Information sharing nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione

ANTONELLA MARANDOLA
Professore associato di Procedura penale
Università di Trieste

Sommario: 1. Il trattato di Prüm come strumento di cooperazione rafforzata in materia penale. – 2. Lo scambio di informazioni nel Trattato di Prüm: un'attuazione del principio di disponibilità con alcuni limiti e una zona d'ombra. – 3. (Segue): L'istituzione e la conservazione delle banche dati. – 4. (Segue): Le ipotesi particolari di trasmissione di informazioni. – 5. Diritto alla sicurezza *vs* diritto alla riservatezza. – 6. Le prospettive legislative dell'Italia.

1. Il trattato di Prüm come strumento di cooperazione rafforzata in materia penale

La firma del Trattato di Prüm, avvenuta il 27 maggio 2005, da parte di sette Stati membri dell'Unione europea (Belgio, Lussemburgo, Paesi Bassi, Germania, Francia, Spagna e Austria) si pone quale pietra miliare del lungo e complesso *iter* volto a garantire un elevato livello di protezione ai cittadini nello spazio di libertà, sicurezza e giustizia delineato dall'art. 29 del TUE nell'ambito del c.d. terzo pilastro[1]. Le *guidelines* finalizzate alla realizzazione di questo obiettivo sono individuate, ai sensi del par. 2 dell'art. 29 TUE, nella duplice prospettiva, da leggersi in chiave di complementarità e di reciproca interazione, della progressiva armonizzazione degli ordinamenti statuali interni in materia penale, da un lato, e del rafforzamento della cooperazione tra le forze di polizia e le autorità giudiziarie degli Stati membri, dall'altro lato[2].

Collocandosi in questo secondo angolo visuale, il Trattato di Prüm si pone l'obiettivo di potenziare la cooperazione tra le autorità di *law enforcement* nei settori della lotta contro il terrorismo, della criminalità transnazionale e dell'immigrazione clandestina attraverso una serie di strumenti che possono utilmente ricondursi a due aree tematiche[3].

---

1 Per una lettura diacronica degli atti normativi adottati al fine di realizzare lo spazio comune di libertà sicurezza e giustizia proclamato dai Trattati di Amsterdam e di Nizza e ribadito nelle conclusioni prese in seno al Consiglio europeo di Tampere, si vedano, fra gli altri: E. Aprile, *Diritto processuale penale europeo e internazionale*, Padova, Cedam, 2007, *passim*; M Chiavario, *Cooperazione giudiziaria e di polizia in materia penale a livello europeo*, in "Rivista italiana di diritto e procedura penale", 2005, p. 974; L. Salazar, "Le fonti tipiche dell'Unione Europea", in *Rogatorie penali e cooperazione giudiziaria e internazionale*, a cura di G. L. Greca e M. R. Marchetti, Torino, Giappichelli, 2003, pp. 57 sgg. Per un'analisi delle iniziative volte al superamento della architettura dell'*aquis* U.E. fondata su tre pilastri (Comunità europea, PESC, cioè politica estera e sicurezza comune, e GAI, cioè giustizia e affari interni), ad opera prima del Trattato che adotta una Costituzione per l'Europa, sottoscritto a Roma il 12 gennaio 2005, e poi del Trattato di Lisbona del 13 dicembre 2007, si vedano: M. Bargis, *Costituzione per l'Europa e cooperazione giudiziaria in materia penale*, in "Rivista italiana di diritto e procedura penale", 2005, p. 144; G. De Amicis - G. Uzzolino, *Lo spazio di libertà, sicurezza e giustizia nelle disposizioni penali del Trattato che istituisce una Costituzione per l'Europa*, in "Cassazione penale", 2004, p. 3067; T. Rafaraci, "Lo spazio di libertà, sicurezza e giustizia nel crogiuolo della costruzione europea", in *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, a cura di T. Rafaraci, Milano, Giuffré, 2007, pp. 3 sgg.

2 Sottolineano l'esistenza di un rapporto biunivoco tra cooperazione giudiziaria e armonizzazione penale: E. Bernardi, *Strategie per l'armonizzazione dei sistemi penali europei*, in "Rivista trimestrale di diritto penale dell'economia", 2002, p. 789; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale. Verso un sistema integrato di forme e strumenti di collaborazione tra le autorità giudiziarie*, Milano, Giuffrè, 2007, p. 290.

3 Onde individuare l'ambito di applicazione del Trattato con riferimento alle tipologie di reati, qualche indicazione può trarsi dall'elenco di fattispecie delittuose contemplato dall'art. 2 della decisione quadro 2002/584/GAI del Consiglio in materia di mandato d'arresto europeo, pubblicata in *GUUE*, L 190, 18 luglio 2002, p. 1.

La prima, più caratterizzante, si articola in due ulteriori sottosistemi, l'uno attinente alla semplificazione dello scambio di informazioni tra le autorità degli Stati membri come presupposto indispensabile del rafforzamento della cooperazione, l'altro, quale necessario *pendant*, riguardante la predisposizione di adeguate garanzie in materia di tutela dei dati, in tal modo circolanti. In questo settore, il Trattato di Prüm mostra di recepire, con alcuni limiti, le enunciazioni di principio contenute nel Programma dell'Aia adottato dal Consiglio Europeo il 4 novembre 2004[4], ed in particolare l'affermazione secondo cui il potenziamento della cooperazione di polizia e giudiziaria in materia penale richiede «un approccio innovativo» nei confronti dello scambio di informazioni fra le autorità competenti degli Stati membri, le quali dovrebbero informarsi al cd. principio di disponibilità enunciato in seno al Programma.

In sede di prima approssimazione, l'attuazione da parte del Trattato di Prüm del principio di disponibilità – nei termini di accesso, reciproco e diretto, di informazioni contenute nei *databases* di uno Stato membro da parte di un'autorità di altro Stato membro – si caratterizza in quanto si allontana dai precedenti strumenti di informazione, fra i quali quelli previsti dalle Convenzioni di applicazione Schengen ed Europol, basati sul meccanismo della mediazione della richiesta ad un servizio centrale cui sono collegate le banche dati nazionali[5].

La seconda linea tematica, di carattere residuale, comprende una serie di istituti, di matrice prettamente operativa, che configurano altrettante forme di intervento diretto o congiunto delle forze di polizia di uno Stato membro nel territorio e nello spazio aereo di altro Stato con finalità di prevenzione di atti terroristici e di altre attività criminali transfrontaliere, tra i quali la previsione di scorte di sicurezza armata sui voli aerei (art. 17), le misure relative alla lotta contro l'immigrazione illegale (artt. 20 sg.), le forme di intervento congiunto nel territorio di uno Stato membro (art. 24), le operazioni di polizia transfrontaliera in caso di pericolo imminente (art. 25) e la cooperazione su richiesta (art. 27).

Appare opportuno sottolineare come la suddetta distinzione non rileva solo ai fini di una classificazione squisitamente dogmatica, ma anche nell'ottica della futura ricezione delle disposizioni del Trattato in seno all'Unione Europea.

Giova, a tal fine, premettere alcune considerazioni intorno alla natura giuridica del Trattato di Prüm (di seguito denominato Trattato).

Il testo appartiene al *genus* del diritto internazionale pattizio, esulando, per contro, dal diritto comunitario in quanto negoziato da alcuni soltanto degli Stati membri dell'Unione – ma aperto all'adesione di tutti gli altri Stati membri dell'Unione – e concluso al di fuori dello spazio giuridico europeo, senza avva-

---

4 Pubblicato in *GUUE*, C 53, 3 marzo 2005, p. 1.

5 Per un approfondimento sui meccanismi di funzionamento delle banche dati tradizionalmente operanti nell'*aquis* UE, si veda *supra*, F. Decli - G. Marando, "Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia".

lersi degli strumenti preordinati *ad hoc* dal TUE, per le ipotesi di cooperazione rafforzata.

I sette Stati firmatari si proponevano, infatti, di addivenire ad una più stretta collaborazione nel settore della criminalità transnazionale senza pregiudicare le sorti del TUE e lasciando, al contempo, aperta la prospettiva della futura ricezione dell'accordo da parte dell'Unione, sulla base di uno schema analogo a quello a suo tempo seguìto per gli accordi di Schengen.

L'iniziativa protesa alla realizzazione di una cooperazione rafforzata tra alcuni Stati membri – al di fuori delle procedure previste dall'art. 43 TUE – ha sollevato, da una parte, alcune perplessità circa la legittimità delle modalità di adozione del testo[6], mentre, dall'altra parte, ha reso necessario dotare lo strumento *de quo* di alcune clausole di adattamento al fine di garantirne la compatibilità con le disposizioni contenute nel Trattato dell'Unione anche nell'ottica dell'integrazione di Prüm nell'*aquis* UE.

Così, l'art. 47, par. 1, del Trattato enuncia, *in primis*, il principio di prevalenza del diritto dell'Unione Europea sulle norme in esso contenute, qualora quest'ultime risultino incompatibili con le prime; in secondo luogo, l'art. 1, par. 4, prevede che entro tre anni dalla data della sua entrata in vigore dovrà essere avviata una iniziativa volta a consentirne l'integrazione nello spazio giuridico dell'Unione europea «sulla base di una valutazione dell'esperienza acquisita grazie all'attuazione del Trattato stesso».

A tale disposizione è stata data realizzazione, in seguito all'intenso dibattito avviato dalla Presidenza tedesca dell'Unione durante la riunione dei ministri svoltasi a Dresda il 15-16 gennaio 2007, con una prima proposta, sottoscritta da tredici Stati membri, volta a consentire l'ingresso nel diritto dell'Unione delle principali disposizioni del Trattato, cui è seguita una seconda iniziativa, di poco successiva, di analogo tenore ma proveniente da quindici Stati membri[7].

Successivamente durante il Consiglio GAI del 15 febbraio 2007[8] è stato raggiunto un accordo per la trasposizione delle «parti essenziali» del Trattato mediante lo strumento della decisione del "terzo pilastro"[9]. A questo ha fatto seguito

---

6 Sul punto, il Garante europeo ha messo in luce che il procedimento adottato potrebbe configurare una violazione della procedura di cooperazione rafforzata prevista dall'art. 40 TUE nell'ambito del "terzo pilastro", in quanto gli Stati aderenti a Prüm avrebbero conseguito, mediante l'adozione di tale strumento giuridico, il fine di evitare l'*iter* legislativo previsto in ambito GAI, che subordina l'adozione delle decisioni al requisito dell'unanimità (il testo del Parere è pubblicato in *GUUE*, C 169, 21 luglio 2007, p. 2). Cfr. anche *supra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea", § 8.

