COMMISSIONE EUROPEA

Bruxelles, 20.7.2010

COM(2010)385 definitivo

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia

1. INTRODUZIONE

L'Unione europea ha fatto molta strada da quando, nel 1985 nella località di Schengen, i leader di cinque paesi europei decisero di abolire i controlli alle frontiere comuni. Quell'accordo diede vita, nel 1990, alla convenzione Schengen che conteneva in nuce molte delle politiche odierne di gestione delle informazioni. L'abolizione dei controlli alle frontiere interne ha spronato lo sviluppo di tutta una serie di misure alle frontiere esterne, soprattutto per quanto riguarda il rilascio dei visti, il coordinamento delle politiche di asilo e di immigrazione e il rafforzamento della cooperazione di polizia, giudiziaria e doganale nella lotta alla criminalità transnazionale. Né lo spazio Schengen né il mercato interno potrebbero funzionare oggi senza lo scambio transfrontaliero di dati.

Gli attentati terroristici del 2001 negli Stati Uniti e del 2004 e 2005 a Madrid e Londra hanno dato il via a una nuova dinamica nello sviluppo delle politiche europee di gestione delle informazioni. Nel 2006 il Consiglio e il Parlamento europeo hanno adottato la direttiva sulla conservazione dei dati che permette alle autorità nazionali di contrastare le forme gravi di criminalità conservando i dati di telecomunicazione relativi al traffico e all'ubicazione[1]. Il Consiglio ha poi fatto propria l'iniziativa svedese che semplifica lo scambio transfrontaliero di informazioni nelle indagini penali e nelle operazioni di intelligence e nel 2008 ha approvato la decisione di Prüm per accelerare lo scambio di profili DNA, impronte digitali e dati di immatricolazione dei veicoli nella lotta al terrorismo e ad altre forme di criminalità. La cooperazione transfrontaliera tra unità di informazione finanziaria e tra uffici per il recupero dei beni, le piattaforme in materia di criminalità informatica e il ricorso a Europol ed Eurojust da parte degli Stati membri costituiscono altri strumenti di lotta contro le forme gravi di criminalità nello spazio Schengen.

All'indomani degli attentati terroristici dell'11 settembre 2001 il governo degli Stati Uniti ha istituito il programma di controllo delle transazioni finanziarie dei terroristi (TFTP) per sventare attacchi analoghi monitorando le transazioni finanziarie sospette. Il Parlamento europeo ha di recente approvato la conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni

[1] Non esiste una definizione armonizzata di "reato grave". La decisione del Consiglio che autorizza Europol a consultare il VIS (decisione 2008/633/GAI del Consiglio, GU L 218 del 13.8.2008, pag. 129) nel definire i "reati gravi" fa riferimento all'elenco di reati di cui al mandato di arresto europeo (decisione 2002/584/GAI del Consiglio, GU L 190 del 18.7.2002, pag. 1). La direttiva sulla conservazione dei dati (direttiva 2006/24/CE, GU L 105 del 13.4.2006, pag. 54) lascia agli Stati membri il compito di definire i "reati gravi". La decisione Europol (decisione 2009/371/GAI del Consiglio, GU L 121 del 15.5.2009, pag. 37) contiene un elenco di reati qualificati come "forme gravi di criminalità" che è molto simile, ma non identico, all'elenco di cui alla decisione sul mandato d'arresto europeo.

finanziarie dei terroristi (accordo TFTP UE-USA)[2]. Anche lo scambio dei dati del codice di prenotazione (*Passenger Name Records* – PNR) con i paesi terzi ha aiutato l'UE a combattere il terrorismo e altre forme gravi di criminalità[3]. Dopo aver concluso accordi PNR con USA, Australia e Canada, la Commissione ha recentemente deciso di rivedere ex novo il suo approccio per l'attuazione di un sistema PNR nell'UE e la condivisione di tali dati con paesi terzi.

Tutte queste misure hanno permesso la libera circolazione nello spazio Schengen, hanno contribuito a prevenire e combattere attentati terroristici e altre forme gravi di criminalità e sostenuto lo sviluppo di una politica comune in materia di visti e asilo.

Con la presente comunicazione per la prima volta vengono illustrate tutte le misure dell'UE, vigenti o in fase di attuazione o di esame, che disciplinano la raccolta, la conservazione o lo scambio transfrontaliero di informazioni personali a fini di contrasto o di gestione dell'immigrazione. I cittadini hanno diritto di sapere quali sono i loro dati personali trattati e scambiati, chi li scambia e per quali finalità. A queste domande risponde, con trasparenza, il presente documento chiarendo, per ciascuno strumento, lo scopo principale, la struttura, il tipo di dati personali che tratta, l'elenco delle autorità che hanno accesso a tali dati e le disposizioni in materia di protezione e conservazione, ma anche facendo qualche esempio del modo in cui tali strumenti funzionano nella pratica (allegato I). Esso fissa poi i principi che devono essere alla base della concezione e della valutazione degli strumenti di gestione delle informazioni nello spazio di libertà, sicurezza e giustizia.

