'obbligo di equiparazione. Anche sotto il profilo del richiamo alla sanzione, la decisione sembra aver fatto un passo indietro rispetto alla proposta, nella quale questo limite non compariva. Infine, il considerando n. 8 riprende l'eccezione che compariva nell'art. 5, par. 2, della proposta e raccomanda di evitare che – per effetto dell'equiparazione – la persona

---

129 Cfr. *Relazione della Commissione per le libertà civili, la giustizia e gli affari interni sulla proposta di decisione quadro del Consiglio relativa alla considerazione delle decisioni di condanna*, cit., p. 15.

130 Così, J.B. Jacobs-D. Blitsa, *op. cit.*, p. 121.

interessata «abbia un trattamento meno favorevole di quello che avrebbe se la condanna precedente fosse stata pronunciata da un giudice nazionale».

Vi è poi un altro considerando che, inserito per rispondere alle preoccupazioni di alcuni Stati membri[131], suscita più di qualche perplessità. Si tratta del numero 13 della versione definitiva, in forza del quale «l'esclusione della possibilità di riesame di una precedente decisione di condanna non dovrebbe impedire agli Stati membri di pronunciare, se necessario, una decisione che produca effetti giuridici equivalenti a quelli della precedente decisione di condanna». Tale puntualizzazione lascia probabilmente aperta la porta all'eventuale previsione, da parte dello Stato, di un qualche filtro (magari giurisdizionale) rispetto alla condanna straniera. Non sfuggirà, che proprio in tal modo si rischierebbe però di vanificare il risultato conseguito dal (quasi totale) superamento dei motivi di non considerazione. Al fine di minimizzare tale rischio, occorre dunque interpretare in modo molto rigoroso l'ultima parte del considerando, la quale chiarisce che «however, the procedures involved in issuing such a decision should not, in view of the time and procedures or formalities required, render it impossible to attach equivalent effects to a previous conviction handed down in another Member State»[132].

Al di là di tali dubbi, non si può negare che la decisione n. 675 del 2008 segni un significativo passo avanti nell'attuazione del principio del reciproco riconoscimento. Se attuata dagli Stati membri in termini rigorosi – o, comunque, per effetto del canone dell'interpretazione conforme alla decisione quadro, che vincola i giudici nazionali[133] – essa consentirà di precostituire le condizioni affinché possa entrare effettivamente in funzione quel sistema di scambio di informazioni sulle precedenti condanne disegnato dalle decisioni 315 e 316 del 2009.

11. Riflessioni conclusive

All'esito di questo percorso, si può rilevare come i due obiettivi indicati dalla Commissione nel Libro bianco del 2005 – quello relativo allo scambio di informazioni sulle condanne e quello riguardante l'impiego delle stesse nel procedimento penale – siano stati perseguiti con grande determinazione dallo stesso Consiglio. Ciò che è dipeso dal realizzarsi di una speciale saldatura tra la spinta all'integrazione europea e gli interessi degli Stati membri: in questi anni, infatti,

131 V. il *Documento del Consiglio n. 13568/06*, 18 ottobre 2006, <http://register.consilium.europa.eu/pdf/en/06/st13/st13568.en06.pdf>, p. 6.

132 Ancora una volta, si riporta la versione inglese, in quanto quella italiana appare viziata da un errore di traduzione che rende incomprensibile la portata della specificazione.

133 Cfr. *infra*, M. Gialuz, "Banche dati europee e procedimento penale italiano", § 3, nota 43.

in molti Paesi europei si sono andati diffondendo una «cultura del controllo»[134] e un diritto penale del tipo d'autore[135], che hanno portato ad attribuire una crescente importanza alla storia criminale del singolo, sia nell'ambito della giustizia penale intesa in senso lato (con riguardo all'applicazione di norme processuali, al trattamento sanzionatorio, nonché all'esecuzione della pena), sia in campi diversi (primo tra tutti quello dell'*employment screening*)[136]. In numerosi ordinamenti, tale tendenza si è accompagnata naturalmente all'inasprimento sensibile del trattamento della recidiva, sulla scia di quella (non certo felice) esperienza maturata negli Stati Uniti nel decennio precedente[137].

Proprio tale contesto politico-culturale ha indubbiamente agevolato, sia l'approvazione della decisione quadro 2008/675/GAI, sulla considerazione delle pronuncia di condanna nel nuovo procedimento penale, sia l'adozione delle decisioni n. 315 e 316 del 2009.

Come si è visto, queste due decisioni prevedono l'istituzione di un sistema europeo di informazione sui casellari nazionali a rete diffusa. In un certo senso, si tratta di una scelta coerente con un approccio che il legislatore europeo ha accolto in altri ambiti della cooperazione informativa: lo stesso Garante europeo per la protezione dei dati ha registrato un vero e proprio *trend* nel senso della creazione di «decentralised systems consisting of constellations of databases which will work more like peer to peer networks than centralised systems»[138]. È un'opzione che comporta evidentemente l'abbandono, non solo dell'ipotesi del casellario eu-

---

134 L'espressione è ripresa dal noto libro di D. Garland, *La cultura del controllo. Crimine e ordine sociale nel mondo contemporaneo*, ed. it. a cura di A. Ceretti, Milano, Il Saggiatore, 2007.

135 Cfr., tra i tanti, G. Flora, *Verso un diritto penale del tipo d'autore?*, in "Rivista italiana di diritto e procedura penale", 2008, p. 564; G. Messina, *La Corte di Cassazione contro il nuovo diritto penale dell'"autore recidivo" rifiuta l'applicazione obbligatoria della recidiva reiterata*, *ibidem*, p. 896; D. Pulitanò, "La cultura del controllo. Uno sguardo recente sulla storia del sistema penale italiano", in *Pena, controllo sociale e modernità nel pensiero di David Garland*, a cura di A. Ceretti, Milano, Giuffrè, 2005, p. 109.

136 Si legga, in particolare, T. Thomas, *op. cit.*, pp. 106 sgg.

137 V. S. Fiore, "La 'construction' de l'ennemi. La reforme de la recidive en Italie", in *Le nouveau droit de la récidive*, cit., p. 57, il quale segnala la singolare coincidenza per cui, nel dicembre del 2005, a distanza di poche settimane, sia la Francia che l'Italia hanno riformato l'istituto della recidiva. Con riguardo alla l. 5 dicembre 2005, n. 251, v., anche per ulteriori indicazioni, S. Corbetta, "Il nuovo volto della recidiva: 'tre colpi e sei fuori'?", in *Nuove norme su prescrizione del reato e recidiva*, a cura di A. Scalfati, Padova, Cedam, 2006, pp. 53 sgg.; A. Della Bella, *Three strikes and you are out: la guerra al recidivo in California e i suoi echi in Italia*, in "Rivista italiana di diritto e procedura penale", 2007, pp. 832 sgg.; E. Dolcini, *La recidiva riformata. Ancora più selettivo il carcere in Italia*, *ibidem*, pp. 515 sgg., il quale riferisce di un ripensamento della recidiva in senso lato anche nell'ordinamento tedesco (p. 519). Per un commento delle riforme del 2005 e del 2007 in Francia, v. i saggi pubblicati nel volume *Le nouveau droit de la récidive*, cit.

138 Testualmente, *Comments on the Communication of the Commission on interoperability of European databases*, 10 marzo 2006, <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2006/06-03-10__Interoperability__EN.pdf>, p. 4.

ropeo centralizzato, ma anche dell'alternativa tratteggiata nel Libro bianco.

Ebbene, l'idea di un indice europeo delle condanne non era affatto – come è stato detto – uno «*soothing compromise*»[139], al quale la Commissione era giunta venendo incontro alle richieste degli Stati membri. Si trattava invece di un modello di casellario giudiziario europeo a rete centralizzata assai più razionale ed efficiente rispetto a quello successivamente accolto nel progetto pilota e nella decisione quadro n. 315 del 2009.

Più razionale, anzitutto, per una ragione economica. Esso evita di far entrare nel meccanismo dello scambio di informazioni un soggetto statuale terzo (rispetto allo Stato di condanna e a quello interessato all'informazione), quale lo Stato di nazionalità. Il che è un vantaggio, perché l'inclusione dello Stato di nazionalità nel meccanismo dello scambio crea svariati problemi. Anzitutto, essa determina la necessità per lo Stato di condanna di comunicare a quest'ultimo, sia la condanna, sia i successivi aggiornamenti. Si potrebbe obiettare che ciò accadrebbe ugualmente nel caso dell'indice europeo. Ma non è così: in tale sistema lo Stato di condanna trasmetterebbe solo l'informazione che esiste un'iscrizione a carico di un soggetto oppure che questa è stata cancellata. In secondo luogo, il coinvolgimento dello Stato di cittadinanza porta con sé inevitabilmente il rischio di un possibile conflitto tra la disciplina dello Stato di condanna e quella dello Stato di cittadinanza. Tant'è che, come si è visto, la decisione quadro n. 315 del 2009, subito dopo aver riconosciuto la centralità dello Stato di cittadinanza come collettore delle informazioni, è costretta a configurare lo Stato di condanna come il vero *owner of the data*. Con questa irrisolta contraddizione, si finisce per aumentare inutilmente la complessità del sistema: già sono da mettere in conto le discrasie tra lo Stato richiedente e quello di condanna; dunque non sembra abbia senso creare artificiosamente il rischio di ulteriori conflitti.

Il modello del casellario con il baricentro nell'indice europeo si mostra altresì più efficiente. Anzitutto, sotto il profilo della tutela della privacy: come si è appena notato, il meccanismo posto a fondamento della proposta di decisione quadro determina una duplicazione dei dati, che raddoppia i rischi per l'interessato[140]. Ma il sistema in parola è senza dubbio più efficiente dal punto di vista della circolazione delle informazioni, per la semplice ragione che funziona naturalmente anche rispetto ai cittadini non europei e alle persone di cui non è nota la nazionalità.

Nonostante questi vantaggi del modello centralizzato, la scelta a favore di un casellario europeo a rete diffusa sembra ormai irreversibile. Rimane, allora, l'auspicio che un'iniziativa volta a creare un indice europeo delle condanne sia presa

---

139 Questa la locuzione utilizzata da C. Stefanou – H. Xanthaki, "Introduction: How did the idea of a European Criminal Record come about?", cit., p. 17.

140 Pertanto, non si può che condividere l'opinione di chi ha rilevato come «la protection de la vie privée puisse mieux être respectée dans la mise en place d'un tel dispositif [l'indice europeo] que dans celle d'une interconnexion des fichiers nationaux» (così, V. Havy, *op. cit.*, p. 174).

almeno con riferimento ai cittadini di Stati terzi e ai soggetti la cui nazionalità non è nota, per i quali il meccanismo messo in campo non può funzionare. Non è, infatti, ammissibile che, per costoro, ci si appoggi ai canali della cooperazione di polizia.

Per altro verso, non si può che richiamare il legislatore europeo ad attuare il necessario ravvicinamento delle garanzie processuali e della protezione dei dati personali. La piena attuazione del canone del reciproco riconoscimento, pure nella sua forma specifica di libera circolazione delle informazioni estratte dai casellari nazionali, postula infatti una fiducia reciproca, che si potrà raggiungere – soprattutto dopo l'allargamento – solo con l'armonizzazione delle garanzie processuali[141] e la fissazione di una solida cornice garantistica in tema di protezione dei dati.

Da quest'ultimo punto di vista, la decisione quadro 2008/977/GAI[142], sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale appare del tutto insoddisfacente. Essa, infatti, si riferisce soltanto ai trattamenti derivanti dalla cooperazione informativa e non si prefigge l'obiettivo dell'armonizzazione del trattamento domestico. E, dunque, con riguardo alla rettifica, alla cancellazione e al blocco dei dati personali contenuti nel casellario giudiziario, si limita semplicemente a rinviare alle norme nazionali (art. 4, par. 4). Alla luce di tale approccio rinunciatario della normativa generale e considerata la delicatezza dei dati relativi alle condanne penali[143], il legislatore europeo avrebbe dovuto inserire nella decisione quadro n. 315 del 2009 una disciplina specifica e puntuale, volta ad armonizzare gli ordinamenti nazionali quanto al profilo dei contenuti degli archivi, dei termini di conservazione, dei diritti dell'interessato e dei legittimati all'accesso[144].

---

141 In termini generali, cfr. il *Libro verde della Commissione. Garanzie procedurali a favore di indagati e imputati in procedimenti penali nel territorio dell'Unione europea*, <http://eur-lex.europa.eu/LexUriServ/site/it/com/2003/com2003__0075it01.pdf>. V., per tutti, M. Bargis, *Costituzione per l'Europa e cooperazione giudiziaria in materia penale*, in "Rivista italiana di diritto e procedura penale", 2005, p. 160; V. Mitsilegas, "Trust-building Measures in the European Judicial Area in Criminal Matters: Issues of Competence, Legitimacy and Inter-institutional Balance", in *Security Versus Freedom? A Challenge for Europe's Future*, a cura di T. Balzacq e S. Carrera, Ashgate, Aldershot, 2006, pp. 280 sgg.; T. Rafaraci, "Lo spazio di libertà, sicurezza e giustizia nel crogiuolo della costruzione europea", in *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, a cura di T. Rafaraci, Milano, Giuffrè, 2007, p. 14.

142 In *GUUE*, L 350, 30 dicembre 2008, p. 60. Su tale fonte, v. *supra*, S. Ciampi, *op. cit.*, § 5.

143 Si pensi che l'art. 6 della Convenzione n. 108 del Consiglio d'Europa equipara i dati di carattere personale relativi alle condanne penali ai dati indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose, nonché ai dati relativi allo stato di salute e alla vita sessuale: per queste categorie di informazioni viene sancito il divieto di elaborazione automatica e, comunque, una protezione supplementare rispetto a quella genericamente riconosciuta per i dati diversi.