7 Il testo dell'iniziativa è pubblicato in *GUUE*, C 71, 28 marzo 2007, p. 35.

8 Si veda il Comunicato stampa, 2781ª sessione del Consiglio "Giustizia e affari interni", Bruxelles, 15 febbraio 2007.

9 Sul punto, alcuni dubbi sono stati sollevati con riferimento alla base giuridica della decisione di cui all'art. 34, par. 2, lett. *c*), del Trattato UE e si è ritenuta, per contro, più adeguata la base giuridica della decisione quadro di cui all'art. 34, par. 2, lett. *b*), caratterizzata da una maggiore

una Risoluzione del Parlamento Europeo (7 giugno 2007) che si è espressa in senso favorevole all'adesione della proposta di decisione da parte del Consiglio.

L'iniziativa ha, infine, trovato definitiva consacrazione nella recente decisione 2008/615/GAI, del 23 giugno 2008, la quale, come premesso, si propone, tra l'altro, di incorporare la sostanza delle disposizioni in seno al quadro giuridico europeo.

Mantenendo, per il momento, fermo lo sguardo sul tenore normativo del Trattato è necessario operare un *distinguo* tra due settori tematici: da un lato, si collocano le disposizioni afferenti allo scambio di dati tra le autorità degli Stati membri e alla correlativa tutela delle informazioni, in relazione alle quali, trattandosi di materie attinenti al "terzo pilastro", si prevede l'integrale inserimento in ambito europeo; dall'altro lato, si situano gli istituti che coinvolgono materie nelle quali esiste una competenza comunitaria, come le indicate disposizioni relative agli agenti di sicurezza a bordo degli aerei (cd. *air marshals*, *ex* art. 17), le misure volte a combattere l'immigrazione clandestina (artt. 20 sg.), quelle concernenti le operazioni di polizia transfrontaliera in caso di pericolo imminente (art. 25) e la cooperazione su richiesta (art. 27).

2. Lo scambio di informazioni nel Trattato di Prüm: un'attuazione del principio di disponibilità con alcuni limiti e una zona d'ombra

È opinione condivisa in dottrina che la dimensione transnazionale delle nuove forme di criminalità organizzata, unitamente al carattere dinamico che ne consente la dislocazione su vasta scala all'interno del territorio dell'Unione europea e all'impiego di tecniche criminose che consentono di travalicare i confini dei singoli Stati, ha reso necessario potenziare il coordinamento tra le autorità nazionali assicurando la circolarità dei dati in possesso dei singoli Stati sia a fini preventivi che di indagine[10].

A tal riguardo, un vero e proprio spartiacque in tema di interscambio di informazioni è rappresentato, come già anticipato, dal Programma dell'Aia, adottato nel novembre del 2004 dal Consiglio Europeo a Bruxelles. Il Consiglio, coniando il cd. principio di disponibilità, ha previsto che, a far data dal 1° gennaio 2008, l'accesso e lo scambio di informazioni e di *intelligence* tra gli Stati membri dell'Unione debba avvenire in modo tale che un ufficiale di contrasto di uno Stato membro, che necessiti di informazioni in funzione preventiva e di repressione di determinati reati possa ottenerle direttamente da un altro Stato membro, alle

---

apertura alla consultazione del Parlamento, in quanto lo strumento da adottare perseguirebbe, sia pure indirettamente, il fine di armonizzare le legislazioni tra gli Stati membri.

10 Per la definizione di "reato transnazionale", in seguito all'entrata in vigore della Convenzione di Palermo, si veda E. Rosi, "Il reato transnazionale", in *Criminalità organizzata transnazionale e sistema penale italiano. La Convenzione ONU di Palermo*, a cura di E. Rosi, Milano, Ipsoa, 2007, pp. 67 sgg.

stesse condizioni previste per le autorità interne. Superando le precedenti impostazioni in materia, il principio *de quo* mira a realizzare la condivisione dei dati (*information sharing*) in possesso di un singolo Stato con le autorità di *law enforcement* degli altri Stati, preludendo, per tale via, alla creazione di uno spazio di libera circolazione delle informazioni, nel rispetto delle norme di garanzia sulla protezione dei dati raccolti[11].

Per un verso, infatti, l'enunciazione del principio di disponibilità in materia di scambio di informazioni rappresenta una netta innovazione rispetto agli assetti dei circuiti informativi tradizionalmente operanti su scala europea – quali SIS (Sistema Informativo Schengen), E-TECS di Europol, EPOC-III di Eurojust – il cui funzionamento, informandosi al principio di base che i dati appartengono a chi li detiene, si fonda sulla mediazione di una unità centrale attivabile a richiesta delle sezioni nazionali e degli Stati membri, i quali stabiliscono limiti e condizioni di accesso ai propri databases[12].

Per altro verso, l'obiettivo posto dal Programma dell'Aia si pone quale lineaguida degli strumenti giuridici volti a realizzare il rafforzamento della cooperazione giudiziaria mediante l'interscambio diretto delle informazioni in possesso dei singoli Stati[13].

La materia dello scambio di informazioni sulla base del principio di disponibilità trova compiuta ed autonoma trattazione negli artt. 2-15 del Capitolo II del Trattato, recante la disciplina delle modalità con cui avviene l'*information sharing* (artt. 2-12) e la previsione della trasmissione di dati in occasione di grandi eventi (artt. 13-15), cui deve aggiungersi, per contiguità di contenuto, la menzione specifica dello scambio di dati in funzione di contrasto al terrorismo (art. 16), benché attratta nell'orbita del Capitolo III, dedicato alle misure di prevenzione di attacchi terroristici[14].

Sotto tale profilo, deve evidenziarsi che il merito della prospettiva coltivata dal Trattato è non solo quella di consentire che le informazioni confluiscano in un unico *network* di banche dati direttamente consultabile dalle autorità interne

---

11 Per un approfondimento del principio di disponibilità nel quadro del Programma dell'Aia, si rinvia, ancora, a S. Ciampi, *op. cit*.

12 Al riguardo, si veda *supra*, F. Decli - G. Marando, *op. cit*.

13 Tra gli strumenti giuridici che attuano il principio di disponibilità enunciato dal Programma in ambito UE si annoverano: la proposta di decisione quadro della Commissione n. 490 del 2005 sullo scambio di informazioni in virtù del principio di disponibilità; la decisione del Consiglio n. 671 del 2005 concernente lo scambio di informazioni e la cooperazione in materia di reati terroristici, 2005/671/GAI del 20 settembre 2005 (in *GUUE*, L 253, 29 settembre 2005, p. 22); la decisione del Consiglio n. 960 del 18 dicembre 2006 sull'applicazione del principio di disponibilità allo scambio di informazioni tra i Paesi UE al fine del rafforzamento della cooperazione di polizia (in *GUUE*, L 386, 29 dicembre 2006, p. 89). Per un approfondimento, si veda, *amplius*, S. Ciampi, *op. cit*.

14 Per un' analisi testuale del Trattato, si veda F. Gandini, *Il trattato di Prüm articolo per articolo. Ecco le nuove frontiere per la sicurezza. Banche dati antiterrorismo e interventi congiunti in 7 Stati Ue*, in "Diritto e giustizia", 2006, n. 37, pp. 57 sgg.

degli Stati membri, ma anche quella di realizzare, attraverso gli impegni assunti dalle Parti contraenti a livello internazionale, e, sia pure indirettamente, una armonizzazione degli ordinamenti interni dei singoli Stati[15].

Orbene, il potenziamento della cooperazione transfrontaliera che il testo *de quo* consente, anche e, soprattutto, nell'ottica della lotta al terrorismo e alla criminalità transfrontaliera, soddisfacendo pienamente i requisiti sostanziali del Programma dell'Aia, ha, come si è detto, indotto il Consiglio dell'Unione europea a fare proprie le disposizioni del Trattato attraverso la decisione 2008/615/GAI[16].

L'atto europeo mutua e recepisce quelle disposizioni che vengono, quindi, ad inserirsi, a pieno titolo, all'interno della cornice legislativa europea determinando, del pari, l'accelerazione dell'operatività dei meccanismi di fruizione "diretta" dei dati di *intelligence* di cui dispongono i singoli Stati, in ossequio alle direttive del Programma[17], rendendo, fra l'altro, superflua la predisposizione di uno schedario unico "europeo" che avrebbe comportato costi e tempi indubbiamente più ampi.

By-passando la singola adesione degli Stati che ne avevano assunto l'iniziativa e estendendone la valenza agli altri Stati membri dell'Unione, la decisione del 2008 ricalca in larghissima parte, infatti, il contenuto e la sostanza del Trattato: essa contiene disposizioni riguardanti il trasferimento automatizzato di profili DNA; dati in materia di impronte digitali (*fingerprints*) e dati relativi ai veicoli iscritti nei pubblici registri e, più in generale, dei dati in relazione a eventi di rilievo a dimensione transfrontaliera, nell'intento univoco di prevenire reati terroristici e potenziare la cooperazione di polizia sovranazionale.

Al fine di realizzare la condivisione di informazioni, gli Stati membri si impegnano, infatti, a istituire e conservare tre banche dati nazionali accessibili online e contenenti profili di DNA, dati in materia di impronte digitali (*fingerprints*) e dati relativi ai veicoli iscritti nei pubblici registri. A differenza di quest'ultima banca dati, che permette di accedere immediatamente ai dati relativi al proprietario a partire dal numero di immatricolazione, gli archivi con profili DNA e quelli dattiloscopici non consentono di pervenire direttamente ad una identificazione della persona cui si riferiscono, ma sono soggetti ad un procedimento comune di consultazione che si articola in due fasi (cd. doppio binario).

---

15 Configura l'armonizzazione come una tecnica normativa che persegue il ravvicinamento di diversi ordinamenti, il quale può presentarsi in forma spontanea o indotta, S. Allegrezza, "Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo", in *L'area di libertà sicurezza e giustizia*, cit., p. 702.

