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.