144 Cfr., in tal senso, l'auspicio (rimasto inascoltato) di G. Busia, "La protezione dei dati personali", in *Verso l'Europa dei diritti*, a cura di G. Amato e E. Paciotti, Bologna, il Mulino, 2005, p. 148,

Con riferimento invece all'aspetto della promozione di garanzie minime in materia di processo penale, la vicenda relativa alla proposta di decisione quadro sui diritti dell'imputato nel processo non induce a grande ottimismo[145].

il quale sollecita anche un ripensamento sul piano nazionale.

145 Da ultimo, v. S. Allegrezza, *L'armonizzazione della prova penale alla luce del trattato di Lisbona*, in "Cassazione penale", 2008, p. 3892; C. Arangüena Fanego, *Proposta di decisione quadro su determinati diritti processuali nei procedimenti penali nel territorio dell'Unione europea*, *ivi*, 2008, p. 3058; M. Jimeno-Bulnes, "The Proposal for a Council Framework Decision on Certain Procedural Rights in Criminal Proceedings throughout the European Union", in *Security versus Justice? Police and Judicial Cooperation in the European Union*, a cura di E. Guild e F. Geyer, Ashgate, Aldershot, 2008, pp. 171 sgg.; B. Nascimbene, *Le garanzie giurisdizionali nel quadro della cooperazione giudiziaria penale europea*, in "Diritto penale e processo", 2009, p. 523.

Banche dati europee e procedimento penale italiano

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

Sommario: 1. Introduzione. – 2. I sistemi informativi quali strumenti di trasmissione di provvedimenti giudiziari o di richieste inerenti al procedimento. – 3. Le banche dati europee come contenitori di informazioni utili per l'accertamento dei fatti: il limite territoriale. – 4. (Segue): il limite funzionale. – 5. (Segue): il limite derivante dalla tutela del diritto alla protezione dei dati. – 6. Conclusioni.

1. Introduzione

In termini generali, è possibile individuare due tipologie molto diverse di rapporto tra le banche dati europee e il procedimento penale.

Il primo è quello che vede i sistemi informativi – soprattutto quelli centralizzati – impiegati come strumenti di trasmissione di un provvedimento o di una richiesta emessi nel corso di un procedimento giudiziario. In questi casi, la banca dati è destinataria di "impulsi" che provengono dall'autorità giudiziaria.

La seconda relazione, invece, è quella per cui la banca dati rappresenta un contenitore di informazioni, che possono essere utili per l'accertamento dei fatti e delle responsabilità. In quest'ottica, è il procedimento penale a essere destinatario di dati immagazzinati in archivi informatici.

In questo saggio, si analizzeranno entrambe le prospettive, prendendo in considerazione soltanto il procedimento penale italiano. Come si vedrà, la prima non pone particolari problemi sul piano teorico, mentre con riguardo alla seconda si affronteranno due interrogativi inediti e tra loro connessi. Da un lato, la questione relativa al se e in quale misura le banche dati europee possano divenire fonti di prova, ossia operare come sorgenti di elementi cognitivi utilizzabili nel procedimento penale; dall'altro, la domanda relativa al se e in quale misura il rafforzamento delle banche dati e della cooperazione informativa possa consentire di aggirare gli ostacoli della cooperazione giudiziaria.

2. I sistemi informativi quali strumenti di trasmissione di provvedimenti giudiziari o di richieste inerenti al procedimento

Quanto alla prima tipologia di rapporto tra banche dati e procedimento penale, il sistema informativo che più si presta a veicolare atti pronunciati in sede giudiziaria è senz'altro il SIS.

Va ricordata, anzitutto, la segnalazione ai fini dell'arresto, disciplinata dall'art. 95 CAAS, la quale ha gli stessi effetti della domanda di arresto provvisorio ai fini di estradizione prevista dall'art. 16 della Convenzione europea di estradizione[1]. Si è osservato che il numero di segnalazioni inserite ai sensi dell'art. 95 CAAS ai fini dell'arresto o dell'estradizione non è mai stato particolarmente elevato, soprattutto se paragonato a quello relativo alle segnalazioni degli stranieri ai fini della

1 Su tale sistema, cfr. J. P. Pierini, *Iscrizione della richiesta di arresto provvisorio ai fini estradizionali nel SIS, valutazione dell'urgenza e reiterazione dell'arresto ad opera della polizia giudiziaria*, in "Cassazione penale", 2000, p. 3071; L. Salazar, *L'estradizione nella Convenzione di Schengen*, in "Diritto penale e processo", 1998, p. 1034. In giurisprudenza, riconosce l'equiparazione dell'iscrizione nel SIS alla domanda di arresto provvisorio, Cass., sez. VI, 25 giugno 1999, Tepes, in "Cassazione penale", 2000, p. 3069.

non ammissione, effettuate ai sensi dell'art. 96 CAAS[2]. Nondimeno, va rilevato che proprio tale procedura ha consentito nel passato di procedere a importanti arresti, come a quelli di Cuntrera e Caruana in Spagna, o quelli di Gelli e Ocalan[3].

Com'è noto, tale strumento di diffusione è stato valorizzato dalla decisione quadro 2002/584/GAI in materia di mandato d'arresto europeo, la quale ha previsto la possibilità di dare attuazione al mandato d'arresto europeo proprio attraverso la segnalazione nel Sistema di Informazione Schengen (SIS). L'art. 9, par. 2, della decisione attribuisce all'autorità emittente il mandato d'arresto europeo il potere di disporre la segnalazione «in ogni caso», e, quindi, tanto nell'ipotesi in cui il luogo ove si trova il ricercato sia sconosciuto, quanto nell'evenienza in cui esso sia noto, ma vi sia l'esigenza di accelerare la procedura[4]. Per questo, si è sostenuto che la segnalazione nel SIS sarebbe divenuta la modalità ordinaria di trasmissione del mandato di arresto europeo[5]; e, in effetti, le rilevazioni statistiche sembrano confermare questa previsione[6].

Se effettuata conformemente all'art. 95 CAAS, tale segnalazione *equivale* a un mandato d'arresto europeo. Attualmente, però, poiché il SIS non può contenere tutte le informazioni necessarie, si precisa che l'equiparazione opera anche se non vengono inseriti tutti i dati, i quali vengono poi trasmessi dal SIRENE. Il problema dovrebbe essere risolto con l'avvio – ancora incerto nella data – del SIS II: la decisione del Consiglio dell'Unione 2007/533/GAI sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II)

---

2 È stato rilevato che la segnalazione effettuata *ex* art. 95 CAAS non ha mai raggiunto il due per cento di tutti i dati relativi alle persone: cfr. H. Busch, *The dream of total data collection - status quo and future plans for EU information systems*, <http://www.statewatch.org/analyses/no-61-eu-databases.pdf>, p. 1. Per le statistiche più recenti, cfr. il *Documento SIS Database Statistics dd. 01/01/2008, n. 5441/08*, 30 gennaio 2008, <http://register.consilium.europa.eu/pdf/en/08/st05/st05441.en08.pdf>, p. 2; nonché, il *Documento SIS Database Statistics dd. 01/01/2009, n. 5764/09*, 28 gennaio 2009, <http://register.consilium.europa.eu/pdf/en/09/st05/st05764.en09.pdf>, p. 2.

3 Cfr. A. De Felice, "Intervento", in Corpus iuris, *pubblico ministero europeo e cooperazione internazionale*, a cura di M. Bargis e S. Nosengo, Milano, 2003, p. 36. Per ulteriori casi di applicazione del SIS quale mezzo di trasmissione di richieste di estradizione, M. Pisani, *Domanda di arresto provvisorio a fini estradizionali e Sistema d'Informazione Schengen*, in "Rivista italiana di diritto e procedura penale", 2001, p. 332; Id., *Francia-Germania: il caso Sirven e il Sistema Schengen*, *ibidem*, p. 569.

4 V. M. Bargis, *Il mandato di arresto europeo dalla decisione quadro alle prospettive di attuazione*, in "Politica del diritto", 2004, p. 91.

5 Così, P. Troisi, "L'arresto operato dalla polizia giudiziaria a seguito della segnalazione nel sistema di informazione Schengen", in *Mandato di arresto europeo e procedure di consegna*, a cura di L. Kalb, Milano, Giuffrè, 2005, p. 176, 219 s.

6 V. il *Documento del Consiglio n. 10330/2/08*, 16 settembre 2008, <http://register.consilium.europa.eu/pdf/en/08/st10/st10330-re02.en08.pdf>, p. 3; *Documento del Consiglio n. 11371/2/07*, 27 luglio 2007, <http://register.consilium.europa.eu/pdf/en/07/st11/st11371-re02.en07.pdf>, p. 3. Anche secondo G. De Amicis, "Mandato d'arresto europeo", in *Lezioni di diritto penale europeo*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2007, p. 568, l'impiego del SIS per la trasmissione del mandato d'arresto ha un'alta incidenza statistica.

prevede, infatti, che, «nel caso di persone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto europeo, lo Stato membro della segnalazione inserisce nel SIS II una copia del mandato d'arresto europeo originale» (art. 27). Resta, inoltre, salvo lo scambio di ulteriori informazioni mediante gli uffici SIRENE.

La scelta di consentire la diffusione del mandato d'arresto mediante il SIS ha suscitato qualche perplessità da parte della dottrina, la quale ha rilevato che il sistema di informazione Schengen risulta inquinato da dati scorretti o non aggiornati[7]. Non si può negare che la constatazione sia per certi versi corretta: invero, si è lamentata spesso l'inefficienza dei meccanismi volti ad assicurare l'aggiornamento e la cancellazione dei dati inseriti nel SIS o, sul piano soggettivo, il diritto all'autodeterminazione informativa[8].

Ciò induce evidentemente a richiedere che siano migliorati i controlli sul SIS e che siano garantiti in termini effettivi i diritti di accesso, rettifica e cancellazione dei dati inseriti nel SIS. Da questo punto di vista, è fondamentale la piena attuazione della norma dell'art. 111 CAAS (e domani dell'art. 59 decisione 2007/533/GAI), la quale riconosce a chiunque il diritto di adire la giurisdizione o l'autorità competente in base al diritto nazionale con un'azione di rettifica, di cancellazione, di informazione o di indennizzo relativamente ad una segnalazione che lo riguardi[9]. Nondimeno, il funzionamento imperfetto dei meccanismi garantistici – riscontrato, giova specificarlo, soprattutto con riferimento alle segnalazioni effettuate *ex* art. 96 CAAS – non sembra poter condurre addirittura a contestare alla radice la stessa possibilità di impiegare il SIS per diffondere il mandato d'arresto europeo.

Per quel che riguarda specificamente la disciplina nazionale, che ha recepito la decisione quadro, occorre distinguere tra procedura passiva e attiva.

Quanto alla prima, l'art. 11 l. 69 del 2005 prevede che, «nel caso in cui l'autorità competente dello Stato membro ha effettuato la segnalazione nel Sistema di informazione Schengen (SIS) nelle forme richieste, la polizia giudiziaria procede all'arresto della persona ricercata». L'arresto segna l'inizio della procedura passiva: la polizia dovrà, infatti, porre l'interessato immediatamente – e comunque

---

7 Cfr. S. Buzzelli, "Il mandato d'arresto europeo e le garanzie costituzionali sul piano processuale", in *Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna*, a cura di M. Bargis ed E. Selvaggi, Torino, Giappichelli, 2005, p. 101.

8 Da ultimo, v. E. Brouwer, *The Other Side of Moon The Schengen Information System and Human Rights: A Task for National Courts*, <http://shop.ceps.eu/BookDetail.php?item__id=1642>, pp. 5 sgg.

9 Come ha rilevato E. Brouwer, *op. cit.*, p. 1, riprendendo quanto affermato dall'autorità di controllo Schengen, «the cornerstone in safeguarding data subjects' rights is the enforcement of final court decisions and data protection authorities by the member state issuing the SIS alert». Peraltro, la stessa Autorità di controllo ha rilevato come l'attuazione dell'art. 111 CAAS sia tutt'altro che soddisfacente (*Rapport de l'Autorité de contrôle commune de Schengen sur une enquête relative à la mise en œuvre de l'article 111 de la Convention d'application de l'Accord de Schengen*, 18 gennaio 2008, <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/shengen/rapport__schengen__article__111__francais.pdf>, p. 19).

non oltre ventiquattro ore – a disposizione del presidente della corte d'appello e dare immediata comunicazione dell'avvenuto arresto al Ministro della giustizia. Quest'ultima informazione è indispensabile – anche laddove la segnalazione nel SIS sia corredata di tutte le informazioni che lo rendono equivalente al mandato d'arresto europeo – per consentire al Ministro di attivarsi per chiedere l'inoltro del mandato e della documentazione ulteriore richiesta dall'art. 6, comma 4, l. 69 del 2005. La trasmissione del verbale al presidente della corte d'appello nel cui distretto l'arresto è stato eseguito è necessaria invece al fine di porre l'organo monocratico in condizione di decidere sulla convalida del provvedimento restrittivo della libertà personale, entro le successive quarantotto ore[10]. Ove non risulti che l'arresto sia stato eseguito per errore di persona o fuori dei casi previsti dalla legge, il presidente lo convalida con ordinanza, la quale, però, perde efficacia se, entro dieci giorni, non perviene il mandato d'arresto europeo o la segnalazione della persona nel SIS, corredata di tutte le indicazioni previste dall'art. 6 l. 69 del 2005.