16 Pubblicata in *GUUE*, L 210, 6 agosto 2008, p. 1. Va poi segnalata la contestuale decisione 2008/616/GAI, volta a stabilire le disposizioni amministrative e tecniche necessarie all'attuazione della decisione 2008/615/GAI (in *GUUE*, L 210, 6 agosto 2008, p. 12).

17 In ambito UE, il principio di disponibilità nell'ottica del Programma dell'Aia era stato recepito nella proposta di decisione quadro COM (2005) 490 def., del 12 ottobre 2005. Cfr., *supra*, S. Ciampi, *op. cit.*, § 4. In argomento, si veda anche la decisione 2005/671/GAI del 20 settembre 2005 (in *GUUE*, L 253, 29 settembre 2005, p. 22).

La prima fase disciplina l'accesso automatizzato on-line alle informazioni contenute all'interno delle banche dati. Come si è anticipato, essa non consente l'accesso diretto ai dati che permettono di risalire all'identità della persona interessata, ma, più semplicemente, rende disponibili i soli indici di consultazione. Pertanto, mediante la procedura di accesso automatizzato (cd. sistema *hit/no hit*) l'autorità richiedente potrà attingere unicamente ad un indice di consultazione anonimo e ad un numero di riferimento (*reference index*) al fine di verificare la presenza del dato nell'archivio.

La procedura di accesso, a seconda del tipo di informazione in possesso della parte richiedente, si articola in due differenti modalità di ricerca.

Sotto tale aspetto, il Trattato, prima, e la decisione europea, poi, prevedono che, ove l'autorità compulsante disponga di un profilo DNA riferibile ad una persona identificata, questa può avviare una procedura di consultazione automatizzata (*automated searching*) al fine di verificare se il dato immesso nel sistema trovi una concordanza all'interno del complesso di informazioni registrate nell'archivio. Lo scopo della consultazione è, pertanto, quello di accertare se la banca dati contenga un profilo corrispondente a quello trasmesso. Al termine della ricerca automatizzata, la parte compulsante è raggiunta da una informazione che comunica, in caso di esito positivo, il solo *reference index*, attestante la sussistenza in banca dati del profilo richiesto, e, in caso di esito negativo, l'impossibilità di registrare una concordanza tra i dati immessi e quelli registrati.

Ove, per contro, la parte richiedente disponga di un profilo DNA che non sia attribuibile a persona determinata o determinabile (cd. *open record*), viene dato avvio ad un procedimento di comparazione (*automated comparison*). La procedura di comparazione viene attivata mediante la trasmissione del profilo anonimo al fine di saggiarne la corrispondenza con tutti i dati contenuti in archivio, siano o meno riferibili a persona determinata.

Le due forme di accesso alla banca dati, pertanto, si distinguono principalmente in ragione della fonte di compulsazione, costituita, nel primo caso, da un profilo identificato, e, nel secondo caso, da una traccia aperta, mentre la procedura di ricerca avviene in forma automatizzata, con modalità analoghe.

Un ulteriore elemento di differenziazione è dato dalla comunicazione relativa agli esiti della ricerca alla Parte compulsante: l'inoltro avviene, in forma non automatizzata, a cura dell'autorità richiesta e solo nei casi in cui il sistema abbia permesso di registrare una concordanza.

Quando l'accesso automatizzato on-line mediante consultazione o comparazione abbia dato esito positivo, si apre, infatti, la seconda fase del procedimento che riguarda la trasmissione delle informazioni ricollegabili ai dati di indice all'autorità richiedente. Sotto tale profilo, la disciplina appare, invero, piuttosto scarna: la normativa internazionale si limita, infatti, a prevedere la necessità di una richiesta esplicita da parte dell'autorità interessata ad ottenere le ulteriori informazioni ricollegabili all'indice di consultazione, e rinviando, per i profili procedurali, alle norme di diritto interno dello Stato membro e alle Convenzioni sull'assistenza giudiziaria *ivi* vigenti.

Il Trattato lascia impregiudicata la centrale questione se in capo alla Parte richiesta debba configurarsi un obbligo, un onere o una mera facoltà di trasmettere l'informazione all'autorità richiedente. Esula, parimenti, dalla disciplina pattizia, la specificazione dei modi e dei tempi del procedimento informativo. Sul punto, il Trattato si limita, infatti, ad operare un generico rinvio alle pregresse Convenzioni regolanti i rapporti di assistenza giudiziaria tra gli Stati dell'Unione europea (artt. 5 e 10)[18].

La materia, com'è noto, è regolata dalla Convenzione europea di Strasburgo del 20 aprile 1959[19], nonché dalla Convenzione sull'assistenza giudiziaria adottata dal Consiglio dell'Unione europea il 29 maggio 2000[20]. Il rinvio a tali atti normativi parrebbe configurare, a carico dei soli Stati che abbiano ratificato gli accordi *de quibus*[21], un dovere dell'autorità interna di dare seguito alla richiesta di trasmissioni di informazioni collegate al *reference index*. Il rifiuto di adempiere potrebbe essere opposto solo nei casi espressamente previsti e, in ogni caso, dovrebbe essere corredato di motivazione[22].

La smagliatura normativa è lasciata indenne nel testo della decisione 2008/615/GAI, che conferma il richiamo alla normativa interna.

Verosimilmente, la questione potrebbe essere risolta ricorrendo alle decisioni-quadro 2006/960/GAI e 2008/977/GAI che configurano una sorta di "mutua

---

18 Diversamente, la proposta di decisione quadro in tema di principio di disponibilità configurava *expressis verbis* un obbligo in capo all'autorità richiesta di fornire le informazioni richieste entro termini prestabiliti, potendo opporre un rifiuto solo in casi tassativi.

19 Ai sensi della Convenzione di Strasburgo, l'assistenza giudiziaria deve essere concessa dalle Parti contraenti secondo le modalità stabilite dallo Stato richiesto, e può essere rifiutata solo in casi tassativamente indicati (art. 2) e con atto motivato (art. 19); il testo specifica, poi, i casi nei quali la comunicazione può avvenire in via diretta tra le autorità dei singoli Stati (art. 15).

20 La Convenzione di mutua assistenza del 29 maggio 2000 modifica il precedente quadro normativo spostando il baricentro del coordinamento tra gli Stati e specificando le modalità e i termini che scandiscono il procedimento di trasmissione degli atti e delle informazioni. In particolare, l'accordo pone a carico dello Stato richiesto l'obbligo formale di fornire l'assistenza nel rispetto delle modalità (par. 1) e dei termini (par. 2) indicati dall'Autorità richiedente, anziché dalla Parte richiesta, prevedendo, in caso di inottemperanza, che quest'ultima sia tenuta a darne pronta informazione.

21 La Convenzione sull'assistenza giudiziaria del 2000 non è stata ratificata dall'Italia, e, pertanto, non è entrata in vigore nel nostro ordinamento: in argomento, si veda E. Aprile, *op. cit.*, p. 48; E. Zanetti, "Le convenzioni vigenti", in *Rogatorie penali e cooperazione giudiziaria internazionale*, cit., pp. 79 sgg.

22 Cfr. la decisione n. 960 del 2006, che, dando piena attuazione al principio di disponibilità, prevede il diritto della parte richiedente, con correlativo obbligo di attivazione in capo all'autorità richiesta, di ottenere i dati alle medesime, o più favorevoli condizioni previste per gli organi competenti sul piano nazionale. A tal fine, la parte interessata deve inoltrare una richiesta motivata che fa sorgere a carico dell'interlocutore un dovere di fornire le informazioni e i dati di *intelligence* entro otto ore, prorogabile fino a tre giorni, nel caso in cui la richiesta sia contrassegnata dal requisito dell'urgenza, ed entro una settimana nei casi non urgenti. Per un approfondimento, si rinvia a S. Ciampi, *op. cit.*, § 9.

circolarità" delle informazioni, rafforzandosi, così, l'idea della reciproca complementarietà dei più recenti strumenti normativi sopranazionali[23].

In ogni caso, qualora venga riscontrata una concordanza, al punto di contatto nazionale dello Stato richiedente sono notificati, per via automatizzata, i dati indicizzati; in forma automatizzata avviene altresì la comunicazione negativa.

Il Trattato non chiarisce, peraltro, se le richieste ai punti di contatto nazionali possano provenire solo dall'autorità di polizia o anche dall'autorità giudiziaria.

Sul punto, a favore della soluzione di una creazione e gestione dei rapporti tra "punti di contatto" e , dunque, della soluzione meno ampia si è espressa la dottrina[24]. La conclusione merita condivisione anche alla luce di quanto stabilisce il testo adottato dal Consiglio europeo che polarizza il suo campo di applicazione nel settore delle attività preventive del crimine, di competenza esclusiva delle autorità di *intelligence*[25], senza peraltro, che possa trascurarsi il fatto che il corredo degli strumenti indicati è creato ai fini dello scambio di informazioni, vale a dire al duplice obiettivo della prevenzione e del perseguimento dei reati.

Più precisamente, l'accesso alla banca dati DNA appare riservato esclusivamente alle attività di investigazione, come attesta l'*incipit* degli artt. 3 e 4 della decisione 2008/615/GAI («per le indagini penali»), mentre gli archivi relativi ai dati *fingerprints* e di immatricolazione dei veicoli sono compulsabili solo in casi concreti e, quanto al primo, sia per finalità preventive che di indagine (art. 8), e quanto al secondo, in ulteriore aggiunta, anche per altri illeciti che rientrino nella competenza dei tribunali e delle procure e per il mantenimento della sicurezza e all'ordine pubblico (art. 12). Se così è, appare preferibile che il testo del 2008 abbia voluto riferirsi alle autorità a cui gli ordinamenti dei singoli Stati attribuiscano una "competenza specifica" nei settori menzionati.

In conclusione, nel tessuto normativo in esame il principio di disponibilità riceve un'attuazione equilibrata, sotto il profilo sia quantitativo, sia procedimentale: da un lato, l'accesso è limitato a determinate categorie di informazioni, quali i profili di DNA, le impronte digitali e i dati relativi ai veicoli. In questa prospettiva, rispetto al Trattato, i confini di operatività del meccanismo che governa lo scambio dei dati vengono ampliati unicamente sotto l'aspetto quantitativo, fermo restando che entrambi i testi ne circoscrivono l'applicazione rispetto ad una parte soltanto delle informazioni rilevanti sul fronte della prevenzione e della repressione dei reati[26].

