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

STEFANO CIAMPI
Dottore di ricerca in Scienze penalistiche
Università di Trieste

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

1. Introduzione

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

---

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

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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

---

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

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

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

2. Il Programma dell'Aia

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

19 V. *infra*, § 3 e 5.

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

35 Cfr. § 4.

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

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

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

---

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

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

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

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

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

---

40 V. *amplius infra*, § 5.

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

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

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

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

---

42 Cfr. *infra*, § 5.

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

51 Compendiate nell'apposita Sezione II del Capo III.

52 V. *supra*, § 1.

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

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

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

---

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

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

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

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

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

---

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

57 V. *supra*, § 1.

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

62 Su cui v. *infra*, § 7.

63 Cfr. *infra*, § 8.

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

65 V. *supra*, § 2.

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

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

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

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

---

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

68 Art. 13, par. 2.

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

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

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

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

---

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

71 V. *infra*, § 8.

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

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

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

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

---

72 *Infra*, § 7 segg.

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

79 Artt. da 8 a 18.

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

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

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

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

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

---

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

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

84 Considerando n. 6a.

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

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

85 Considerando n. 18.

86 Considerando n. 20.

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

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

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

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

---

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

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

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

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

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

---

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

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

94 Cfr. l'emendamento n. 60.

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

---

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

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

6. Il percorso di avvicinamento alla "disponibilità informativa"

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

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

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

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

113 V. *infra*, § 9.

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

115 Lo si è visto *supra*, § 4.

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

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

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

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

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

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

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

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

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

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

117 V. *infra*, § 9.

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

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

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

---

118 *Supra*, § 4.

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

120 V. *infra*, § 8.

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

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

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

121 Cfr. *supra*, § 4.

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

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

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

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

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

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

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

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

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

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

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

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

---

126 Emendamento n. 3.

127 Emendamento n. 18.

128 Emendamento n. 19.

129 Emendamento n. 14.

130 Emendamenti nn. 20 e 21.

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

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

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

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

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

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

134 Cfr. *infra* nel testo.

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

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

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

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

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

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

---

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

139 V. *infra*, nel testo.

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

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

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

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

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

---

141 Cfr. agli artt. 5 e 10.

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

165 V. *supra*, § 4.

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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

10. Riflessioni conclusive

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

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

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

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

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

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

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

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

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

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

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

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

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

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