Dottrina e giurisprudenza si sono soffermate su diversi i profili della disciplina, ma, per quel che ci riguarda, merita porre in rilievo due snodi problematici.

Il primo concerne la valenza della segnalazione del SIS ai fini dell'arresto: sulla scorta della lettura congiunta dell'art. 11 l. 69 del 2005, dell'art. 9 della decisione quadro e degli artt. 64 e 95 CAAS, la dottrina aveva prospettato il carattere automatico dell'arresto[11]. In effetti, la giurisprudenza ha confermato che, in presenza di una segnalazione nel SIS, l'arresto da parte della polizia giudiziaria si configura come «atto 'dovuto'»: esso è subordinato soltanto alla verifica che la relativa segnalazione sia stata effettuata da una "autorità competente" di uno Stato membro dell'Unione europea e che la stessa sia avvenuta nelle "forme richieste", mentre va esclusa qualsiasi valutazione in ordine all'urgenza dell'arresto[12]. Inoltre, si è precisato che l'obbligo dell'arresto deriva dalla mera segnalazione nel SIS, la quale può anche precedere temporalmente il mandato d'arresto europeo: la segnalazione nel SIS equivale, infatti, a una «richiesta di 'arresto preventivo ai fini della consegna'»[13].

Siffatta disciplina ha suscitato più di qualche perplessità, nella parte in cui configura l'arresto come automatico. Si è sostenuto, invero, che essa non sarebbe pienamente compatibile con l'art. 13, comma 3, Cost., il quale richiede la ricorrenza di «casi eccezionali di necessità e urgenza» affinché l'autorità di pubblica

---

10 Cfr., per tutti, M.R. Marchetti, "Mandato d'arresto europeo", in *Enciclopedia del diritto. Annali*, II.1, Milano, Giuffrè, 2008, p. 548.

11 Cfr. N. Galantini, *L'adattamento del mandato d'arresto europeo nella legge attuativa della decisione quadro*, in "Cassazione penale", 2005, p. 4089; Ead., *Prime osservazioni sul mandato d'arresto europeo*, in "Foro ambrosiano", 2002, p. 267.

12 Così, Cass., sez. VI, 5 giugno 2006, Volanti, in "Diritto e giustizia", 2006, n. 28, p. 56. Analogamente, O. Villoni, "Il mandato d'arresto europeo: autorità competenti e contenuto", in *Mandato d'arresto europeo*, cit., p. 200.

13 Testualmente, Cass., sez. VI, 22 novembre 2005, Calarese, in "Foro italiano", 2006, II, c. 280.

sicurezza possa adottare provvedimenti provvisori di limitazione della libertà personale[14]. Secondo un'interpretazione costituzionalmente orientata sarebbe pertanto necessaria una valutazione sull'urgenza e, pertanto, sull'esistenza di un concreto pericolo di fuga da parte della persona segnalata[15]. In realtà, la Cassazione ha dichiarato manifestamente infondata la questione di legittimità costituzionale sollevata con riferimento all'art. 11 nella parte in cui esclude un tale vaglio: a detta dei giudici di legittimità, infatti, nel caso in questione non può essere invocato l'art. 13, comma 3, Cost., perché non si è in presenza di un arresto eseguito in un caso eccezionale dalla polizia giudiziaria, ma dell'esecuzione di un provvedimento della competente autorità giudiziaria[16].

Il secondo profilo problematico concerne gli atti che debbono essere trasmessi per evitare la caducazione del provvedimento di convalida adottato dal presidente della corte di appello: come si è notato, l'art. 13 l. 69 del 2005 prevede che l'ordinanza di convalida perde efficacia se, nei dieci giorni successivi all'adozione, non perviene il mandato di arresto oppure la segnalazione della persona nel SIS, la quale equivale al mandato d'arresto «purché contenga le indicazioni di cui all'articolo 6». Ora, proprio quest'ultimo richiamo ha suscitato qualche dubbio interpretativo, in quanto l'art. 6 prevede al primo comma una serie di elementi che sono presenti nel mandato d'arresto e, quindi, anche nella segnalazione nel SIS; al comma quarto, invece, contempla la trasmissione di atti ulteriori il cui contenuto non si desume generalmente dalla segnalazione nel SIS. Pertanto, la giurisprudenza è stata chiamata a chiarire se il provvedimento perda efficacia anche nel caso di trasmissione della sola segnalazione non accompagnata da tali atti (in particolare, il problema si è posto con riguardo al mancato invio della relazione sui fatti addebitati alla persona). La Corte di cassazione ha escluso tale eventualità, ritenendo che l'equipollenza della segnalazione rispetto al mandato d'arresto sussiste quando essa presenta i requisiti di cui al comma primo dell'art. 6 l. 69 del 2005: insomma, il richiamo all'art. 6 andrebbe limitato alla sola disposizione del primo comma[17].

---

14 V. M. Tiberi, *Il mandato d'arresto europeo*, Roma, Istituto Poligrafico e Zecca dello Stato, 2006, p. 104; P. Troisi, *op. cit.*, pp. 213 sg.

15 In questi termini, A. Scalfati, *La procedura passiva di consegna*, in "Diritto penale e processo", 2005, p. 950.

16 Così, Cass., sez. VI, 5 giugno 2006, Volanti, cit., p. 56.

17 Cass., sez. VI, 13 dicembre 2005, Cusini, in "Cassazione penale", 2006, p. 3567, la quale ha precisato che «la relazione, al pari degli altri elementi indicati nel comma 4, è necessaria ai fini della decisione sulla richiesta di consegna, ma non costituisce elemento necessario della segnalazione»; analogamente, da ultimo, Cass., sez. VI, 23 aprile 2008, R.P., in "CED Cassazione", n. 239427; Cass., sez. VI, 23 dicembre 2008, P.m. in c. S.B., inedita. In termini critici rispetto a tale soluzione giurisprudenziale, R. Belfiore, *Mandato d'arresto europeo e segnalazione nel SIS: quali atti possono essere richiesti all'autorità di emissione?*, in "Cassazione penale", 2006, pp. 4121 sgg.; D. Servi, *Mandato di cattura europeo: segnalazione nel S.I.S. e requisiti necessari alla misura cautelare*, *ivi*, 2006, pp. 3572 sgg.; nonché, in precedenza, A. Barazzetta-R. Bricchetti, *Misure cautelari: rinvii*

In relazione alla procedura attiva, l'art. 29, comma 2, l. n. 69 del 2005 assegna direttamente all'autorità giudiziaria competente per l'emissione del mandato – ossia al giudice, se si tratta di mandato basato su un provvedimento cautelare e al pubblico ministero, se si è al cospetto di un mandato vòlto a eseguire una sentenza definitiva – il potere di disporre l'inserimento nel SIS della segnalazione della persona. Concretamente, l'autorità giudiziaria, dopo aver adottato il mandato d'arresto secondo un modello corrispondente a quello allegato alla decisione quadro, dovrà predisporre i formulari Schengen A ed M – che contengono le informazioni richieste dall'art. 95, par. 2, CAAS – e trasmetterli alla Divisione SIRENE della Direzione Centrale di Polizia Criminale-Servizio per la Cooperazione Internazionale di Polizia[18]. Peraltro, fintanto che non sarà operativo il SIS-II, al quale aderiranno tutti gli Stati membri dell'Unione, l'autorità emittente dovrà diffondere le ricerche attraverso il Servizio Interpol (per quel che riguarda gli Stati non connessi al SIS). Essa dovrà, inoltre, provvedere, tramite il competente ufficio di polizia, a inserire i dati relativi alla persona ricercata nel Sistema Informatizzato Interforze di polizia[19]. Sempre alla stessa autorità giudiziaria competente ai sensi dell'art. 28 l. 69 del 2005 spetterà chiedere l'eliminazione della segnalazione dal SIS, nel caso di revoca, annullamento o perdita di efficacia del provvedimento restrittivo[20].

A parte la segnalazione effettuata per consentire l'esecuzione di un mandato d'arresto europeo – che, ove non si applichi la decisione quadro avrà l'efficacia della richiesta di arresto per fini di estradizione –, la Convenzione di applicazione dell'accordo di Schengen contempla altre segnalazioni che sono volte a consentire l'esecuzione – in luoghi non predefinibili – di atti rilevanti per il procedimento penale.

Giova ricordare, anzitutto, la segnalazione prevista dall'art. 98 CAAS. Siffatta disposizione consente di inserire nel sistema, su richiesta dell'autorità giudiziaria, i dati «relativi ai testimoni, alle persone citate a comparire dinanzi all'autorità giudiziaria nell'ambito di un procedimento penale per rispondere di fatti che sono stati loro ascritti, o relativi alle persone alle quali deve essere notificata una sentenza penale o una richiesta»: la segnalazione viene introdotta ai fini della co-

---

al rito da decifrare, in "Guida al diritto", 2005, n. 19, pp. 85-86; A. Scalfati, *La procedura passiva di consegna*, cit., p. 949. Nella giurisprudenza di merito, va segnalata anche Corte App. Bologna, 21 giugno 2005, Guillemin, in "Foro italiano", 2005, II, c. 522, la quale ha riconosciuto che il giudice può decidere anche sulla richiesta di esecuzione sulla base degli atti trasmessi attraverso il SIS e alla documentazione inviata tramite il SIRENE.

18 Cfr. la *Circolare ministeriale n. 1-1489/05/U del 24 giugno 2005*, in "Rivista italiana di diritto e procedura penale", 2006, p. 389; nonché, G. Iuzzolino, *L'emissione del mandato d'arresto europeo tra ermeneutica e prassi*, in "Cassazione penale", 2008, p. 2126.

19 V. ancora G. Iuzzolino, *L'emissione del mandato d'arresto europeo*, cit., p. 2127.

20 Cfr. F. Siracusano, "Il procedimento di emissione del mandato d'arresto europeo", in *Mandato d'arresto europeo*, cit., p. 406.

municazione del luogo di soggiorno o del domicilio dei soggetti. Nella decisione 2007/533/GAI tale segnalazione viene implementata: il capo VII è dedicato proprio alla «segnalazione di persone ricercate per presenziare ad un procedimento giudiziario» e l'art. 35 prevede che le informazioni richieste vengano comunicate allo Stato membro richiedente «tramite scambio di informazioni supplementari», laddove oggi la trasmissione avviene conformemente alla disciplina nazionale e alle vigenti convenzioni relative all'assistenza giudiziaria (art. 98, par. 2, CAAS). Negli anni, il numero di soggetti segnalati per fini giudiziari è progressivamente cresciuto – si è passati dalle 35.317 segnalazioni *ex* art. 98 CAAS presenti nel 2005, alle 64.684 del 2008, e, infine, alle 72.958 segnalazioni presenti nel 2009[21] –, ma siffatta opportunità non è ancora sufficientemente praticata, nonostante la sua indubbia utilità anche al fine di ridurre il numero degli irreperibili.

Altrettanto significativa nell'ottica della ricerca di un oggetto rilevante ai fini dell'accertamento penale è la segnalazione prevista dall'art. 100 CAAS. Tale norma consente, infatti, di inserire nel SIS i «dati relativi agli oggetti ricercati a scopo di sequestro o di prova in un procedimento penale». Per la verità, non può trattarsi di qualsiasi bene, ma soltanto degli oggetti rubati, altrimenti sottratti o smarriti, indicati dalla stessa statuizione. Si tratta di veicoli a motore di una certa cilindrata, di rimorchi e roulotte, di armi da fuoco, di documenti intatti o di documenti d'identità rilasciati (passaporti, carte d'identità, patenti di guida) oppure, infine, di banconote registrate.

In effetti, questa forma di segnalazione è ben più utilizzata, tant'è che la decisione SIS II – nell'apposito capo intitolato «segnalazione di oggetti a fini di sequestro o di prova in un procedimento penale» – ha esteso il novero degli oggetti che possono essere segnalati, ricomprendendovi natanti e aeromobili, certificati di immatricolazione per veicoli e targhe di veicoli, nonché valori mobiliari e mezzi di pagamento, quali assegni, carte di credito, obbligazioni, titoli e azioni, rubati, altrimenti sottratti, smarriti o falsificati (art. 38). Anche per queste segnalazioni, la decisione SIS II ha previsto che, qualora dall'interrogazione emerga l'esistenza di una segnalazione per un oggetto rinvenuto, l'autorità che la constata si mette in contatto con l'autorità che ha effettuato la segnalazione per concordare le misure necessarie e che le indicazioni relative vengano trasmesse tramite il veicolo delle informazioni supplementari.

Come si vede, il sistema informativo Schengen presenta molteplici possibilità di impiego in relazione al procedimento penale (inteso in senso lato). A seconda delle scelte del legislatore europeo, esso potrà fungere da vero e proprio canale di trasmissione di quella che è stata suggestivamente definita eurordinan-

---

21 Cfr. *Documento SIS Database Statistics dd. 01/01/2005*, 2 giugno 2005, <http://register.consilium.europa.eu/pdf/en/05/st08/st08621.en05.pdf>, p. 2; *Documento SIS Database Statistics dd. 01/01/2008*, cit., p. 2; nonché, il *Documento SIS Database Statistics dd. 01/01/2009*, cit., p. 2.

za[22] – come accade nel caso del mandato d'arresto europeo – oppure potrà funzionare come mezzo di ricerca preliminare che rende possibile l'innesco di una cooperazione giudiziaria: la scoperta della persona o dell'oggetto aprirà infatti un procedimento di cooperazione, che varia a seconda degli strumenti giuridici disponibili.