---

23 Si veda, *amplius*, S. Ciampi, *op. cit.*

24 V., per l'esegesi più restrittiva anche rispetto al Trattato, F. Gandini, *op. cit.*, p. 67.

25 Sul distinguo tra attività di *intelligence* e attività di indagine, si veda M. L. Di Bitonto, "Raccolta di informazioni e attività di *intelligence*", in *Contrasto al terrorismo interno e internazionale*, a cura di R. E. Kostoris e R. Orlandi, Torino, Giappichelli, 2006, p. 253.

26 Da questo punto di vista, le categorie di informazioni compulsabili sono più limitate rispetto a quanto previsto nella proposta di decisione quadro del 12 ottobre 2005, nella proposta

Dall'altro lato, l'accesso on-line agli archivi DNA e *fingerprints* mediante il sistema *hit/no hit* consente di accertare unicamente se il dato oggetto della ricerca è contenuto nella banca dati di riferimento, essendo invece precluso l'accesso diretto ad ogni altra informazione ad esso riconducibile.

Il considerando n. 18 della decisione 2008/615/GAI identifica, infatti, nel «sistema '*hit/no hit*' la struttura più idonea di raffronto dei profili anonimi, in quanto i dati supplementari a carattere personale sono scambiati solo dopo una risposta positiva; in quanto la loro trasmissione e la loro ricezione sono disciplinati dalla legislazione nazionale, fra le quali quelle relative all'assistenza giudiziaria. In tal modo si garantisce un sistema adeguato di protezione dei dati, essendo inteso che la trasmissione di dati personali ad un altro Stato membro richiede un livello adeguato di protezione dei dati da parte degli Stati riceventi».

Il principio di disponibilità risulta, invece, attuato *in toto* con riferimento ai veicoli registrati, in quanto la consultazione on-line della relativa banca dati consente di accedere, a partire dal numero di identificazione del veicolo o dal numero di targa, direttamente ai dati relativi al proprietario. Si assiste, pertanto, ad una graduazione del principio di disponibilità sulla scorta del grado di invasività dei dati oggetto di trasmissione.

3. (Segue): L'istituzione e la conservazione delle banche dati

Uno dei tratti più caratterizzanti del sistema di scambio di informazioni prefigurato dal Trattato, prima, e dall'atto del Consiglio, poi, concerne, come si è detto, l'istituzione di tre archivi centralizzati, contenenti rispettivamente i dati degli schedari nazionali di analisi DNA, i profili dattiloscopici (AFIS) e i dati contenuti nei registri nazionali dei veicoli. Deve, tuttavia, evidenziarsi come l'obbligo di costituzione e mantenimento (art. 2) è configurato a carico degli Stati dell'Unione solo con riferimento alla banca dati DNA, mentre gli archivi sulle impronte digitali (art. 8) e sui veicoli registrati (art. 12), generalmente già istituiti dagli Stati firmatari, sono oggetto di un mero dovere di conservazione e di accesso.

Il profilo istitutivo va, dunque, circoscritto alla creazione di una banca dati nazionale di analisi DNA.

La sua costituzione viene assunta quale *condicio sine qua non* di adesione al Trattato (artt. 2, parr. 3 e 42), ma il presupposto, com'è intuibile, è superato dalla decisione europea.

Peraltro, si è già chiarito come il sistema del doppio binario informativo obblighi ciascuno Stato a rendere accessibili alla consultazione diretta unicamente gli indici di riferimento, senza che sia possibile pervenire immediatamente

---

di decisione quadro del Regno di Svezia, e, infine, nella decisione quadro n. 960 del 2006. Sul punto, si veda, *supra*, S. Ciampi, *op. cit.*, § 8.

all'identificazione della persona cui i dati si riferiscono (artt. 2, par. 2 e 3, par. 2). In questa sede, occorre aggiungere che il *reference index* è costituito da un numero e da un profilo ricavato dalla parte non codificante del DNA (cd. *junk DNA*)[27].

Gli Stati, in altri termini, devono limitare la trasmissione dei risultati delle analisi DNA alle zone cromosomiche prive di espressione genetica, escludendo quei segmenti dai quali siano desumibili informazioni su specifiche caratteristiche ereditarie o sullo stato di salute. La previsione si inserisce, invero, nel solco della posizione già adottata dall'Unione Europea in materia di scambio dei risultati di analisi del DNA con due successive Risoluzioni del Consiglio, rese in data 9 giugno 1997 e 25 giugno 2001[28], in cui gli Stati membri vengono esortati a circoscrivere il materiale di scambio ai dati concernenti il profilo non codificante della molecola DNA. Nella medesima prospettiva, trattandosi di una scienza *in fieri*, il Consiglio ha stabilito che, qualora l'evoluzione scientifica consentisse di trarre informazioni su specifiche caratteristiche ereditarie dai marcatori DNA, gli Stati membri sarebbero tenuti a precluderne la disponibilità allo scambio e a distruggere i risultati delle analisi DNA da essi ricevuti e contenenti tali informazioni.

Gli elementi di alimentazione della banca dati sono rappresentati da due *species* di dati: da un lato, si pongono i profili che consentono l'identificazione della persona interessata e dall'altro le cd. tracce aperte, ovvero non attribuibili ad alcuno[29]. Il testo della decisione 2008/615/GAI – al pari, peraltro, del Trattato – nulla dispone in merito al procedimento di estrazione e tipizzazione del profilo, né in relazione alle categorie di persone che possono essere sottoposte ai prelievi, né, infine, alle modalità tecniche di raccolta.

Quanto al profilo della conservazione degli archivi, ci si è chiesti se il generico obbligo di mantenimento includa anche quello di alimentazione della banca dati mediante la raccolta di dati e informazioni da parte dei singoli Stati. Sul punto, soccorre l'interpretazione sistematica con l'art. 7 della decisione 2008/615/GAI che, analogamente a quanto prevede il Trattato, stabilisce uno specifico obbligo di attivazione in capo ai singoli Stati nei casi in cui diviene necessario acquisire un profilo DNA di un soggetto che si trova nel territorio della Parte richiesta ed è indiziato di reato nell'ambito di un procedimento in corso nello Stato richiedente. In tale ipotesi, il Paese richiesto, cui venga presentata domanda motivata contenente l'indicazione dello scopo e del titolo giuridico dell'atto («mandato

---

27 L'art. 1-*bis* della proposta di decisione del Consiglio, emendata dal Parlamento, definisce le parti non codificanti del DNA come «le aree cromosomiche che non contengono alcuna espressione genetica, ovvero non note per fornire espressione genetica, ovvero non note per fornire informazioni su caratteristiche ereditarie specifiche», precisando che «senza pregiudizio di eventuali progressi scientifici, non verranno rivelate, né ora né in futuro, ulteriori informazioni sulla parte non codificante del DNA».

28 La seconda è pubblicata in *GUUE*, C 187, 3 luglio 2001, p. 1.

29 V., per ulteriori approfondimenti sulla struttura e proprietà del DNA, R. Dominici, "Prova del DNA", in *Digesto delle discipline penalistiche*, X, Torino, Utet, 2002, pp. 373 sgg.

o una dichiarazione di inchiesta dell'autorità competente, come richiesto dalla sua legislazione nazionale»), deve accordare l'assistenza giuridica allo Stato richiedente ai fini del prelevamento e analisi del profilo genetico del soggetto sottoposto ad indagini o un procedimento penale, nel rispetto del diritto interno dello Stato membro richiesto. Da tale dettagliata disciplina, pur regolante la richiesta di acquisizione del profilo DNA nel caso specifico in cui sia in corso un procedimento penale, pare doversi dedurre, sulla base dell'argomento interpretativo per cui *ubi lex voluit dixit, ubi noluit tacuit*, l'inesistenza di un obbligo generico di alimentazione delle banche dati in capo ai singoli Stati, dovendosi interpretare il dovere di mantenimento come un generico impegno di conservazione degli archivi nazionali, pur nella consapevolezza che l'obiettivo che si prefigge la decisione, qual è quella di realizzare un miglioramento della cooperazione giudiziaria e di polizia e una facilitazione dello scambio di informazioni per aprire una nuova dimensione nella lotta alla criminalità passa, fra l'altro, attraverso un suo "corretto" mantenimento.

4. (Segue): Le ipotesi particolari di trasmissione di informazioni

Gli artt. 13-15 del provvedimento del Consiglio d'Europa del 23 giugno 2008 regolano la trasmissione di dati di natura non personale (art. 13) e personale (art. 14) ai fini del mantenimento dell'ordine pubblico e della sicurezza, nonché della prevenzione di reati, in occasione di grandi eventi a carattere transfrontaliero, tra i quali vengono menzionati, in via esemplificativa, le manifestazioni a carattere sportivo e le riunioni del Consiglio europeo. Lo scambio di informazioni in siffatte occasioni rientra, nondimeno, nel novero degli strumenti predisposti in seno all'Unione europea al fine di rafforzare la cooperazione degli Stati membri, essendo oggetto di previsione specifica dell'Azione comune 97/339/GAI[30] e, successivamente, della Risoluzione del Consiglio adottata in data 29 aprile 2004[31] in relazione alla sicurezza delle riunioni del Consiglio europeo e di altri eventi di pari risonanza.

Il quadro normativo regolante il procedimento di trasmissione di informazioni contempla, in tal caso, due fattispecie procedurali che si differenziano in relazione al menzionato carattere personale o meno del dato oggetto di scambio[32].

---

30 L'Azione comune 97/339/GAI del 26 maggio 1997 è stata adottata dal Consiglio in base all'art. K.3 del Trattato UE in materia di cooperazione nel settore dell'ordine pubblico e della pubblica sicurezza, ed è pubblicata in *GUUE*, L 147, 5 giugno 1997, p. 1.

31 In *GUUE*, C 116, 20 aprile 2004, p. 18. Sul punto, si veda anche l'iniziativa del Regno dei Paesi Bassi in vista dell'adozione della Decisione del Consiglio concernente il rafforzamento della cooperazione di polizia in occasione di grandi eventi, pubblicata in *GUUE*, C 101, 27 aprile 2005, p. 36.

