La cooperazione informativa quale motore del sistema europeo di sicurezza

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

2. Principio di disponibilità in senso lato e cooperazione informativa

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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