Nell'ipotesi in cui il bene individuato tramite il SIS vada sottoposto a sequestro o confisca, potrà essere adottato un provvedimento di blocco o di sequestro ai sensi della decisione quadro 2003/577/GAI[23]. Per la verità, in tal caso, il sistema SIS potrebbe forse essere utilizzato anche come strumento indiretto di esecuzione di un provvedimento già adottato in relazione a un bene la cui localizzazione non sia nota: in tale evenienza, la segnalazione nel SIS potrebbe essere volta a localizzare il bene e, quindi, in ultima analisi, a eseguire il provvedimento. Non si ha invece la possibilità di una vera e propria trasmissione dell'eurordinanza tramite il SIS, in quanto l'art. 4 della decisione quadro ne prevede in ogni caso l'invio diretto all'autorità giudiziaria competente per l'esecuzione. Qualora questa non sia nota, si prescrive che l'autorità giudiziaria dello Stato di emissione si attivi attraverso tramite i punti di contatto della Rete giudiziaria europea.

Nel caso in cui la segnalazione si riferisca a un bene ai fini di prova, la sua scoperta potrà condurre oggi all'emissione di un mandato europeo di ricerca della prova volto ad acquisire l'oggetto: dopo un *iter* preparatorio piuttosto travagliato è giunta in porto la decisione quadro relativa al mandato europeo di ricerca delle prove (2008/978/GAI)[24]. Il problema è che questa non contempla il SIS quale pos

---

22 Cfr. G. Iuzzolino, "La decisione sull'esecuzione del mandato d'arresto europeo", in *Mandato d'arresto europeo*, cit., p. 274.

23 In *GUUE*, L 196, 2 agosto 2003, p. 45.

24 In *GUUE*, L 350, 30 dicembre 2008, p. 72. Sul mandato europeo di ricerca della prova, cfr., tra i tanti, S. Allegrezza, "Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo", in *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, a cura di T. Rafaraci, Milano, Giuffrè, 2007, p. 691; R. Belfiore, *Il mandato europeo di ricerca delle prove e l'assistenza giudiziaria nell'Unione europea*, in "Cassazione penale", 2008, p. 3894; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale*, Milano, Giuffrè, 2007, pp. 156 sgg.; Id., *Il mandato europeo di ricerca delle prove: un'introduzione*, in "Cassazione penale", 2008, p. 3033; A. IJzerman, "From the CATS Portfolio: The European evidence warrant", in *European evidence warrant. Transnational Judicial Inquiries in the EU*, a cura di J.A.E. Vervaele, Antwerpen, Intersentia, 2005, pp. 5 sgg.; N. La Rocca, "Prova (prospettive europee)", in *Digesto delle discipline penalistiche*, IV Agg., Torino, Utet, 2008, pp. 840 sgg.; G. Melillo, "Il mutuo riconoscimento e la circolazione della prova", in *L'area di libertà sicurezza e giustizia*, cit., p. 465; J.R. Spencer, "The problems of trans-border evidence and European initiatives to resolve them", in *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2008, p. 477; C. Williams, "Overview of the Commission's proposal for a Framework Decision on the European evidence warrant", in *European evidence warrant*, cit., pp. 69 sgg. Da ultimo, si veda la *Relazione sulla proposta di decisione quadro del Consiglio relativa al mandato europeo di ricerca delle prove diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali*

sibile veicolo di trasmissione del mandato europeo: l'art. 8 prevede, infatti, che il MER (mandato europeo di ricerca delle prove) possa essere trasmesso direttamente «all'autorità competente di uno Stato membro in cui l'autorità competente dello Stato di emissione abbia motivi legittimi per ritenere che si trovino o, nel caso di dati elettronici, che siano direttamente accessibili in base alla legislazione dello Stato di esecuzione oggetti, documenti o dati pertinenti». Anche in tal caso, come in quello della decisione n. 577 del 2003, l'alternativa è la trasmissione mediante il sistema di telecomunicazione protetto della Rete giudiziaria europea (art. 8, par. 3).

La scelta compiuta dal legislatore europeo dipende probabilmente dalla circostanza che l'emissione del mandato di ricerca della prova presuppone generalmente la previa identificazione dell'oggetto e quindi dello Stato in cui si trova il bene. Il sistema che ne deriva è tale per cui, per ricercare un bene da acquisire a fini di prova, si può utilizzare il SIS: solo una volta che tale bene sia individuato, si potrà emettere il MER e trasmetterlo direttamente all'autorità dello Stato competente. Siffatta opzione appare limitativa, soprattutto se la si confronta con quella effettuata in tema di mandato d'arresto, ove pure viene in gioco il bene essenziale della libertà personale. In particolare, appare irragionevole che l'inserimento nel SIS a fini di ricerca dell'oggetto di prova possa riguardare soltanto determinati beni (come si è visto, solo quelli indicati nell'art. 100 e nell'art. 38 decisione SISII).

3. Le banche dati europee come contenitori di informazioni utili per l'accertamento dei fatti: il limite territoriale

Ancor più interessante e problematica si presenta la prospettiva *lato sensu* probatoria, che vede i soggetti coinvolti nel procedimento penale come fruitori delle informazioni *contenute nelle* o *prodotte dalle* banche dati europee.

Da questo punto di vista, la domanda centrale è se, e in quale misura, le banche dati europee possono operare come fonti di prova in senso tecnico, ossia come sorgenti di elementi cognitivi utilizzabili nel procedimento penale. La risposta a tale interrogativo passa attraverso una precisazione preliminare e l'analisi di tre profili problematici strettamente connessi tra di loro.

La precisazione riguarda la nozione di banche dati europee, la quale va intesa in senso molto ampio. In essa vanno ricompresi, tanto gli archivi centrali dell'Unione – quali SIS, SID, TECS di Europol, EPOC-II di Eurojust, Eurodac, VIS –, quanto le banche dati istituite a fini preventivi e repressivi dai singoli Stati membri, quali in particolare le banche dati di polizia[25], gli archivi contenenti in-

---

(13076/2007 – C6-0293/2008 – 2003/0270(CNS), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0408+0+DOC+PDF+V0//IT>, pp. 1 sgg.

25 Si allude ad archivi corrispondenti a quello che è il Centro elaborazione dati del Dipartimento

formazioni dattiloscopiche[26] e le banche dati genetiche[27]. Proprio l'attuazione del principio di disponibilità ha portato anzitutto all'introduzione di legami più o meno stretti tra queste diverse basi di dati nazionali, secondo il modello dell'in-

---

della pubblica sicurezza, istituito presso il Ministero dell'Interno (Ufficio per il coordinamento e la pianificazione), con l'art. 8 l. 1 aprile 1981, n. 121: al riguardo, per tutti, M. Bonetti, *Riservatezza e processo penale*, Milano, Giuffrè, 2003, pp. 288 sgg.; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, Giuffrè, 1997, pp. 565 sgg.; A.A. Dalia, sub *artt. 7-11*, in "Legislazione penale", 1982, pp. 50 sgg.; P. Gallerini Monaci, *Il Centro elaborazione dati presso il Ministero dell'interno. Problemi e prospettive*, in "Rivista trimestrale di diritto e procedura civile", 1984, pp. 540 sgg.; A. Intini – A.R. Casto – D.A. Scali, *Investigazione di polizia giudiziaria*, Roma, Laurus Robuffo, 2006[7], pp. 91 sgg.; L. Mone, *L'amministrazione della pubblica sicurezza e l'ordinamento del personale*, Roma, Laurus Robuffo, 2007[15], p. 62; M. Pisani, *Criminalità organizzata e cooperazione internazionale*, in "Rivista italiana di diritto e procedura penale", 1998, p. 711. Solo per citarne alcune, si pensi al *Police National Computer*, operante presso l'*Home Office* della Gran Bretagna (cfr. *Database State*, <http://www.jrrt.org.uk/uploads/database-state.pdf>, pp. 21 sg.; T. Thomas, *Criminal Records. A Database for Criminal Justice System and Beyond*, New York, Palgrave Macmillan, 2007, pp. 27 sgg.), o all'INPOL, utilizzato dal *Bundeskriminalamt* tedesco (cfr. *The Bundeskriminalamt Facts and Figures 2008*, <http://www.bka.de/profil/broschueren/facts2008.pdf>, p. 10), oppure, ancora, al *Système de circulation hiérarchisée des enregistrements opérationnels de la police sécurisés* (CHEOPS), impiegato dalla polizia francese (cfr. A. Bauer - C. Soullez, *Fichiers de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion?*, Parigi, La Documentation française, 2007, pp. 15 sgg.).

26 Il riferimento è alle banche dati corrispondenti a quella del Casellario Centrale d'Identità, istituito presso il servizio polizia scientifica della direzione centrale anticrimine della polizia di Stato, che utilizza il sistema automatizzato AFIS e contiene i cartellini segnaletici di circa quattro milioni di persone (così, A. Spinela – G. Solla, *L'identificazione personale nell'investigazione scientifica: DNA e impronte*, in "Cassazione penale", 2009, p. 433; nonché, A. Intini – A.R. Casto – D.A. Scali, *op. cit.*, p. 138). Si pensi, ad esempio, al *National Fingerprint Database* (IDENT1), che consente alle forze di polizia di Inghilterra, Scozia e Galles, di confrontare più di sedici milioni di «sets of ten-prints» (cfr. <http://www.npia.police.uk/en/10504.htm>; nonché, *Database State*, cit., p. 23), oppure al sistema identificativo utilizzato dal *Bundeskriminalamt* tedesco, che conserva i dati relativi a più di tre milioni di persone (v. *The Bundeskriminalamt*, cit., p. 8), o, ancora, al *Fichier automatisé des empreintes digitales* (FAED), istituito nel 1987 e comune a polizia e *gendarmerie* (v. A. Bauer - C. Soullez, *op. cit.*, pp. 44 sgg.).

27 Al riguardo, si leggano, anche per ulteriori indicazioni bibliografiche, G. Capoccia, *Istituzione di una banca dati del DNA a fini identificativi e di giustizia*, in "Rassegna penitenziaria e criminologica", 2007, pp. 47 sg.; C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un "diritto comune" europeo*, in "Diritto penale e processo", 2007, pp. 386 sgg.; P. Felicioni, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milano, Ipsoa, 2007, pp. 193 sgg.; C. McCartney, *Forensic Identification and Criminal Justice. Forensic science, justice and risk*, Portland, Willan Publishing, 2006, pp. 159 sgg.; P.D. Martin – H. Schmitter – P.M. Schneider, *A brief history of the formation of DNA databases in forensic science within Europe*, in "Forensic Science International", 2001, pp. 225 sgg.; A. Moustiers, "Preuve et biotecnologies: l'utilisation des empreintes génétiques à des fins judiciaires", in *La preuve pénale. Internationalisation et nouvelles technologies*, a cura di O. de Frouville, Parigi, La Documentation française, 2007, pp. 177 sgg.; L. Picotti, *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali nel processo penale*, in "Il diritto dell'informazione e dell'informatica", 2003, pp. 722 sgg.; L. Scaffardi, *Le Banche dati genetiche per fini giudiziari e i diritti della persona*, <http://www.forumcostituzionale.it/site/images/stories/pdf/documenti__forum/paper/0114__scaffardi.pdf>; P.M. Schneider – P.D. Martin, *Criminal DNA databases: the European situation*, in "Forensic Science International", 2001, pp. 232 sgg.

terconnessione (dei casellari giudiziari) ovvero dell'accesso on-line indiretto o diretto (previsto dal trattato di Prüm e dalla decisione 2008/615/GAI con riguardo rispettivamente ai dati indicizzati contenuti negli schedari di analisi del DNA e ai sistemi automatizzati d'identificazione dattiloscopica). In secondo luogo, ha condotto al rafforzamento dell'obbligo di trasmissione dei dati contenuti in archivi nazionali secondo quanto previsto dalla decisione 2009/315/GAI, in materia di casellario giudiziario e dalla decisione quadro 2006/960/GAI per le banche dati gestite direttamente dalle autorità di *law enforcement* oppure per quelle alle quali siffatte autorità hanno accesso diretto[28].

I tre profili problematici che andranno affrontati coincidono con tre possibili limiti all'utilizzo delle banche dati europee quali fonti di prova. Il primo ha natura spaziale e dipende dalla circostanza che le banche dati europee contengono informazioni raccolte al di fuori del territorio nazionale. Il secondo limite ha natura funzionale ed è legato all'individuazione dei canali attraverso i quali i dati possono essere immessi nel procedimento penale, dal momento che si tratta spesso di informazioni raccolte nel corso di indagini amministrative. Il terzo limite si ricollega direttamente alla tutela del diritto alla protezione dei dati personali.