32 La sopravvenienza dell'atto europeo che fa proprio il contenuto sostanziale del Trattato consente di superare il nodo interpretativo legato alla definizione di «dato personale», non tanto perché la nozione sarebbe ivi ricavabile, quanto piuttosto per il fatto che utili indicazioni possono essere tratte dalla decisione–quadro del Consiglio 2008/977/GAI sulla protezione dei

In ambedue i *sub*-procedimenti si prevede che gli Stati europei interessati possano procedere allo scambio di informazioni, sia di propria iniziativa che a seguito di richiesta inoltrata da altra Parte contraente, con atto motivato che faccia menzione dello specifico evento. La trasmissione, sia spontanea che a richiesta, avviene per mezzo di punti di contatto nazionali designati *ad hoc* all'atto del deposito degli strumenti di ratifica (art. 15) e nel rispetto della legislazione nazionale dello Stato membro che li trasmette.

Comune ad entrambi è, peraltro, lo scopo della trasmissione, da identificarsi, come si è premesso, nella prevenzione di reati e nel mantenimento dell'ordine e della sicurezza pubblica in occasione dei già segnalati avvenimenti di natura transnazionale.

Parrebbero, invece, finalizzati a garantire un maggior grado di tutela dei dati a carattere personale gli elementi di differenziazione delle due fattispecie: così, da un lato, l'art. 14 prevede che la trasmissione, spontanea o a richiesta, dei dati a carattere personale debba trovare fondamento in una presunzione di pericolosità della persona interessata.

Sotto tale aspetto, deve segnalarsi che tale giudizio prognostico è ancorato a criteri non soddisfacenti quanto a determinatezza della fattispecie: la norma opera, infatti, un generico riferimento a «condanne definitive o altre circostanze facciano presupporre che le persone interessate commetteranno reati» – non meglio identificati – «in occasione di questi eventi o che costituiranno una minaccia per l'ordine e la sicurezza pubblici», rimettendo, dunque, alla totale discrezionalità dell'autorità competente la valutazione in ordine alla sua ricorrenza.

Dall'altro lato, si prevede un limite all'utilizzo e alla conservazione dei dati personali: le informazioni ottenute possono essere impiegate "esclusivamente" ai fini della prevenzione dei reati e del mantenimento dell'ordine pubblico, e solo nell'ambito dell'evento menzionato nell'atto di trasmissione. Non appena la conservazione del dato appare, dunque, infruttuosa perché l'obiettivo è stato raggiunto o non può più esserlo, i dati dovranno essere cancellati immediatamente. In ogni caso, l'art. 14, par. 2, prevede, con apposita norma di chiusura, che l'informazione non possa essere conservata per più di un anno.

Anche lo strumento della trasmissione di informazioni ai fini della prevenzione di attacchi terroristici – regolato all'art. 16 – costituisce parte integrante dell'*aquis* UE in quanto contemplata dalla decisione n. 2003/48/GAI del Consiglio della UE[33], sostituita dalla successiva decisione n. 2005/671/GAI adottata dal Consiglio il 20 settembre 2005 in relazione al rafforzamento della cooperazione investigativa nel settore dei reati di terrorismo[34].

---

dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. L'art. 2 del testo precisa, infatti, che per dato personale deve intendersi «qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata») [...]».

33 Pubblicata in *GUUE*, L 16, 22 gennaio 2003, p. 68.

34 Pubblicata in *GUUE*, L 253, 29 settembre 2005, p. 22. In merito, si veda, G. De Amicis,

L'art. 16 configura, invero, una facoltà, e non un obbligo, in capo ai singoli Stati di procedere allo scambio di dati personali e altre informazioni al fine di prevenire attacchi terroristici.

La disposizione contempla alcune norme di interpretazione autentica al fine di determinare il suo corretto ambito di applicazione: così, i reati di terrorismo, in relazione ai quali è prevista la facoltà di scambio di dati, si individuano sulla base della tipologia delle figure criminose elencate dagli artt. 1-3 della decisione quadro 2002/475/GAI adottata dal Consiglio dell'Unione il 13 giugno 2002 in relazione alla lotta contro il terrorismo[35]; inoltre, la trasmissione può avere ad oggetto dati personali, cioè le informazioni concernenti una persona fisica identificata o identificabile, comprensivi, ai sensi del par. 2 dell'art. 16, del nome, cognome, data e luogo di nascita e di una descrizione dei fatti che giustificano la presunzione di pericolosità posta alla base dell'inoltro.

Quanto ai profili procedurali, l'invio a fini preventivi può avvenire in relazione a casi concreti e quando vi siano «particolari circostanze» idonee a fondare una presunzione di pericolosità del soggetto interessato in relazione alla commissione dei reati *de quibus*[36]. Anche in tal caso, la norma in esame non fornisce alcun chiarimento sul punto, ma si limita ad ancorarne l'operatività alla sussistenza di specifiche circostanze e in relazione a casi concreti, per cui sarà l'autorità di *intelligence* ad operare un giudizio di prognosi a fronte di parametri del tutto insoddisfacenti sia dal punto di vista della tassatività, quanto della determinatezza.

5. Diritto alla sicurezza *vs* diritto alla riservatezza

Nella prospettiva volta alla realizzazione di «uno spazio comune di giustizia» attraverso il rafforzamento della cooperazione giudiziaria e di polizia, il Programma dell'Aia e il rispettivo Piano di attuazione focalizzano l'attenzione su due punti nevralgici destinati a condizionare le successive iniziative *in subiecta materia*: da un lato, il principio di disponibilità diviene criterio-guida della disciplina della trasmissione di informazioni tra le autorità di *intelligence* e giudiziarie degli Stati membri, dall'altro lato, la previsione di un sistema operativo che consenta l'accesso reciproco e diretto dei singoli Stati ai *databases* nazionali viene ancorata alla indispensabile predisposizione di adeguate garanzie per la tutela delle notizie a carattere personale.

Cooperazione giudiziaria e corruzione internazionale, cit., p. 288.

35 Pubblicata in *GUUE*, L 164, 22 giugno 2002, p. 3.

36 Si tratta di una trasmissione con finalità di prevenzione, differenziandosi, quindi, quanto ad ambito di applicazione, dalla decisione n. 671 del 2005 che prevede la trasmissione di informazioni ai fini investigativi.

La necessità di operare un bilanciamento tra cooperazione informativa e tutela del dato, in un'ottica di superamento della tradizionale contrapposizione tra esigenze di sicurezza e garanzie individuali, trova accoglimento, all'interno dell'Unione europea, inizialmente, nella predisposizione di due coeve proposte di decisione quadro del 2005, di cui una volta ad attuare il principio di disponibilità e l'altra, quale indispensabile *pendant*, afferente alla materia del trattamento delle informazioni personali[37]. Per lungo tempo sono state disattese le sollecitazioni volte ad accelerare l'attuazione della seconda proposta in via prioritaria rispetto agli strumenti deputati a regolare lo scambio di informazioni nell'ottica della disponibilità[38], creando una disciplina poco organica in seno al perimetro del cd. terzo pilastro[39].

Va, dunque, apprezzata l'adozione della decisione quadro 2008/977/GAI[40], diretta alla regolamentazione e protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, che sembrerebbe poter fornire qualche preziosa indicazione circa il regime da applicarsi anche ai dati in esame, benché debba evidenziarsi la sua natura puramente residuale in quanto il considerando n. 39 della decisione quadro precisa che «questa dovrebbe lasciare impregiudicata la pertinente serie di disposizioni sulla protezione dei dati» degli atti adottati a norma del titolo VI del trattato sull'Unione europea, che contengono norme specifiche riguardanti la protezione dei dati, fra cui le disposizioni di protezione dei dati che disciplinano il trasferimento automatizzato tra Stati membri di profili DNA, dati dattiloscopici e dati nazionali di immatricolazione dei veicoli.

Per tale via, *iuxta* l'impostazione adottata dal Consiglio, tuttavia, la protezione del dato personale, nella duplice dimensione di diritto soggettivo dell'interessato all'autodeterminazione informativa e alla riservatezza, da un lato, e di strumento di tutela oggettiva che consenta il controllo sulla genuinità del dato, dall'altro

---

37 V. *supra*, S. Ciampi, *op. cit.*, § 4-5.

38 Nel *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (COM (2005) 475 def.)*, 19 dicembre 2005, in *GUUE*, C 47, 25 febbraio 2006, p. 27, si era sottolineata la necessità che l'entrata in vigore dell'iniziativa *de qua* precedesse l'adozione delle decisioni relative allo scambio di informazioni e *intelligence* tra gli Stati membri.

39 In particolare, non si applicano al "terzo pilastro" la direttiva 95/46/CE e il Regolamento (CE) n. 45/2001, recanti i principi fondamentali in materia di tutela dei dati. Di conseguenza, i sistemi informativi operanti nel settore della cooperazione giudiziaria di polizia, non potendosi richiamare ad un quadro giuridico unitario in materia di protezione dei dati, risultano vincolanti esclusivamente agli atti esplicitamente richiamati. Così, la Convenzione di applicazione Schengen contiene un rinvio espresso, a tutela dei dati gravitanti all'interno del SIS (Sistema Informativo Schengen), ai principi stabiliti dalla Convenzione del Consiglio d'Europa n. 108/1981 e dalla Raccomandazione R 15(87); analogo richiamo è contenuto nella Convenzione istitutiva Europol. Per ulteriori considerazioni si rinvia a F. Decli - G. Marando, *op. cit.*

40 In *GUUE*, L 350, 30 dicembre 2008, p. 60.

lato, si candida ad assumere il ruolo primario di condizione necessaria all'attuazione del principio di disponibilità.

In ambito europeo, la decisione 2008/615/GAI, fa proprio, dunque, il disegno di reciproca compenetrazione tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati affiorante dal Piano di attuazione del Programma dell'Aia.

Le disposizioni inerenti alla protezione delle informazioni personali sono contenute, infatti, in un coacervo di norme (artt. 24 sg.) che trova collocazione successiva rispetto a tutte le fattispecie regolanti la trasmissione di dati contemplati dal provvedimento. La scelta di ordine sistematico conferma la conclusione, già ricavabile, fra l'altro, sul piano dell'esegesi interpretativa, secondo cui le norme in tema di tutela dei dati personali parrebbero applicabili a tutti gli scambi di informazioni, sia spontanei che a richiesta, normativamente previsti dalla decisione e, nell'ambito peculiare della trasmissione dei dati DNA, ad entrambe le fasi del sistema del doppio binario informativo disciplinato dagli artt. 2 sgg.[41].

In particolare, l'art. 25 si propone di assicurare l'osservanza del *corpus* normativo di tutela della riservatezza subordinando l'applicabilità dei meccanismi di scambio di informazioni a due condizioni cumulative: per un verso, si richiede che le legislazioni degli Stati membri rispettino gli *standard* di garanzia offerti dalle fonti di diritto internazionale vigenti in materia, e segnatamente la Convenzione del Consiglio d'Europa del 28 gennaio 1981 ed il relativo Protocollo addizionale dell'8 novembre 2001, nonché la Raccomandazione n° R (87) 15 del Comitato dei Ministri del Consiglio d'Europa; per altro verso, nell'ottica della disponibilità, condizione di legittimità dello scambio di informazioni è che i Paesi membri abbiano dato attuazione interna al complesso di norme sulla protezione dei dati contenute nel Capo VI della decisione, assegnando, così, una posizione prioritaria alle disposizioni concernenti la tutela della privacy rispetto all'attuazione dello scambio di informazioni, garantendone, parimenti, l'effettività[42].

Il quadro normativo di protezione del dato si sviluppa in due direzioni complementari.

---

41 Qualche dubbio si sarebbe potuto profilare in relazione alla trasmissione dell'indice di riferimento in esito alla prima fase del doppio binario. Tuttavia, qualora si accolga la nozione di «dato personale» fornita dalla direttiva 95/46/CE, recepita anche dall'art. 2 della proposta di decisione–quadro del Consiglio del 4 ottobre 2005, ai sensi della quale per dato personale si intende «qualsiasi informazione concernente una persona fisica identificata o identificabile [...]», diviene inevitabile concludere per la classificazione dell'indice di riferimento nell'alveo dei dati a carattere personale.

42 In base all'art. 25, par. 2, il rispetto delle condizioni *de quibus* è verificato dal Consiglio che decide all'unanimità. Va ricordato, peraltro, come il par. 3 preveda una deroga per gli Stati membri in cui la trasmissione di dati personali sia già stata avviata a norma del Trattato del 27 maggio 2005 fra il Regno di Belgio, la Repubblica Federale di Germania, il Regno di Spagna, la Repubblica Francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria.

Il primo profilo attiene alla tutela dell'autodeterminazione informativa – sia dello Stato che detiene il dato sia della persona fisica interessata – al fine di rendere possibile il controllo sulle fasi di trasmissione e utilizzo dell'informazione e garantirne, per questa via, la genuinità e l'attualità. Su tale versante, viene in gioco la dimensione oggettiva della protezione della qualità dell'elemento oggetto di scambio, nella raggiunta consapevolezza che la disponibilità on-line degli archivi nazionali potrà realizzare tanto più un effettivo rafforzamento della cooperazione di polizia quanto più i dati in essi contenuti siano veritieri e controllabili.

Così, si prevede che le informazioni possano venir impiegate solo per gli scopi per cui sono state trasmesse (art. 26) e solo dall'autorità, dagli organi e dai tribunali competenti a procedere per realizzare le finalità per le quali le informazioni sono rese disponibili (art. 27). Tuttavia, lo Stato membro che gestisce lo schedario può autorizzare il trattamento per scopi diversi o ammettere la comunicazione ad altre autorità, purché il trattamento sia consentito dal diritto interno (art. 26, par. 1). Il rispetto della legislazione nazionale vale, altresì, per il Paese destinatario.

Inoltre, gli Stati membri debbono osservare una serie di obblighi inerenti alla tutela della qualità e alla conservazione del dato.

Sotto tale aspetto, essi devono, in primo luogo, garantire la genuinità del dato sotto il profilo della sua esattezza e attualità (art. 28). Qualora, su segnalazione della persona interessata o d'ufficio, l'informazione dovesse, infatti, rivelarsi inesatta o non più aggiornata, o qualora sia stato trasmesso un dato che non poteva essere reso disponibile, gli Stati membri interessati devono essere informati e sono tenuti a procedere alla sua rettificazione o cancellazione (art. 28, par. 1). Nel caso in cui non sia possibile controllarne l'attendibilità, il dato deve essere contrassegnato[43]. L'apposizione dell'indicatore di validità, che avviene allorché l'esattezza del dato è contestato dalla persona interessata e quando non è possibile stabilire se siano corretti o inesatti, è disciplinato, con rinvio, in base al diritto nazionale del Paese membro. Deve sottolinearsi che l'informazione – ancorché di "dubbia attendibilità" – rimane, comunque, indicizzata, quindi, non limitata nel suo trattamento.

Proprio tale aspetto meriterebbe, forse, una maggiore attenzione da parte del legislatore europeo e quello nazionale, attese le implicazioni derivanti sul soggetto interessato dal lato impiego che le nuove forme di cooperazione e di circolazione consentono.

Peraltro, la sua rimozione potrà avvenire solo previo consenso dell'interessato o su decisione del Tribunale o dell'autorità competente in materia di controllo della protezione dei dati (art. 28, par. 2). Con apposita norma di chiusura, si prevede, poi,

---

43 Giova ricordare che la previsione *de qua* coincide con la "caratterizzazione", contenuta nella decisione quadro n. 977 del 2008, in tema di tutela di dati personali, e definita come il contrassegno dei dati personali memorizzati senza l'obiettivo di limitarne il trattamento in futuro (art. 2): sul punto, si veda, ancora, S. Ciampi, *op. cit.*, § 5.

il dovere dello Stato di provvedere alla cancellazione delle informazioni allorquando esse non risultino più necessarie ai fini per cui sono state richieste o, in ogni caso, allo scadere del termine massimo previsto dal diritto interno (art. 28, par. 3).

La decisione 2008/615/GAI annovera, poi, una nuova tipologia di dati: le informazioni cd. «bloccate», caratterizzate dal fatto che il dato non può essere cancellato, in quanto tale attività pregiudicherebbe gli interessi della persona interessa. Merita osservare come tale tipologia di dati possa, comunque, venir utilizzata e trasmessa, anche se per le sole finalità che ne hanno impedito la cancellazione.

In secondo luogo, gli Stati devono tutelare la protezione e la sicurezza dei dati da ogni forma di distruzione, perdita o divulgazione non autorizzata (art. 29).

In terzo luogo, i Paesi dell'Unione devono garantire un adeguato controllo del percorso di trasmissione, ricezione e utilizzo del dato, sia nei casi in cui il trasferimento venga reso in forma non automatizzata, sia nel caso in cui la consultazione avvenga on-line (art. 30). Nel primo caso, l'invio e la ricezione del dato devono essere documentati con atto che contenga l'indicazione dell'oggetto dell'informazione, della data dell'accesso, del motivo della trasmissione e dell'autorità richiedente. Nel secondo caso, si prevede che l'accesso on-line possa essere effettuato solo dai funzionari dei punti di contatto predisposti *ad hoc* e sia debitamente registrato. La registrazione indica, infatti, il contenuto dell'informazione, la data e l'ora dell'accesso, l'indicazione dell'autorità richiedente e dell'autorità che gestisce i dati. Comune a entrambe le previsioni è la norma di garanzia che stabilisce un onere di registrazione di tali dati sia in capo alla Parte richiedente che in capo alla Parte ricevente, al fine di renderne possibile il successivo controllo riservato alle autorità nazionali competenti in materia di protezione dei dati, sulla sussistenza dei presupposti di legittimità delle trasmissioni. Il procedimento di controllo è, in ogni caso, attivato su domanda della persona interessata o d'ufficio, da parte dell'autorità nazionale competente, sulla base dei *dossier* relativi ai dati oggetto di trasmissione (art. 30, par. 5).

Il secondo profilo della disciplina relativa alla protezione dei dati si propone di garantire il diritto soggettivo della persona interessata alla tutela delle informazioni personali, sia nella prospettiva – di segno positivo – della "autodeterminazione" informativa, assicurando al soggetto la possibilità di controllare la veridicità, l'aggiornamento, la circolazione e l'uso delle informazioni che lo riguardano, sia nella componente – di segno negativo – della riservatezza, prescrivendo l'esclusione di alcuni dati dalla categoria delle informazioni accessibili e assicurando il riconoscimento del cd. diritto alla cancellazione del dato[44].

---

44 I due aspetti fondamentali compresi nell'alveo del diritto alla protezione dei dati personali sono evidenziati, fra gli altri, da: A. Baldassarre, "Diritti inviolabili", in *Enciclopedia Giuridica Treccani*, XI, Roma, Istituto dell'Enciclopedia Italiana, 1989, p. 20; S. Rodotà, "Tecnologie dell'informazione e frontiere del sistema socio-politico", in *Banche dati, telematica e diritti della persona*, a cura di G. Alpa e M. Bessone, Padova, Cedam, 1984, p. 93; *adde*, più di recente, C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un diritto comune europeo*, in "Diritto penale e processo", 2007, p. 385.

Così, l'art. 31 della decisione stila un catalogo di diritti di informativa e di impulso all'autorità competente, che si aggiungono alla facoltà del soggetto, prevista dall'art. 28, di richiedere allo Stato di verificare la correttezza e l'aggiornamento dei dati oggetto di trasmissione, al fine di operarne la rettifica, la cancellazione o l'apposizione del contrassegno, nonché alla possibilità di adire, ai sensi dell'art. 39, l'autorità nazionale al fine di attivare il procedimento di controllo sulla legittimità delle trasmissioni.

In particolare, l'art. 31 garantisce alla persona coinvolta specifici diritti di conoscenza riguardo le notizie a lui relative, sulla loro origine, i destinatari, la base giuridica e proclama *expressis verbis* il diritto di ottenere la rettifica e la correzione dei dati errati o trattati illecitamente. In caso di violazione dei diritti di protezione, il soggetto interessato potrà adire congiuntamente un Tribunale indipendente e imparziale, come previsto dall'art. 6 Convenzione europea dei diritti dell'uomo, e un'autorità indipendente di controllo ai sensi dell'art. 28 della direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché la loro libera circolazione, e potrà ottenere una riparazione in forma specifica o un risarcimento per equivalente. La procedura viene regolata con rinvio al diritto nazionale.