---

28 Riprendendo implicitamente la distinzione – operata da G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access*, Antwerp-Apeldoorn, Maklu, 2005, p. 15 – tra le informazioni alle quali le autorità di *law enforcement* hanno accesso autonomamente e quelle per le quali è necessaria un'autorizzazione dell'autorità giudiziaria, la decisione quadro 960 del 2006 attua il canone di disponibilità solo rispetto alle prime. Tra esse vengono annoverate però tre categorie di dati. Anzitutto, quelli detenuti direttamente da autorità incaricate dell'applicazione della legge (art. 2, lett. c). In secondo luogo, le informazioni «conservate in una banca dati alla quale un'autorità incaricata dell'applicazione della legge può accedere direttamente» (art. 4, par. 1): si pensi, solo per fare un esempio, agli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, che le imprese sono tenute a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'interno (ai sensi dell'art. 55, comma 7, d.lgs. 1 agosto 2003, n. 259) (per un panorama comparato delle informazioni alle quali le autorità di *law enforcement* hanno accesso, cfr. ancora G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *op. cit.*, p. 15). Infine, la decisione prende in considerazione anche «qualsiasi tipo di informazioni o dati detenuti da autorità pubbliche o da enti privati che siano accessibili alle autorità incaricate dell'applicazione della legge *senza il ricorso a mezzi coercitivi*»; in tal caso, si può trattare di qualsiasi informazione, anche non contenuta in una banca dati, che l'autorità di *law enforcement* può conseguire senza la necessità dell'autorizzazione dell'autorità giudiziaria. Per quel che riguarda i dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, dipenderà dai singoli ordinamenti: com'è noto, la direttiva 2006/24/CE ne prescrive la conservazione per un periodo non inferiore a sei mesi e non superiore a due anni dalla data della comunicazione (art. 6), ma rinvia agli ordinamenti nazionali la disciplina relativa all'accesso (cfr. il considerando n. 25), prevedendo soltanto che esso sia consentito solo alle «autorità nazionali competenti»: è possibile che, in alcuni ordinamenti, queste siano le stesse autorità di *law enforcement* e, in tal caso, si potrà ritenere attuato appieno anche per questi dati il canone di disponibilità (cfr. *supra*, M. Gialuz, "La cooperazione informativa quale motore del sistema europeo di sicurezza", § 5).

Prendendo le mosse dal primo aspetto, si tratta di capire se e in che misura le banche dati europee e gli strumenti giuridici che prevedono lo scambio di informazioni tra di esse possono garantire la libera circolazione dei dati anche nell'ottica del procedimento penale. È evidente che tutti i modelli di collegamento delle banche dati nazionali e, a maggior ragione, le banche dell'Unione garantiscono una rapida circolazione delle informazioni sul *piano operativo*: il punto è verificare se queste informazioni sono utilizzabili anche in un contesto ad alto tasso di formalizzazione, qual è il procedimento penale.

A tal fine, può essere ragionevole partire proprio dal canone di disponibilità, il quale ha come ambito naturale la cooperazione di polizia – tanto che il Programma dell'Aia lo enuncia esplicitamente nella parte dedicata al rafforzamento della sicurezza (§ 2)[29] –, ma finisce per estendersi anche al procedimento penale. Lo stesso documento ribadisce l'auspicio per una migliore circolazione dei dati anche nella parte relativa al rafforzamento della giustizia con riguardo alle informazioni desumibili dai casellari giudiziali nazionali (§ 3.3.1). Ma la diffusività del principio è stata soprattutto riaffermata, non a caso, con riferimento alla cooperazione in materia di terrorismo, dal considerando n. 4 della decisione 2005/671/GAI, concernente lo scambio di informazioni relative alla lotta contro tale forma di criminalità: vi si afferma, infatti, che «il campo d'applicazione degli scambi di informazioni deve essere esteso a tutte le fasi dei procedimenti penali, comprese le condanne e a tutte le persone, gruppi o entità oggetto di un'indagine, di un'azione penale o di una condanna per reati di terrorismo»[30].

Ciò premesso, ci si deve evidentemente soffermare sui principali strumenti normativi che hanno dato attuazione al canone di disponibilità. Il primo è costituito dalla decisione quadro n. 960 del 2006[31].

Se sotto il profilo dell'ambito soggettivo, non vi è dubbio che la decisione si riferisca alle sole autorità di polizia (con esclusione dell'autorità giudiziaria), con riguardo all'ambito oggettivo di operatività, è altrettanto sicuro che essa si applica anche all'attività di polizia giudiziaria successiva all'acquisizione di una *notitia criminis*[32]. Ciò emerge chiaramente dal fatto che la decisione quadro attiene sia allo scambio di informazioni relative alle operazioni di *intelligence* criminale, sia a quelle relative all'indagine penale (art. 1, par. 1). La prima (ossia la *criminal intelligence operation*) viene definita come «una fase procedurale nella quale, in una fase precedente all'indagine penale, un'autorità competente incaricata dell'applicazione della legge, ai sensi della legislazione nazionale, ha facoltà di raccogliere,

---

29 Cfr. *Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea*, in *GUUE*, C 53, 3 marzo 2005, p. 7.

30 In *GUUE*, L 253, 29 settembre 2005, p. 22.

31 In *GUUE*, L 386, 29 dicembre 2006, p. 89.

32 Cfr. *supra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea", § 9.

elaborare e analizzare informazioni su reati o attività criminali al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti» (art. 2, lett. *c*); l'indagine penale (ossia la *criminal investigation*) viene invece indicata come «una fase procedurale nella quale le autorità incaricate dell'applicazione della legge o le autorità giudiziarie competenti, compresi i pubblici ministeri, adottano misure per individuare e accertare i fatti, le persone sospette, e le circostanze in ordine a uno o più atti criminali accertati» (art. 2 lett. *b*).

Pertanto, se nel corso di un'indagine penale, in uno Stato membro è necessario ottenere un'informazione detenuta da un'autorità di polizia di un altro Stato in una propria banca dati oppure in una banca dati – pubblica (ad es. registro anagrafico) o privata (ad es. gestore di telefonia) – alla quale la polizia ha accesso diretto, la polizia che indaga può chiedere la trasmissione del dato e lo Stato estero dovrà trasmettere l'informazione – salvi casi tassativi di rifiuto – entro i termini brevi indicati dall'art. 4. Si badi, tale trasmissione avverrà al di fuori delle vie della cooperazione giudiziaria: potranno essere utilizzati i canali – assai agili – della cooperazione di polizia (art. 6).

La decisione fornisce un'ulteriore indicazione sul proprio ambito di applicazione: l'art. 1, par. 4, precisa, infatti, che essa non impone alcun obbligo per gli Stati membri di fornire informazioni e *intelligence* da utilizzare «come prove dinanzi ad un'autorità giudiziaria» («as evidence before a judicial authority»), né conferisce il diritto a utilizzarle a tal fine. Laddove lo Stato ricevente voglia impiegare le informazioni a tale scopo, deve ottenere il consenso dello Stato che le ha fornite, se è necessario, in virtù della legislazione nazionale di quest'ultimo e facendo ricorso agli strumenti di cooperazione giudiziaria vigenti tra gli Stati membri.

L'ambito di operatività dei meccanismi semplificati di trasmissione dei dati risulta pertanto delimitato – ai nostri fini – da un confine di ordine (per così dire) spaziale e da uno di natura funzionale: il primo deriva dal riferimento all'indagine penale, mentre il secondo si desume dall'esclusione della possibilità di utilizzare le informazioni come prove dinnanzi a un'autorità giudiziaria. Spetterà, dunque, al legislatore nazionale, in sede di attuazione della decisione quadro, adeguare tali limiti di ordine generale al contesto processuale italiano.

Con riguardo al concetto di "indagine penale", sembra che esso possa coincidere con quello di indagine preliminare: si tratta, infatti, dello spazio procedimentale che precede l'elevazione di un'accusa. Sarà quindi esclusa la possibilità di utilizzare i dati ottenuti in forza della decisione n. 960 nella fase strettamente processuale. Qualche problema in più potrebbe sorgere, invece, per l'altro limite. Nel nostro ordinamento, si potrebbe essere indotti a pensare che il secondo vincolo si limiti a specificare il primo. In quest'ottica, il divieto di utilizzo delle informazioni davanti all'autorità giudiziaria a fini probatori potrebbe essere concepito come divieto di impiegare i dati nel processo: nel corso delle indagini, invece, i dati trasmessi in attuazione del canone di disponibilità potrebbero essere sempre utilizzati. In tal senso, peraltro, potrebbe deporre l'orientamento giu-

risprudenziale che si è sviluppato in ordine all'istituto dello scambio spontaneo di informazioni previsto dall'art. 10 della Convenzione del Consiglio d'Europa sul riciclaggio (del 1990), dall'art. 46 della CAAS e ora anche dall'art. 7 della Convenzione dell'Unione europea sull'assistenza giudiziaria[33]: si è, infatti, stabilito che la documentazione acquisita per i canali di polizia è equivalente a quella acquisita mediante rogatoria[34] oppure che è estranea alla disciplina delle rogatorie[35] e se n'è ammesso l'utilizzo in indagini preliminari, in udienza preliminare e ai fini dell'adozione di misure cautelari, fermo in ogni caso il limite del rispetto dei diritti fondamentali garantiti dall'ordinamento giuridico nazionale[36].

Ebbene, una lettura che conduca a sovrapporre il limite funzionale a quello spaziale non può essere accolta. Non pare potersi escludere che un "utilizzo come prova dinanzi a un'autorità giudiziaria" si può avere anche nel corso delle indagini preliminari. Naturalmente, viene in mente l'impiego di un elemento di prova ai fini dell'adozione di una misura cautelare: in tal caso, invero, vi è un giudizio sulla probabile responsabilità. Al contrario, non sembra potersi parlare di "utilizzo come prova dinanzi a un'autorità giudiziaria" nel caso di provvedimento che autorizza un mezzo di ricerca della prova invasivo: in tale ipotesi, non vi è un accertamento – sia pure provvisorio – sulla responsabilità di un soggetto, ma tutt'al più (nel solo caso delle intercettazioni di comunicazioni) un vaglio relativo alla sussistenza di un fatto di reato. Insomma, la motivazione del provvedimento autorizzatorio è incentrata piuttosto sull'utilità dell'atto invasivo nell'individuazione di elementi conoscitivi che sulla ricostruzione del passato. In sede di attuazione della decisione occorrerà, allora, chiarire che i dati trasmessi in forma semplificata potranno essere utilizzati dalla polizia o dal pubblico ministero, sia per fini strettamente investigativi, sia per giustificare l'adozione di atti volti a

---

33 Al riguardo, cfr. E. Calvanese, *Cooperazione giudiziaria tra Stati e trasmissione spontanea di informazioni: condizioni e limiti di utilizzabilità*, in "Cassazione penale", 2003, pp. 458 sgg.; A. Ciampi, *L'assunzione di prove all'estero in materia penale*, Padova, Cedam, 2003, pp. 357 sgg.; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale. Verso un sistema integrato di forme e strumenti di collaborazione tra le autorità giudiziarie*, Milano, Giuffrè, 2007, pp. 329 sgg.; M.R. Marchetti, *L'assistenza giudiziaria internazionale*, Milano, Giuffrè, 2005, pp. 245 sgg.

34 Così, Cass., sez. I, 31 ottobre 2002, Moio, in "Archivio della nuova procedura penale", 2003, p. 132.

35 In tal senso, Cass., sez. III, 6 novembre 2002, Pils, in "Archivio della nuova procedura penale", 2003, p. 508, la quale si riferiva però a documentazione acquisita prima dell'accertamento della *notitia criminis*, ossia in una fase in cui non trovano ancora spazio le garanzie previste dagli artt. 727 ss.

36 Questo questo senso, Cass., sez. II, 8 marzo 2002, Pozzi, in "Cassazione penale", 2003, p. 449; Cass., sez. I, 1° dicembre 2000, Rondinella e altro, in "Centro elaborazione dati della Cassazione", n. 218214; Cass., Sez. I, 9 maggio 2000, Franzoni, *ivi*, n. 216737; Cass., sez. I, 10 luglio 1997, Ibba, in "Archivio della nuova procedura penale", 1997, p. 432; Cass., sez. I, 25 giugno 1991, Ferrante, in "Cassazione penale", 1991, II, p. 260. A tale riguardo, cfr. R. Vanni, *Spunti sul crimine transnazionale: utilizzabilità nel corso delle indagini preliminari di rogatorie passive, spazio investigativo e spazio cautelare, moderna cooperazione internazionale*, in "Il foro ambrosiano", 2003, pp. 88 sgg.

ricercare altri elementi conoscitivi necessari ad accertare il fatto criminoso: non potranno, invece, essere impiegati dal giudice per la decisione cautelare.

Il secondo strumento che ha dato attuazione al canone di disponibilità è senza dubbio la decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera[37]. Essa ha recepito il Trattato di Prüm nell'ordinamento comunitario e ha fissato, almeno per quanto concerne la circolazione delle informazioni personali relative ai profili DNA e ai dati dattiloscopici, un limite ancora più stringente. Infatti, è previsto – ai fini di indagine penale – un accesso diretto ai dati di indice; ma per la trasmissione dei dati personali che si riferiscono ai dati di indice rispetto ai quali è emersa una concordanza, gli artt. 5 e 10 della decisione stabiliscono un rinvio al diritto nazionale dello Stato richiesto. Il che significa che, di regola, essa dovrà seguire le procedure dell'assistenza giudiziaria: nondimeno, a rendere più agevole la trasmissione delle informazioni potrebbero intervenire proprio le norme della decisione n. 960 del 2006 e delle leggi nazionali che vi daranno attuazione[38], nonché quelle della decisione quadro sul mandato europeo di ricerca della prova. Diverso, invece, il discorso in ordine ai dati di immatricolazione dei veicoli, per i quali è previsto un accesso effettivamente diretto (art. 12 decisione n. 615 del 2008): pertanto, sembra potersi concludere che l'autorità dello Stato membro la quale effettua la consultazione e ottiene l'informazione relativa ai proprietari o agli utenti di un veicolo o al veicolo stesso potrà utilizzarlo nel procedimento penale senza che sia necessario un passaggio attraverso i meccanismi dell'assistenza giudiziaria.

L'ultimo filone da prendere in considerazione è quello relativo all'attuazione del canone di disponibilità nell'ambito delle informazioni relative a precedenti condanne dell'imputato[39]. Al riguardo, la decisione n. 876 del 2005 si limita a intervenire sullo strumento tradizionale di cooperazione previsto dagli artt. 13 e 22 della Convenzione di assistenza giudiziaria del 1959, prevedendo l'obbligo, per lo Stato richiesto, di trasmettere la risposta con il modulo standardizzato, immediatamente e comunque in un termine non superiore a dieci giorni (art. 3). Diverso, invece, l'impianto sotteso al sistema costituito dalla decisione quadro sull'organizzazione e il contenuto degli scambi sulle informazioni estratte dal casellario giudiziario (2009/315/GAI) e dalla decisione che istituisce il sistema europeo di informazione sui casellari giudiziari (2009/316/GAI). Sulla base di tale pacchetto normativo, le informazioni relative alla storia penale dell'imputato ottenute attraverso il sistema informatizzato potranno essere utilizzate nel corso del

37 In *GUUE*, L 210, 6 agosto 2008, p. 1. V. *supra*, A. Marandola, "*Information sharing* nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione".

38 Cfr. *supra*, S. Ciampi, *op. cit.*, § 10.

39 V. *supra*, M. Gialuz, "Il casellario giudiziario europeo: una frontiera dell'integrazione in materia penale".

procedimento penale (art. 9 della decisione n. 315), inteso in senso ampio come comprendente «la fase precedente al processo penale, la fase del processo penale stesso e l'esecuzione della condanna» (art. 1, lett. *b*, della decisione n. 315).

Per la verità, gli ostacoli all'impiego delle informazioni in parola nel procedimento penale italiano – ai fini dell'applicazione dei diversi istituti basati sulla "memoria"[40] – sembrano venire dalla disciplina interna. Dalla lettura congiunta dell'art. 730 c.p.p. e dell'art. 3 comma 1 lett. a del Testo unico in materia di casellario giudiziale (d.P.R. 14 novembre 2002, n. 313), si evince come le sentenze straniere acquisiscano rilevanza – anche soltanto come meri fatti storico giuridici – solo con il riconoscimento[41]. Si badi, però, che il legislatore italiano sarà chiamato a superare siffatta scelta: dovrà, infatti, dare attuazione alla decisione quadro sulla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale (2008/675/GAI)[42], la quale prescrive proprio di equiparare la sentenza emessa in altro Stato dell'Unione a quella interna (art. 3, par. 1). Probabilmente, tale risultato può essere conseguito già a livello interpretativo – in applicazione del canone dell'interpretazione conforme alla decisione quadro[43] – valorizzando la norma dell'art. 696 c.p.p.

In conclusione, pertanto, si può affermare che il quadro che emerge dagli strumenti normativi che danno attuazione al canone di disponibilità è piuttosto composito. Vi è un primo livello che riguarda le informazioni più sensibili – quali quelle relative ai profili DNA o alle impronte digitali –, per le quali si prevede che debbano essere utilizzati i canali tradizionali dell'assistenza giudiziaria. Vi è poi un livello intermedio, relativo ai dati trattati da autorità di *law enforcement* (ossia di fonte poliziesca), con riguardo ai quali si consente una trasmissione diretta e deformalizzata ai soli fini investigativi. Infine, vi è un terzo livello, che concerne i dati giudiziari attinenti ai precedenti penali e ai dati meno sensibili (quali quelli relativi agli autoveicoli), nel quale si assiste effettivamente al superamento dell'ostacolo territoriale. Sicché, le informazioni contenute in una base dati nazionale possono essere trasmesse all'autorità di *law enforcement* o all'auto-

---

40 Cfr., per una puntuale ricognizione, D. Negri, "La circolazione del '*curriculum* criminale' tra i procedimenti penali", in *Contrasto al terrorismo interno e internazionale*, a cura di R. Kostoris e R. Orlandi, Torino, Giappichelli, 2006, p. 319.

41 Cfr. *supra*, M. Gialuz, "Il casellario giudiziario europeo", cit., § 4, nota 63.

42 In *GUUE*, L 220, 15 agosto 2008, p. 32.

43 Cfr., per tutti, A. Ciampi, "L'ordinamento italiano e le decisioni quadro quale strumento di cooperazione di polizia e giudiziaria", in *Equo processo: normativa italiana ed europea a confronto*, a cura di L. Filippi, Padova, Cedam, 2006, pp. 89 sgg.; *L'interpretazione conforme al diritto comunitario in materia penale*, a cura di F. Sgubbi e V. Manes, Bologna, Bononia University Press, 2007, pp. 53 sgg.; M. Marchegiani, *L'obbligo di interpretazione conforme alle decisioni quadro: considerazioni in margine alla sentenza Pupino*, in "Diritto dell'Unione Europea", 2006, p. 563; A. Weyembergh, "L'effectivité du troisième pilier de l'Union Européenne et l'exigence de l'interprétation conforme: la Cour de Justice pose ses jalons (note sur l'arrêt Pupino, du 16 juin 2005, de la Cour de Justice des Communautés européennes)", in *Per un rilancio del progetto europeo*, cit., pp. 353 sgg.

rità giudiziaria di altro Stato membro e utilizzate nell'ambito del procedimento penale (inteso in senso lato).

4. (Segue): il limite funzionale

Nell'ottica del legislatore europeo, si dovrebbero distinguere tre categorie di elementi conoscitivi, che assumono rilievo nell'attività di prevenzione e repressione dei reati: l'"*intelligence*", l'"*information*" e l'"*evidence*". Delle prime due si è detto: esse vengono definite dall'art. 2, lett. d, della decisione n. 960 del 2006 come «qualsiasi tipo di informazioni o dati detenuti da autorità incaricate dell'applicazione della legge» oppure «da autorità pubbliche o da enti privati che siano accessibili alle autorità incaricate dell'applicazione della legge senza il ricorso a mezzi coercitivi». La differenza tra esse risiede nella circostanza che l'*intelligence* non è connessa a una specifica indagine penale, mentre di *information* si parla con riferimento a elementi conoscitivi che si ricollegano a un'indagine volta alla ricostruzione di un fatto di reato[44]. La definizione di *evidence* si desume invece dalla decisione quadro sul mandato europeo di ricerca della prova: si tratta degli «oggetti, documenti e dati» da utilizzare nei procedimenti penali avviati da un'autorità giudiziaria (artt. 1, parr. 1 e 5).

Ebbene, mentre con riguardo alla categoria delle *pre-evidence*[45] – che ricomprende *intelligence* e *information*, che si collocano in uno stadio preliminare a quello relativo all'esercizio dell'azione penale – lo scambio è governato sempre e comunque dal principio di disponibilità, con riferimento all'*evidence* il quadro è più variegato: se in passato si doveva ricorrere agli strumenti di assistenza giudiziaria tradizionali[46], dopo l'adozione della decisione 2008/978/GAI e la sua attuazione, si potrà impiegare lo strumento riconducibile al canone del reciproco

---

44 Cfr. E. De Busser, *The architecture of data exchange*, in "International Review of Penal Law", 2007, p. 37, la quale precisa come l'*intelligence* sia qualificata talora «as 'soft' data – as opposed to 'hard' data – which stands for information, indicating the fact whether data can be endorsed by documents (f.e. sentences, witness statements, etc.) and is therefore reliable or not». Cfr. anche *supra*, § 3. Va notato che la nozione di *intelligence*, che emerge a livello europeo appare assai più ampia rispetto a quella fatta propria dalla dottrina italiana: al riguardo, cfr. *supra*, S. Ciampi, *op. cit.*, § 7.

45 La locuzione "pre-evidence phase" è utilizzata da G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *op. cit.*, p. 26.

46 In tal senso, G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *op. cit.*, p. 27, che escludono che l'attuazione del canone di disponibilità possa riguardare la cooperazione giudiziaria; nonché, E. De Busser, *op. cit.*, p. 38, la quale sottolinea la necessità che gli ambiti rimangano distinti utilizzando un'immagine efficace: «the notions of pre-evidence and evidence can be described as two storeys in the house of EU exchange of data. The ground floor represents all information and intelligence that will be able to be exchanged according to the principle of availability»; «the top floor represents all evidence to be exchanged in accordance with bi- and multilateral mutual legal assistance instruments».

riconoscimento, ossia il mandato europeo di ricerca della prova. Un problema potrebbe sorgere per il fatto che il MER ha un ambito di applicazione ristretto, in quanto non si applica ad esempio ai dati sulle comunicazioni conservati dai fornitori di servizi di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di comunicazione (art. 4, par. 2, lett. *e*).

Ad ogni modo, quale che sia il canale attraverso il quale l'elemento conoscitivo proveniente da archivi europei è trasmesso all'autorità (di polizia o giudiziaria) italiana, viene in rilievo un secondo possibile limite al suo utilizzo nel procedimento penale. Anche per i dati in relazione ai quali può essere superato l'ostacolo territoriale si pone, infatti, un problema di ordine funzionale: il procedimento penale dovrebbe essere impermeabile ai risultati dell'attività di *intelligence* o di indagine amministrativa. Tale sbarramento è tradizionalmente volto a garantire il rispetto del canone di separazione dei poteri dello Stato e a salvaguardare i diritti della persona sottoposta al procedimento penale.

Ebbene, non è un mistero che i confini tra attività di *intelligence* e di indagine penale si vanno facendo sempre più blandi e che si registra un tendenziale aumento dell'osmosi tra l'ambito della prevenzione e quello della repressione. Già negli anni novanta, la dottrina italiana lo aveva ben messo in luce, soprattutto con riferimento ai procedimenti relativi alla criminalità organizzata: si era parlato di inchieste preparatorie, prodromiche alle vere e proprie indagini penali[47]. Successivamente, il fenomeno dell'allentamento della separazione tra attività di *intelligence* e attività di polizia si è consolidato soprattutto con riguardo ai reati terroristici e nel contesto del *security paradigm*[48].

A favorire l'interconnessione tra i due momenti è stata anche la diffusione dell'*intelligence led policing*[49], ossia di quel paradigma investigativo che si fonda sull'impiego di tutte le informazioni disponibili, sulle tecniche di analisi criminale (come ad esempio il *profiling*), e, in definitiva, proprio sulla stretta cooperazione tra autorità di *law enforcement* e servizi di *intelligence*. Tale modello è stato recepito

---

47 Il riferimento è a R. Orlandi, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis*?*, in "Rivista italiana di diritto e procedura penale", 1996, pp. 283 sgg.

48 Cfr., in particolare, D. Derenčinović - A.M. Getoš, *Cooperation of law enforcement and intelligence agencies in prevention and suppression of terrorism – european perspective*, in "International Review of Penal Law", 2007, pp. 82 sg.; G. Marullo, "Il ruolo e le attività di intelligence e delle forze di polizia nella lotta alla criminalità organizzata ed al terrorismo nei paesi dell'Unione europea, nel rispetto della Convenzione del Consiglio d'Europa per la protezione dei dati personali e la Convenzione europea sui diritti dell'uomo", in *La cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo*, a cura di M. Cherif Bassiouni, Milano, Giuffrè, 2005, p. 187; J.A.E. Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?", in *L'area di libertà sicurezza e giustizia*, cit., pp. 485-486.

49 Sul quale, cfr., per tutti, J. Ratcliffe, *Intelligence-Led Policing*, Cullompton, Willan Publishing, 2008, p. 6.

nel Programma dell'Aia – ove si parla di *intelligence-led law enforcement* o, nella versione italiana, di «metodologia di contrasto basata sull'intelligence» (§ 2.3) – e ad esso è in qualche misura riferibile la stessa configurazione dell'Europol.

Non sfuggirà che in tale modello, che si è sviluppato soprattutto con riguardo alla lotta al terrorismo e ai reati di criminalità organizzata[50], assumono un ruolo essenziale proprio le banche dati di polizia e, in certa misura, il collegamento tra le queste e quelle dei servizi segreti[51]: basti pensare al sistema di informazione e, soprattutto, agli archivi di analisi dell'Europol, che sono costituiti per la raccolta, il trattamento o l'utilizzazione di dati con «lo scopo di venire in aiuto all'indagine criminale» (art. 10, par. 2, Convenzione Europol). Ora, le informazioni contenute nel sistema informativo vanno comunicate dall'Europol alle unità nazionali interessate (art. 13 Convenzione Europol) e potranno essere utilizzate dai servizi competenti degli Stati membri «per prevenire e combattere la criminalità che rientra nella competenza dell'Europol e le altre forme gravi di criminalità» (art. 17 Convenzione Europol)[52]. Pertanto, tali informazioni potrebbero anche avere ingresso nel procedimento penale, magari indirettamente, ossia attraverso le relazioni di servizio, che possono avere un impiego probatorio nel corso delle indagini preliminari o nei riti premiali[53].

Parallelamente a quella tra attività di *intelligence* e attività di indagine penale, si è andata affievolendo la linea di separazione tra ispezione amministrativa e indagine penale: ciò riguarda i poteri di accertamento della Commissione[54], ma soprattutto le indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF). Com'è noto, il regolamento (CE) n. 1073/1999[55] riconosce all'OLAF il potere di svolgere indagini – espressamente qualificate "amministrative" dall'art. 2 – esterne o interne (artt. 3 e 4), ossia rispettivamente rivolte nei confronti di soggetti

---

50 Cfr., con riguardo all'esperienza inglese, Ö. Ülgen, *The UK's new serious organized crime agency (SOCA): combining intelligence and law enforcement*, in "International Review of Penal Law", 2007, p. 153.

51 V., in termini critici, P. De Hert - S. Gutwirth, *Interoperability of police databases within the EU: an accountable political choice?*, <http://papers.ssrn.com/sol3/papers.cfm?abstract__id=971855>, p. 9.

52 A tali disposizioni corrispondono gli artt. 17 e 19 della Decisione del Consiglio che istituisce l'Ufficio europeo di polizia: cfr. *Documento del Consiglio n. 8706/3/08*, 9 ottobre 2008, <http://register.consilium.europa.eu/pdf/it/08/st08/st08706-re03.it08.pdf>.