Ad una prima analisi, la disciplina sulla tutela dei dati trasmessi nel quadro dello scambio fra gli Stati dell'Unione fin qui analizzata non sembrerebbe pienamente conforme ai parametri regolanti lo scambio di informazioni richiamati dall'art. 34, par. 1, del Trattato dell'Unione[45] e, più in generale, dei diritti fondamentali previsti dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, la regola in base alla quale il dato può essere trasmesso solo per uno scopo determinato (cd. il principio di finalità del trattamento[46]) stabilita all'art. 26 parrebbe trovare un'attuazione solo parziale non appena si ponga mente al fatto che, a tale proclamazione formale, segue la previsione, nel secondo periodo del primo paragrafo, della sua derogabilità da parte del legislatore interno, senza, peraltro, che l'operatività della deroga venga circoscritta a casi e modi tassativi. Come si comprende, dunque, la discrezionalità degli Stati, seppur vincolata al requisito dell'autorizzazione da parte dello Stato emittente e al rispetto della legislazione dello Stato ricevente, consente che la "circolarità" del dato, in quanto del tutto discrezionale, venga, di fatto, lasciata sostanzialmente intatta.

Inoltre, il testo del 23 giugno 2008 dedica, *sub* art. 28, un'ampia previsione normativa al tema della tutela della genuinità del dato, ma la qualità dell'infor-

---

45 Anche l'art. 34 del Trattato vincola gli Stati aderenti ad assicurare un livello di protezione dei dati che corrisponda a quello previsto dalla Convenzione del Consiglio d'Europa n. 108 del 1981, dal Protocollo dell'8 novembre 2001 e dalla Raccomandazione del Comitato dei ministri del Consiglio d'Europa n. R (87) 15.

46 Sul principio di scopo quale criterio guida cui deve informarsi il trattamento dei dati personali, si vedano, fra gli altri, i contributi di C. Fanuele, *op. cit.*, p. 392; P. Felicioni, *Accertamenti sulla persona e processo penale*, Milano, Ipsoa, 2007, p. 184.

mazione viene misurata esclusivamente in rapporto ai parametri della esattezza e dell'aggiornamento, senza che vengano menzionate le caratteristiche dell'adeguatezza, pertinenza e non eccessività, espressamente considerate, invece, dalla Convenzione n. 108 del 1981. La medesima disposizione prevede, inoltre, un sistema di controllo, da effettuarsi solo *ex post*, sulla correttezza e l'aggiornamento del dato trasmesso, con esclusione di qualsiasi previsione volta a consentire una verifica in via preventiva circa la sussistenza dei presupposti di legittimità della trasmissione che avrebbe consentito di realizzare un maggior grado di tutela dell'informazione di carattere personale e sensibile.

6. Le prospettive legislative dell'Italia

Volgendo lo sguardo alle modalità di attivazione dei meccanismi fin qui illustrati ed al compendio di norme di cui il nostro Paese dispone, si constata come in Italia non esiste ancora una (ufficiale) banca dati di analisi del DNA.

L'unica struttura simile a quella richiesta per il test del DNA è legata all'identificazione mediante l'impronta digitale, per cui le autorità italiane muovendosi sulla linea prospettica imposta dal Trattato, e sulla scorta degli approdi maturati in seno ai precedenti progetti legislativi miranti all'istituzione di una banca dati nazionale[47], nel luglio del 2008 hanno depositato al Senato il disegno di legge n. 905[48], volto a consentire l'adesione dello Stato italiano al Trattato.

Premesso che l'avvenuta emanazione della decisione 2008/615/GAI, rende più pressante provvedere, per questa via, alla creazione e alla conservazione di archivi nazionali on-line destinati a confluire in un unico *network* di banche dati direttamente consultabile dalle autorità interne degli Stati membri, non pare inopportuno esaminare – sommariamente e limitatamente agli aspetti contemplati nel presente lavoro[49] – il citato disegno di legge[50].

---

47 Tra i progetti legislativi particolare attenzione merita la Proposta di schema di disegno di legge recante "Norme per la istituzione dell'archivio centrale dei profili del DNA e del Comitato tecnico-scientifico di vigilanza", approvato dal Comitato Nazionale per la Biotecnologia e la Biosicurezza (CNBB) il 14 aprile 2005, pubblicato in P. Felicioni, *op. cit.*, pp. 219 sgg.

48 Il testo della proposta, presentata dai Ministri degli affari esteri, dell'interno e della giustizia, è consultabile all'indirizzo <http://www.senato.it/loc/link.asp?tipodoc=DDLPRES&leg=16&id=307774>.

49 Per un commento alle modifiche al codice di rito, cfr., anche per le più ampie indicazioni bibliografiche, C. Fanuele, *op. cit.*, p. 390; P. Felicioni, *op. cit.*, pp. 207 sgg; A. Santosuosso-G. Gennari, *Il prelievo coattivo di campioni biologici e i terzi*, in "Diritto penale e processo", 2007, pp. 395 sgg.

50 L'art. 36 della decisione 2008/615/GAI prevede (al par. 1) che «gli Stati membri adottano le misure necessarie per conformarsi alle disposizioni della presente decisione entro un anno dalla decorrenza degli effetti della presente decisione, fatta eccezione per le disposizioni del capo 2, per le quali le relative misure necessarie sono adottate entro tre anni dalla decorrenza degli effetti della presente decisione e della decisione del Consiglio relativa all'attuazione della

Tralasciando il Capo I, relativo alle disposizioni di autorizzazione all'adesione al Trattato, il Capo II focalizza l'attenzione sulla necessità di istituire un archivio genetico nazionale al fine di garantire alle autorità di *law enforcement* l'accesso diretto on-line ai dati in esso registrati, e, per tale via, di realizzare la condivisione delle informazioni (cd. *information sharing*) quale necessario presupposto di una più efficace cooperazione di polizia e giudiziaria, anche interna.

In particolare, sotto tale aspetto, viene prevista, su un primo versante, la creazione di due organismi paralleli all'interno dei quali si articolano e si suddividono le attività di trattamento dei dati genetici: in particolare, l'art. 5, comma 1, del disegno di legge istituisce la banca dati nazionale DNA, a carattere interforze, presso il Dipartimento della pubblica sicurezza del Ministero dell'Interno, mentre il successivo comma 2 prevede la creazione del Laboratorio centrale della banca dati DNA in seno al Dipartimento dell'amministrazione penitenziaria, presso il Ministero della giustizia.

La previsione di due strutture operative eterogenee consente di tenere distinte le attività di raccolta e comparazione dei profili DNA, riservate alla banca dati (art. 7), dalle operazioni di estrazione dei profili e di conservazione dei campioni biologici, di competenza esclusiva del Laboratorio (art. 8). La condivisibile scelta di operare un *distinguo* tra la sede delle attività di estrazione dei profili DNA dai campioni biologici, da un lato, e il luogo di raccolta e raffronto dei dati, dall'altro lato, risponde alla finalità di tutelare la genuinità dei dati raccolti e di evitare contaminazioni tra le diverse *species* di informazioni trattate.

In linea con le indicazioni precedentemente formulate, l'analisi dei campioni genetici, quale attività necessariamente prodromica rispetto alla registrazione dei profili all'interno della banca dati ai fini consultivi, deve essere condotta nel rispetto delle garanzie di cui all'art. 11, comma 3: la norma prevede che l'attività di analisi ed estrazione del profilo, da effettuarsi unicamente nei laboratori certificati, possa essere svolta esclusivamente sui segmenti non codificanti del genoma umano, da cui non siano, pertanto, desumibili informazioni sul soggetto analizzato, quali, ad esempio, le patologie genetiche e le caratteristiche ereditarie.

La medesima *ratio* di garanzia informa la disciplina della successiva attività di consultazione della banca dati. Disciplinata all'art. 12, comma 1, la regola del trattamento dei dati, l'accesso e la tracciabilità dei campioni è informata al principio del doppio binario informativo, vale a dire dell'accesso di "secondo livello".

All'evidente fine di garantire che l'accesso all'archivio on-line non consenta di pervenire direttamente ai dati identificativi della persona interessata, ma solo ai dati di indice relativi alla sussistenza del profilo all'interno della banca dati, si dispone *expressis verbis* che i profili DNA ed i relativi campioni non permettono

---

presente decisione». La deroga si riferisce, appunto, alle norme che disciplinano l'«accesso in linea e seguito delle richieste» relative ai profili del DNA, dato dattiloscopici, dati di immatricolazione dei veicoli.

l'identificazione diretta del soggetto cui si riferiscono, nel pieno rispetto dell'art. 2 del Trattato, inerente al carattere anonimo dei profili inseriti all'interno della banca dati.

In pratica, la polizia giudiziaria ovvero l'autorità giudiziaria dovranno prima richiedere di effettuare il confronto e, solo se questo è positivo, potranno essere autorizzati a conoscere il nominativo del soggetto cui appartiene il profilo, garantendo, parallelamente, le esigenze di tutela e privacy, che anche la decisione europea intende soddisfare, e la fruizione delle informazioni.

Su un altro versante, il disegno di legge si preoccupa di fornire una risposta alle questioni esegetiche che riguardano l'individuazione dei soggetti deputati ad attingere alle informazioni contenute all'interno degli archivi.

In particolare, premesso che la trasmissione delle informazioni avverrà per il tramite dei punti di contatto nazionali, l'art. 12, comma 2, del testo identifica le autorità autorizzate a compulsare la banca dati, di cui si prevede la costante tracciabilità, stabilendo, fra l'altro, che le richieste potranno pervenire unicamente dalle Forze di polizia, dall' autorità giudiziaria – da intendersi, in ragione della natura dell'attività, comprensiva tanto del pubblico ministero quanto del giudice – e, nei limiti della legislazione, dai difensori (artt. 391-*bis* sgg. c.p.p.), mentre l'accesso al laboratorio, in ragione della maggiore delicatezza delle attività svolte, è consentito alla polizia giudiziaria solo previa autorizzazione del magistrato. In entrambi i casi, la consultazione avviene esclusivamente per finalità di identificazione personale nonché per finalità di collaborazione internazionale di polizia. La precisazione consente, pertanto, di riferire tali operazioni all'ambito delle attività preprocedimentali di polizia e procedimentali in senso stretto.

Un secondo profilo concerne gli elementi di alimentazione della banca dati: come premesso, il punto non è stato direttamente affrontato dalla decisione 2008/615/GAI, che si limita a distinguere i profili riferibili ad un soggetto determinato dalle cd. tracce aperte, ovvero insuscettibili di identificazione, nulla disponendo in merito alle modalità di raccolta ed estrazione degli stessi. A tal proposito, il disegno di legge stila, invece, un catalogo di fonti, da cui è possibile ricavare il materiale biologico ai fini della tipizzazione dei relativi profili DNA e del loro inserimento negli archivi, in relazione a ciascuna delle quali sono stabilite specifiche modalità di acquisizione procedimentale.