53 Cfr., con riguardo all'attività di *intelligence*, M.L. Di Bitonto, "Raccolta di informazioni e attività di *intelligence*", in *Contrasto al terrorismo interno e internazionale*, cit., p. 261. Sull'«ingresso privilegiato che avranno nei procedimenti penali le informazioni fornite da Europol», v. F.M. De Martino, "Europol: flusso transnazionale dei dati personali e loro utilizzazione nel processo penale italiano fra immunità degli agenti e cultura del sospetto», in *Nuove strategie per la lotta al crimine organizzato transnazionale*, a cura di V. Patalano, Torino, Giappichelli, 2003, p. 146.

54 In tal senso, J.A.E. Vervaele, *L'europeizzazione del diritto penale e la dimensione penale dell'integrazione europea*, trad. it. di R. D'Antoni, in "Rivista trimestrale di diritto penale dell'economia", 2005, pp. 137 sg.

55 In *GUCE*, L 136, 31 maggio 1999, p. 1.

non appartenenti alle istituzioni comunitarie o a soggetti che ne fanno parte. Entrambe si concludono con relazioni sui fatti accertati, che, ai sensi dell'art. 9, par. 2, del regolamento (CE) n. 1073/1999, «costituiscono elementi di prova nei procedimenti amministrativi o giudiziari dello Stato membro nel quale risulti necessario avvalersene al medesimo titolo e alle medesime condizioni delle relazioni amministrative redatte dagli ispettori amministrativi nazionali». È stato rilevato come tale norma – che ricalca quella dell'art. 8, par. 3, del regolamento EURATOM n. 2185/1996[56] – stabilisca «il generale principio di non separatezza, ed anzi di circolazione, degli elementi di prova dall'ambito amministrativo comunitario al circuito giudiziario nazionale»[57].

Per quel che riguarda specificamente l'ordinamento italiano, in dottrina si tende ad ammettere l'utilizzo delle relazioni nell'ambito delle indagini preliminari, ma la giurisprudenza è andata ben più in là, ritenendo che gli atti compiuti dall'Uclaf (ossia il diretto predecessore dell'OLAF) possano essere utilizzati anche in dibattimento: trattandosi di «atti promananti da un organo pubblico di controllo», essi possiederebbero «tutti i requisiti prescritti dall'art. 234 c.p.p. per l'inserimento nel fascicolo per il dibattimento»[58].

Come si intenderà, anche per i dati contenuti nei sistemi informativi potrebbe essere impiegata la categoria dei documenti: in effetti, una volta riprodotto il contenuto dichiarativo o rappresentativo su un supporto tradizionale, essi potrebbero essere ricondotti all'ampia nozione dell'art. 234 c.p.p.; oppure, anche a prescindere dalla riproduzione, potrebbero essere sussunti nella definizione di documento informatico, inteso come «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»[59].

---

56 In *GUCE*, L 292, 15 novembre 1996, p. 2.

57 Così, A. Perduca – F. Prato, *Le indagini dell'ufficio europeo per la lotta antifrode (Olaf) ed i rapporti con le autorità giudiziarie*, in "Cassazione penale", 2006, p. 4248. Sul rapporto tra indagine dell'OLAF e procedimento successivo, cfr. O. Broutin, "L'Office de lute antifraud", in *La preuve pénale*, cit., p. 41; S. de Moor, "Transnational investigations and the judicial follow-up to the OLAF inspection reports under the existing cooperation instruments", in *European Evidence Warrant*, cit., pp. 49 sgg.; D. Merckx, "The judicial follow-up of OLAF cases – A national perspective", *ibidem*, pp. 53 sgg.

58 In tal senso, Trib. Marsala, 17 dicembre 1998, XY, in "Cassazione penale", 1999, p. 2687. In termini favorevoli, V. Pacileo, *I rapporti dell'Olaf con le autorità giudiziarie nazionali: forme e modalità di assistenza*, <www.csm.it>, p. 8. In termini critici, invece, A. Perduca-F. Prato, *op. cit.*, p. 4250, secondo il quale in tale pronuncia si è andati oltre a quanto previsto dalla giurisprudenza di legittimità con riferimento ai verbali di constatazione della polizia giudiziaria e dei servizi ispettivi amministrativi nazionali; nonché, C. Bovio, *Le indagini interne ed esterne dell'Olaf: garanzie difensive ed effetti processuali*, <http://appinter.csm.it/internat/relaz/oL13698.pdf>, p. 4, che distingue tra atti effettivamente amministrativi dell'OLAF e atti compiuti durante la vera e propria indagine, i quali, avendo come presupposto gli indizi di illecito, dovrebbero essere svolti con il rispetto delle garanzie previste dal codice di rito penale.

59 Si tratta, come noto, della definizione posta dall'art. 1, lett. *p*), d.lgs. 7 marzo 2005, n. 82, che riprende quella dell'art. 1, lett. *a*, d.P.R. 10 novembre 1997, n. 513: a seguito della soppressione

La questione centrale, allora, è capire se, una volta superato l'ostacolo territoriale – mediante il ricorso alla rogatoria o al mandato europeo di ricerca della prova – essi possano per ciò solo essere acquisiti – laddove possibile – mediante l'inserimento nel fascicolo per il dibattimento ai sensi dell'art. 431 lett. *d* c.p.p. oppure direttamente acquisiti in dibattimento come tali.

Evidentemente, il problema deriva dal fatto che le banche dati considerate sono istituite proprio per finalità di sicurezza e di giustizia: sicché, esse forniranno documenti o informazioni che hanno un qualche legame, più o meno stretto, con l'accertamento penale. E, allora, il rischio è quello di utilizzare tale canale per far refluire in giudizio prove "documentali" che sono formate al di fuori del procedimento penale e da soggetti estranei al procedimento penale italiano, ma che sono *ab origine* destinate a tale contesto.

Occorre peraltro prendere atto che non si può fornire una risposta generalizzata, con riferimento a ciascuna banca dati: se vi sono banche dati tendenzialmente giudiziarie (come quella di Eurojust) oppure di *intelligence* (come quella di Europol) o di polizia (come la banca dati interforze, istituita presso il Ministero dell'Interno) vi sono archivi misti (come il SIS). Si dovrà, dunque, di volta in volta avere riguardo alla singola *res* individuata attraverso la banca dati e acquisita, per qualificarla a seconda dei casi come atto compiuto in un procedimento penale straniero, oppure come atto posto in essere nel corso di attività di *intelligence* criminale preventiva o di un'indagine di polizia amministrativa. Il primo potrà essere acquisito a norma dell'art. 238 c.p.p. e, se si tratti di atto non ripetibile della polizia giudiziaria, potrà essere inserito nel fascicolo per il dibattimento solo se le parti vi consentono oppure dopo l'esame testimoniale dell'autore, compiuto anche mediante rogatoria (art. 78 disp. att. c.p.p.)[60]. Laddove si tratti di dati provenienti da inchieste di *intelligence* o da attività di polizia amministrativa, potranno essere acquisiti come documenti solo se costituiscono veicolo di conoscenze non altrimenti acquisibili al processo per l'impossibilità di assumere oralmente in dibattimento l'atto probatorio[61].

Certo, vista la tendenza permissiva della giurisprudenza, non sarà facile garantire il rispetto del limite funzionale nella prassi: è accaduto, per esempio, che

---

– da parte dell'art. 3 l. 18 marzo 2008, n. 48 – della seconda parte dell'art. 491-*bis* c.p., occorre infatti riferirsi alla nozione generale del codice dell'amministrazione digitale (cfr. G. Amato, *Incerta l'efficacia probatoria del documento*, in "Guida al diritto", 2008, n. 16, p. 55; L. Picotti, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in "Diritto penale e processo", 2008, p. 703; M. Scoletta, "Il nuovo regime penale delle falsità informatiche", in *Sistema penale e criminalità informatica*, a cura di L. Lupária, Milano, Giuffrè, 2009, pp. 8 sgg.).

60 Al riguardo, si legga C. Valentini, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Padova, Cedam, 1998, pp. 212 sg.

61 In tal senso, con riguardo al documento amministrativo atipico, R. Orlandi, *Atti e informazioni della autorità amministrativa nel processo penale*, Milano, Giuffrè, 1992, p. 146.

la qualifica come documenti di atti compiuti dall'ufficio SIRENE abbia consentito di aggirare, tanto il limite funzionale, quanto quello territoriale [62]; in palese violazione del canone di legalità della prova.

5. (Segue): il limite derivante dalla tutela del diritto alla protezione dei dati

Accanto al limite territoriale e a quello funzionale, si pone per i dati contenuti negli archivi informatici – sia quelli europei, che quelli nazionali – un ulteriore vincolo di utilizzazione, derivante dall'esigenza di tutelare quel diritto alla protezione del dato di carattere personale, che trova espresso e autonomo riconoscimento nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea[63].

L'analisi di questo terzo limite non può che prendere le mosse dalla constatazione di una differenza fondamentale nelle banche dati. Esse possono operare come depositi statici di informazioni preesistenti, nei quali la tecnologia informatica consente soltanto di identificare il dato utile, oppure, come contenitori "dinamici" di produzione di informazioni, nei quali la tecnologia informatica consente – si pensi ai sistemi informativi di Eurojust, agli archivi di analisi di Europol, oppure al sistema di indagine del CED interforze[64] – di *elaborare* i dati mettendoli in relazione e dando quindi loro un senso, che non avevano se presi singolarmente. Occorre, allora, distinguere: l'elemento cognitivo fornito al procedimento dalla banca dati può essere – come accade per altre prove: prima tra tutte, la testimonianza – originario oppure derivato. Sarà originario nel caso della banca dati tecnico-scientifica (l'impronta digitale; il profilo genetico; il dato

---

62 Ci si riferisce, in particolare, a una vicenda processuale per molti versi paradigmatica verificatasi davanti al Tribunale di Trieste. Era accaduto che la polizia di frontiera – del valico con la Slovenia – avesse accertato l'esistenza di una segnalazione nel SIS di un veicolo; richiesta la trasmissione di ulteriori informazioni tramite SIRENE tedesco, era risultato che il veicolo era stato oggetto di un'appropriazione indebita. Si è così aperto un procedimento penale per ricettazione e il pubblico ministero ha chiesto – e il tribunale ha concesso – l'acquisizione nel fascicolo per il dibattimento dei formulari SIRENE (A ed M) che contenevano i dati del veicolo e soprattutto il tipo di reato contestato, il luogo e la data dell'appropriazione indebita, l'autorità giudiziaria procedente e altri dati accessori. In tal modo, invece di acquisire con rogatoria gli atti del procedimento penale tedesco, si è qualificato come documento un qualcosa che difficilmente poteva avere tale caratteristica, perché o si trattava di attività di cooperazione di polizia giudiziaria oppure di attività di indagine preventiva.

63 Sull'importanza di tenere distinte la privacy, che costituisce un «tool of opacity» e il *right to data protection*, che configura un «tool of transparency», cfr. P. De Hert – S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in *Privacy and the Criminal Law*, a cura di E. Claes, A. Duff e S. Gutwirth, Anversa-Oxford, Intersentia, 2006, pp. 62 sgg., 103.

64 V. A. Intini – A.R. Casto – D.A. Scali, *op. cit.*, p. 95; A. Manganelli - F. Gabrielli, *Investigare. Manuale pratico delle tecniche di indagine*, Padova, Cedam, 2007, p. 20.

attinente alla comunicazione elettronica)[65]; sarà invece indiretto o derivato, tanto laddove esso derivi dalla rielaborazione dei dati singoli, quanto nel caso in cui coincida con una rappresentazione di un elemento cognitivo esterno inserito nell'archivio non nella sua integralità ma – come normalmente accade – attraverso riferimenti riassuntivi.

Rispetto alla prima tipologia di dati, la tutela del diritto alla protezione si realizza soprattutto attraverso il rispetto dei principi fondamentali del trattamento, primo tra tutti il *principio di finalità limitata*: l'elemento di prova dovrebbe poter essere utilizzato – in tutte le fasi processuali – soltanto ove raccolto anche per finalità di repressione dei reati.

Il problema si pone in relazione a quella tendenza, più volte registrata dal Garante europeo per la protezione dei dati, ad accordare alle autorità incaricate dell'applicazione della legge l'accesso a vari sistemi d'informazione e d'identificazione su vasta scala e l'utilizzazione ai fini di *law enforcement* di dati archiviati per finalità diverse (immigrazione e visti, dati relativi ai passeggeri dei voli aerei e dati relativi alle telecomunicazioni)[66]. Gli esempi più significativi sono quelli dell'Eurodac e del VIS: ossia, di banche dati di "primo pilastro", sviluppate in vista dell'attuazione della politica europea rispettivamente in materia di diritto d'asilo e di visti. Evidentemente, le impronte digitali contenute nell'Eurodac potrebbero essere assai utili per finalità di *law enforcement*: vi è da escludere, però, che possano essere impiegate a fini di identificazione in un procedimento penale. Per quel che riguarda il VIS, invece, recentemente è stata adottata la decisione 2008/633/GAI, che consente un accesso e un impiego limitato dei dati del sistema informazione visti da parte delle autorità di applicazione della legge, e pertanto anche nel procedimento penale[67].