In primo luogo, è prevista la possibilità di prelevare i campioni biologici da determinate categorie di soggetti, selezionati in base al denominatore comune di essere stati sottoposti a misure privative della libertà personale. Il potere di comprimere la libertà di soggetti indiziati o imputati nel corso del procedimento penale si dilaterebbe fino a comprendere, nell'ottica del legislatore, la facoltà del prelievo coattivo del campione biologico[51]. In particolare, ai sensi dell'art. 9, com-

51 Tuttavia, come sottolineato anche dal Garante europeo per la protezione dei dati, il prelievo di sostanze biologiche è misura di maggiore afflittività rispetto alle altre limitazioni della

ma 2, del disegno di legge, possono essere sottoposti al prelievo, volontario o coattivo, di sostanze biologiche i soggetti sottoposti a misure cautelari, precautelari e a misure di sicurezza detentive, e i soggetti cui sia stata applicata la detenzione, l'internamento, o una misura alternativa della detenzione a seguito di sentenza irrevocabile di condanna per un delitto non colposo.

A giustificare tale soluzione induce la considerazione, peraltro, poco conforme al sistema, che lo stato di restrizione più ampio – quello della libertà – dovrebbe comportare quella minore, che consiste nel prelievo coattivo del piccolo saggio di saliva.

Alcune limitazioni sono previste, tuttavia, in base alle categorie di reato per cui si procede. In ogni caso, deve trattarsi di procedimenti per delitti non colposi, per i quali sia consentito l'arresto in flagranza, con esclusione di un elenco di reati regolato per *nomen iuris* dall'art. 9, comma 2, e che contempla, per sommi capi, i delitti che non contengano tra i loro elementi costitutivi la violenza o la minaccia, i delitti contro la pubblica amministrazione, i delitti di falso, i reati fallimentari.

Una riduzione del potere di prelievo coattivo riconosciuto alla polizia giudiziaria è, poi, previsto dal comma 3, ai sensi del quale, in caso di arresto in flagranza o di fermo, l'estrazione del materiale biologico è consentita solo in seguito alla convalida da parte del giudice. S'introdurrebbe, così, una sorta di "autorizzazione" per lo svolgimento di atti invasivi della libertà personale, per loro natura "postumi".

Il procedimento di acquisizione dei campioni biologici dei soggetti privati della libertà personale trova, infatti, specifica disciplina nei commi 3 e 4 dell'art. 9, in cui si prevede che il prelievo venga effettuato dalle forze di polizia giudiziaria, anche mediante ausiliari, nel rispetto della dignità e della riservatezza del soggetto interessato. I campioni prelevati all'esito delle operazioni, di cui deve essere redatto apposito verbale, devono essere inviati a cura della polizia giudiziaria procedente al laboratorio centrale, per la tipizzazione e il successivo inserimento in banca dati.

In secondo luogo, viene in rilievo la possibilità di estrarre i profili dai reperti biologici, cioè dai materiali acquisiti dalla polizia giudiziaria sul luogo del reato o su cose pertinenti al reato, tipicamente all'esito delle attività di perquisizione o sequestro.

A tal fine, il legislatore, da un lato, pone a carico dell'autorità procedente che abbia richiesto – mediante accertamento tecnico, consulenza o perizia – la tipizzazione dei campioni biologici raccolti, il dovere di disporre la trasmissione dei profili alla banca dati DNA. Tale obbligo, per contro, non riguarda i campioni biologici

---

libertà personale previste dal codice di rito penale. Inoltre, la previsione è di dubbia conformità rispetto al canone di proporzionalità che, *in unum* con il principio di scopo, informa la materia del trattamento dei dati e implica che possano essere sottoposti a prelievo di materiale genetico solo i soggetti imputati o gravemente indiziati di delitti a particolare allarme sociale, quali quelli contro la pubblica incolumità. In merito, si veda, C. Fanuele, *op. cit.*, p. 393; R. E. Kostoris, "Prelievi biologici coattivi", in *Contrasto al terrorismo interno e internazionale*, cit., p. 329.

prelevati in seguito ad attività di ispezioni corporali volontarie o coattive. Dall'altro lato, a seguito del passaggio in giudicato della sentenza, il pubblico ministero legittimato ai sensi dell'art. 655, comma 1, c.p.p. ha la mera facoltà di richiedere al giudice dell'esecuzione di disporre l'attività di tipizzazione e trasmissione dei reperti, che non siano mai stati analizzati nel corso del procedimento (art. 10).

In terzo luogo, è consentito il prelievo di materiale biologico sui cadaveri non attribuiti ad alcuno, al fine di consentirne l'identificazione: in tal caso, il procedimento di acquisizione dei profili ricalca quello delineato per il prelievo dai reperti biologici, in linea con quanto pretende, allo stato dell'arte, la legislazione sovranazionale.

Sul diverso fronte della tutela dei dati, il progetto prevede un *corpus* di norme volte a tutelare sia il profilo positivo del diritto alla privacy, inerente all'autodeterminazione informativa e al controllo sulla circolazione del dato, sia il profilo negativo della riservatezza del soggetto interessato, cui attiene la problematica afferente alla conservazione e alla cancellazione dei dati.

Per quanto attiene al primo profilo, l'art. 12, comma 3, – come si è anticipato – prevede che il trattamento e l'accesso alle informazioni contenute negli archivi possa essere effettuato dal personale a ciò autorizzato, in modo tale da garantire la verifica «costante» del dato, assicurando sia l'identificazione dell'operatore sia la registrazione delle attività concernenti i profili e i campioni, in linea con quanto stabilisce l'art. 30 della decisione 2008/615/GAI che impone la tracciabilità «oggettiva» dell'invio (il motivo della trasmissione; i dati trasmessi; la data della trasmissione) e quella «soggettiva» (la denominazione o il codice di riferimento dell'autorità che effettua la consultazione e dell'autorità che gestisce lo schedario).

Per quanto riguarda l'aspetto legato alla conservazione dei dati, il disegno di legge opera un bilanciamento tra il buon funzionamento della banca dati – la cui efficienza, fisiologicamente collegata al fenomeno della recidiva, dipende dal fatto che quanto più il dato viene conservato in archivio tanto più aumentano le probabilità di identificazione delle tracce aperte – e l'opposta *ratio* di garanzia della riservatezza della persona interessata.

L'art. 13, comma 4, prevede, con apposita norma di chiusura, che i termini massimi di conservazione dei profili DNA e dei relativi campioni, da determinarsi in concreto con apposito regolamento attuativo, non possano superare, rispettivamente, i quaranta e i venti anni dall'ultima circostanza che ne ha determinato l'acquisizione.

Sebbene la scelta temporale regga – come si è anticipato – sul rilievo che le continue evoluzioni delle tecniche di tipizzazione e confronto possono rendere necessaria la sua disponibilità onde effettuare delle nuove analisi ogniqualvolta si rendesse disponibile una innovazione in tal senso, va evidenziato che se il *dies a quo* appare eccessivamente generico, è lecito chiedersi, per quanto attiene il *dies ad quem*, se un termine così ampio possa dirsi conforme al principio di proporzionalità, espresso all'art. 5 della decisione quadro 2008/977/GAI, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di

polizia in materia penale – a mente del quale «sono previsti adeguati termini per la cancellazione dei dati personali o per un esame periodico della necessità della memorizzazione dei dati» – e recepito a livello nazionale dal d.lgs. 30 giugno 2003, n. 196, secondo cui i dati possono essere conservati per il tempo necessario al raggiungimento dello scopo perseguito.

Dovrà provvedersi alla cancellazione in ogni caso, anche d'ufficio, prima della scadenza dei termini massimi, dei profili e dei campioni prelevati dai soggetti *ex* art. 9 a seguito di sentenza definitiva di assoluzione nel merito con formula liberatoria (art. 13, comma 1) e dei profili di cui all'art. 7, lett. *c*), a seguito di ritrovamento di persona scomparsa o di identificazione del cadavere, essendo raggiunto lo scopo a cui tende la loro conservazione.

Parrebbe rispondere, invece, ad una logica sanzionatoria, la cancellazione del profilo DNA e la distruzione del relativo campione stabilita all'art. 13, comma 3, ogniqualvolta risulti che le operazioni di prelievo siano state eseguite in violazione del protocollo indicato all'art. 9.

Gli organi preposti al controllo della banca dati e del laboratorio sono, infine, individuati, rispettivamente, nel Garante per la protezione dei dati, che esercita tale funzione nell'ambito delle attribuzioni previste dal d. lgs. n. 196 del 2003, e nel Comitato nazionale per la biosicurezza e le biotecnologie (art. 15): la scelta normativa merita piena condivisione, trattandosi di due istituzioni capaci di offrire la tutela, la più ampia, d'imparzialità nell'espletamento del ruolo di garanzia circa l'osservanza delle norme di sicurezza, in quanto esse si pongono, fra l'altro, come autonome ed estranee rispetto all'attività di raccolta dei dati prefigurata dal disegno di legge e, quindi, conformi a quanto pretende, sul punto, l'art. 30, par. 4, della decisione GAI n. 615 del 2008.

Nel Capo III del provvedimento italiano si dà, poi, attuazione alle forme di cooperazione di polizia ulteriori e residuali, che impongono la condivisione di informazioni on-line tra gli Stati aderenti all'Unione e che la decisione europea contempla agli artt. 17 e 18, in termini di «operazioni congiunte, assistenza in occasioni di assembramenti, catastrofi e incidenti gravi» per le quali è ammesso «uso di armi, munizioni e attrezzature» (art. 19).

In conclusione, com'è emerso, il testo sommariamente esaminato, salvo piccole discrasie, si pone prevalentemente in linea con il quadro tratteggiato a livello europeo, per cui sembra ormai opportuna ed improrogabile la sua adozione. A sollecitare in tal senso, induce, sul versante interno, la constatazione dell'assoluta rilevanza che i dati in esame paiono acquisire ormai non solo ai fini dell'accertamento giudiziale, ma anche in quanto elementi fondamentali per la stessa instaurazione dei processi.