In relazione alle altre banche dati, ossia a quelle che forniscono elementi conoscitivi "mediati", il problema si pone in termini diversi. Il diritto alla protezione del dato personale si declina quale *diritto al controllo della fonte dell'informazione*: in tal senso, pare assumere una certa importanza la disposizione dell'art. 10, comma 2, l. 121 del 1981 (ordinamento di pubblica sicurezza), secondo la quale «i dati e le

---

65 Non sfugge che, anche rispetto a questi dati, vi è una mediazione, come vi è una mediazione dell'apparato percettivo nella testimonianza. Nel caso specifico, la sua portata è contenuta dall'automaticità dell'acquisizione mercé un dispositivo tecnologico o dalla valenza scientifica del procedimento attinente alla raccolta e al confronto del dato.

66 Cfr. *Inventario 2007*, in <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Priorities/06-12-12__priorities__IT.pdf>, p. 2. Con riguardo al 2008, l'Autorità ha riconosciuto che «continuerà la tendenza ad aprire le basi di dati esistenti (sia europee che nazionali) ai fini dell'applicazione della legge, nonostante lo scopo iniziale della base di dati fosse diverso» e ha rinnovato l'impegno per un controllo sull'utilizzo per finalità di *law enforcement* di dati raccolti per altri scopi (<http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Priorities/07-12-20__Priorities__2008__IT.pdf>, p. 3-4).

67 Per questi profili, cfr. *supra*, M. Gialuz, "Principio di accessibilità e banche dati di 'primo pilastro'", § 5.

informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie» – ossia documenti conservati presso PA, sentenze o provvedimenti dell'autorità giudiziaria, atti di procedimenti penali, atti di indagine della polizia –, «fermo restando quanto stabilito dall'art. 240 c.p.p.». In effetti, la *ratio* sottesa a questa norma sembra in qualche misura analoga a quella che sancisce il divieto di utilizzo dell'anonimo o della testimonianza indiretta: il soggetto al quale si riferisce (in senso lato) l'informazione deve poter verificare l'attendibilità della fonte dell'informazione stessa. Generalmente, tale interesse – riconosciuto dal codice in diverse disposizioni, quali quelle degli artt. 195, comma 7, 203, 240 c.p.p. – viene ricondotto a un valore processuale, quale il canone del contraddittorio o il diritto di difesa[68]. In realtà, pare poter essere ricollegato in ultima istanza proprio al diritto alla protezione del dato, che ricomprende (tra le altre) anche la facoltà del titolare di conoscere direttamente la fonte delle informazioni sul proprio conto[69].

In quest'ottica, una norma riferibile specificamente a un archivio, quale quella del Centro di Elaborazione Dati, sembra poter essere generalizzata ed applicata anche alle banche dati europee, come espressione di un principio generale che esclude l'utilizzazione di elementi di prova di fonte ignota. Una conferma in tal senso sembra peraltro poter venire dall'art. 5, par. 5, della Raccomandazione (87) 15 del comitato dei ministri del Consiglio d'Europa (diretta a disciplinare l'utilizzo dei dati a carattere personale nel settore di polizia), secondo il quale «prima che i dati personali siano comunicati deve essere verificata la loro qualità. Nei limiti del possibile, in tutte le trasmissioni di dati, devono essere indicate le decisioni giudiziarie e le decisioni di proscioglimento e i dati basati su opinioni o considerazioni personali devono essere verificati alla fonte prima di essere trasmessi e occorre indicare il loro livello di accuratezza e affidabilità».

Né in senso contrario pare possa deporre la mancata reiterazione di una norma analoga nella recente decisione quadro 2008/977/GAI, che pone una disciplina generale in materia di protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale[70]. È ben vero che l'art. 9 della proposta originaria della Commissione (COM (2005) 475 def., del 4 ottobre 2005)[71] riprendeva quasi testualmente la disposizione dell'art. 5, par. 5, della Rac-

---

68 Cfr., per la testimonianza indiretta, da ultimo, C. Cesari, "Testimonianza indiretta (diritto processuale penale)", in *Enciclopedia del diritto. Annali*, II.1, Milano, Giuffrè, pp. 1136 sgg.; con riguardo all'anonimo, cfr. per tutti P. Corso, *Notizie anonime e processo penale*, Padova, Cedam, 1977, p. 162.

69 Vale la pena riprendere il punto di vista di A.A. Dalia, *op. cit.*, p. 63, il quale ritiene la previsione della necessità di acquisire la fonte come finalizzata proprio a eliminare l'«intermediazione della banca».

70 In *GUUE*, L 350, 30 dicembre 2008, p. 60.

71 *Documento del Consiglio n. 2005/0202 (CNS)*, 4 ottobre 2005, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0475:FIN:IT:PDF>.

comandazione; in realtà, non sembra che la riformulazione del dettato normativo possa assumere significato decisivo: a ben considerare, l'art. 8 della decisione 2008/977/GAI sembra riaffermare proprio il valore della piena controllabilità della fonte, laddove prescrive allo Stato membro che trasmette i dati di corredarli «delle informazioni disponibili che consentono allo Stato membro ricevente di valutare il livello di esattezza, completezza, aggiornamento e affidabilità». Certo, il legislatore europeo avrebbe potuto (e dovuto) essere più chiaro su un punto decisivo come questo. Vi è da auspicare che il legislatore nazionale sia più coraggioso e che, in sede di attuazione della decisione quadro nell'ordinamento italiano, precisi la portata di tale previsione generica e subordini espressamente l'impiego nel procedimento penale dei dati trasmessi all'acquisizione delle fonti documentali originarie.

Di più: sarebbe una buona occasione per specificare il riferimento – di per sé ambiguo – al "procedimento giudiziario", contenuto nell'art. 10, comma 2, l. 121 del 1981. Tale locuzione è stata interpretata restrittivamente, nel senso che la norma opererebbe solo con riguardo al dibattimento[72]. In realtà, pare che essa debba trovare applicazione anche al di fuori del dibattimento, quanto meno in materia cautelare: in tale ambito, infatti, operano, per espressa scelta del legislatore, tanto l'art. 195 c.p.p., quanto l'art. 203 c.p.p.

Un ultimo limite fondamentale, che interessa qualsiasi banca dati, è quello relativo al divieto di decisioni fondate unicamente su un trattamento automatizzato di dati. Ora, tale regola assume nel nostro ordinamento carattere assoluto: l'art. 14 del d.lgs. 30 giugno 2003, n. 196 (codice privacy) – che trova applicazione anche al trattamento effettuato per ragioni di giustizia e a quello da parte di forze di polizia, non essendo tra le norme escluse ai sensi degli artt. 47 e 53 – stabilisce infatti che «nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato». Una disposizione, questa, che riprende l'art. 17 l. 31 dicembre 1996, n. 675, il quale aveva dato attuazione all'art. 15 della direttiva 95/46/CE[73]. Si badi, però, che una norma analoga era stata posta proprio dall'art. 9, comma 4, l. 121 del 1981, sia pure in termini più restrittivi, in quanto si faceva riferimento alle "decisioni giudiziarie"[74].

Ancora una volta, la decisione quadro sulla protezione dei dati personali nel "terzo pilastro" sembra meno restrittiva, in quanto non esclude in assoluto la

---

72 Il riferimento è a S. Fratucello, "La protezione dei dati personali come limite all'accertamento penale nel 'codice della privacy'", in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. Negri, Roma, Aracne, 2007, p. 137.

73 Cfr. G. Buttarelli, *op. cit.*, pp. 341 sgg.; P. Ceccoli, "*sub* art. 14", in *Codice della privacy*, tomo I, Milano, Giuffrè, 2004, p. 191. In termini generali, sul *profiling*, cfr. *supra*, M. Gialuz, "La cooperazione informativa", cit., nota 31.

74 Tale disposizione è stata poi abrogata proprio dalla l. 31 dicembre 1996, n. 675 (art. 43).

possibilità di ricorrere a decisioni fondate esclusivamente su trattamenti automatizzati: si limita a richiedere che essa sia adottata solo se «autorizzata da una legge che precisi i provvedimenti atti a salvaguardare gli interessi legittimi della persona interessata» (art. 7 della decisione quadro 2008/977/GAI).

6. Conclusioni

All'esito delle riflessioni svolte, si può fornire una risposta all'interrogativo dal quale si sono prese le mosse. Senza dubbio le banche dati europee possono funzionare come fonti di prova che, avendo carattere essenzialmente transnazionale, consentono di superare almeno in parte le dinamiche tradizionali dell'assistenza giudiziaria e di fornire direttamente elementi conoscitivi agli attori del procedimento penale.

Come si è visto, la portata di tale affermazione varia a seconda della tipologia di banca dati e della natura dell'informazione che si prende in considerazione.

Per quel che riguarda quelle che possono qualificarsi come "banche dati europee in senso stretto", ossia i sistemi informativi europei centralizzati (SIS, SID, TECS di Europol, EPOC-II di Eurojust, Eurodac, VIS) e le banche dati interconnesse (quali saranno i casellari giudiziari europei e le banche dati relative alle immatricolazioni dei veicoli), che garantiscono una disponibilità *immediata* dell'informazione, si può asserire che permettono di aggirare parzialmente gli strumenti tradizionali di assistenza. Esse forniscono ai soggetti del procedimento penale degli elementi conoscitivi: a quali soggetti e in quali fasi dipende dalla natura del dato.

Ove venga in rilievo un'informazione di origine giudiziaria oppure documentale (ossia riferibile a una *res* prodotta al di fuori del procedimento), quale quella relativa alle precedenti condanne o al numero di immatricolazione di un veicolo, il sistema informativo consente di fornire l'elemento conoscitivo da utilizzare direttamente nella fase preliminare: con riguardo all'ambito cautelare e a quello dibattimentale, il rispetto del diritto alla protezione del dato – che si declina in termini processuali come diritto al contraddittorio e alla difesa – postula l'acquisizione del documento originale dal quale il dato è estratto.

Laddove si tratti invece di un dato che è il frutto di una precedente indagine amministrativa, si aggiungerà il limite funzionale: il "documento" corrispondente potrà essere acquisito – attraverso il mandato europeo di ricerca della prova o mediante rogatoria – solo a condizione che non sia possibile acquisire la prova costituenda.

Non troppo dissimile il discorso relativo alle banche dati europee in senso lato, ossia alle banche dati nazionali per le quali è previsto un collegamento mediato, per effetto dell'accesso indiretto (si allude alle banche dati dattiloscopiche e a quelle genetiche) o dell'obbligo di trasmettere le informazioni in attuazione del canone di disponibilità. In apparenza, oltre ai limiti indicati in precedenza, sembrerebbe esservi un vincolo territoriale: anche l'uso in indagini, per i dati

più sensibili (ossia impronte digitali e profili DNA), sembrerebbe richiedere il ricorso ai canali più garantiti dell'assistenza giudiziaria. In realtà, l'attuazione della decisione quadro n. 960 del 2006 dovrebbe consentire di trasmettere in forma semplificata anche questi dati: ovviamente, solo a fini investigativi e con l'esclusione di un utilizzo "a fini di prova davanti all'autorità giudiziaria", ossia per l'adozione di misure cautelari.

In definitiva, dunque, le banche dati europee possono produrre *direttamente* elementi di prova da utilizzare nella fase del procedimento penale che presenta il minor tasso di formalizzazione, ossia la fase delle indagini preliminari. Almeno con riguardo a questa, si può asserire che esse contribuiscono – insieme ad altri strumenti – al successo di quelle forme alternative di cooperazione in materia penale, che stanno erodendo il campo di applicazione del tradizionale strumento rogatoriale[75]. Si dà peraltro un'eccezione, che deriva dalla tipologia del provvedimento da adottare sulla base delle informazioni derivanti dagli archivi informatici: laddove si tratti di un vero e proprio giudizio – sia pure interinale – sulla responsabilità – qual è quello sotteso all'adozione di una misura cautelare – non si possono impiegare informazioni trasmesse dalle autorità di *law enforcement*, ma è necessario ottenere il documento originario mediante gli strumenti dell'assistenza giudiziaria o l'emissione di un mandato europeo di ricerca della prova.

Per quel che concerne la fase strettamente processuale, occorre distinguere: con riferimento al dibattimento, non v'è dubbio che non si possa utilizzare direttamente l'elemento cognitivo trasmesso dalla banca dati. La banca dati consentirà di individuarlo, ma poi dovrà essere acquisito mediante canali più garantiti. In relazione invece all'udienza preliminare e ai riti alternativi, si deve ulteriormente precisare: va esclusa la possibilità di utilizzare il dato dell'archivio nazionale trasmesso ai sensi della decisione n. 960 del 2006, in quanto essa stessa si riferisce alla sola fase di indagine; si potranno invece utilizzare i dati resi disponibili da quelle che si sono definite banche dati europee in senso stretto.

Ad ogni modo, le banche dati svolgeranno un ruolo fondamentale nell'individuazione delle prove da acquisire successivamente mediante gli strumenti tradizionali di assistenza oppure attraverso le forme previste dalla Convenzione europea di assistenza giudiziaria – purtroppo non ancora ratificata dal nostro Paese –, o, ancora, oggi, attraverso il mandato europeo di ricerca della prova.

---

75 Cfr., per tutti, E. Selvaggi, "Le nuove forme della cooperazione: un ponte verso il futuro", in *Rogatorie penali e cooperazione giudiziaria internazionale*, a cura di G. La Greca e M.R. Marchetti, Torino, Giappichelli, 2003, pp. 465 sgg. Con riguardo, invece, alle nuove prospettive di cooperazione contemplate dalla Convenzione Cybercrime con riferimento specifico ai dati informatici, si leggano, E. Selvaggi, *Cooperazione giudiziaria veloce ed efficace*, in "Guida al diritto", 2008, n. 16, p. 72; Id., *Task force operativa 24 ore al giorno*, *ivi*, 2008, n. 16, pp. 75 sgg.