Passando in rassegna le misure a livello dell'UE che disciplinano la gestione delle informazioni personali e proponendo un insieme di principi per svilupparle e valutarle, la presente comunicazione contribuisce a un dialogo politico informato con tutte le parti interessate. e nel contempo dà una prima risposta alle richieste degli Stati membri di mettere a punto un approccio più "coerente" allo scambio di informazioni personali a fini di contrasto – questione trattata di recente dalla strategia di gestione delle informazioni dell'UE[4] – e per riflettere sull'eventualità di sviluppare un modello europeo di scambio delle informazioni basato sulla valutazione degli strumenti attuali[5].

La limitazione delle finalità è un aspetto fondamentale di quasi tutti gli strumenti esaminati nella presente comunicazione. Un sistema di informazione unico e globale a livello UE con finalità multiple consentirebbe la massima condivisione delle informazioni, tuttavia costituirebbe una limitazione grave e illegittima del diritto della persona alla vita privata e alla protezione dei dati e presenterebbe enormi difficoltà in termini di sviluppo e funzionamento. Nella pratica, le politiche nel settore della libertà, della sicurezza e della giustizia sono andate sviluppandosi progressivamente, istituendo una serie di sistemi e strumenti di informazione

---

2 Risoluzione del Parlamento europeo P7_TA-PROV(2010)0279 dell'8.7.2010.

3 Nella lotta contro le forme gravi di criminalità, i "reati terroristici" sono chiaramente definiti dalla decisione quadro del Consiglio sulla lotta contro il terrorismo (decisione quadro 2002/475/GAI del Consiglio, GU L 164 del 22.6.2002, pag. 3), modificata dalla decisione quadro 2008/919/GAI del Consiglio (GU L 330 del 9.12.2008, pag. 21).

4 Conclusioni del Consiglio su una strategia di gestione delle informazioni per la sicurezza interna dell'UE, Consiglio "Giustizia e affari interni" del 30.11.2009 (strategia di gestione delle informazioni dell'UE); "Libertà, sicurezza, vita privata - Affari interni europei in un mondo aperto", relazione del gruppo consultivo informale ad alto livello sul futuro della politica europea in materia di affari interni ("Gruppo del futuro"), giugno 2008.

5 Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini, documento del Consiglio n. 5731/10 del 3.3.2010, punto 4.2.2.

con dimensioni, portata e obiettivi diversi. Una gestione compartimentata delle informazioni come quella delineatasi negli ultimi decenni contribuisce alla tutela del diritto del cittadino al rispetto della vita privata più di qualsiasi alternativa centralizzata.

La presente comunicazione non concerne le misure relative allo scambio di dati non personali a fini strategici, come le analisi dei rischi o le valutazioni delle minacce in generale, né analizza in dettaglio le disposizioni di protezione dei dati contenute negli strumenti esaminati, in quanto la Commissione, in virtù dell'articolo 16 del trattato sul funzionamento dell'Unione europea, sta portando avanti un'iniziativa distinta su un nuovo quadro globale per la protezione dei dati personali nell'UE. Il Consiglio, dal canto suo, sta esaminando il progetto di direttive di negoziato per un accordo tra l'Unione europea e gli Stati Uniti d'America sulla protezione dei dati personali trasferiti e trattati al fine di prevenire, individuare, indagare e reprimere i reati, compreso il terrorismo, nel quadro della cooperazione di polizia e della cooperazione giudiziaria in materia penale. Poiché i negoziati dovrebbero stabilire le modalità in cui le due parti possono assicurare un elevato livello di tutela dei diritti e delle libertà fondamentali nel trasferire e trattare i dati personali, e non il merito dei trasferimenti o trattamenti, la presente comunicazione non prende in considerazione tale iniziativa[6].

2. STRUMENTI DELL'UE CHE DISCIPLINANO LA RACCOLTA, LA CONSERVAZIONE O LO SCAMBIO DI DATI PERSONALI A FINI DI CONTRASTO O DI GESTIONE DELL'IMMIGRAZIONE

Questa sezione passa in rassegna gli strumenti dell'UE che disciplinano la raccolta, la conservazione o lo scambio transfrontaliero di dati personali a fini di contrasto o di gestione dell'immigrazione. La sezione 2.1 riguarda le misure vigenti o in fase di attuazione o di esame, mentre la sezione 2.2 le iniziative fissate dal piano d'azione per l'attuazione del programma di Stoccolma[7]. Per ciascuno strumento sono riportate informazioni sui seguenti aspetti:

– contesto (se la misura è stata proposta dagli Stati membri o dalla Commissione)[8],

– finalità per cui sono raccolti, conservati o scambiati i dati,

– struttura (sistema d'informazione centralizzato o scambio di dati decentrato),

– ambito dei dati personali,

– autorità che hanno accesso ai dati,

– disposizioni di protezione dei dati,

---

6 COM(2010)252 del 26.5.2010.

7 COM(2010) 171 del 20.4.2010 (Piano d'azione per l'attuazione del programma di Stoccolma).

8 Nel quadro dell'ex terzo pilastro dell'Unione europea (cooperazione di polizia e giudiziaria in materia penale), gli Stati membri e la Commissione condividevano il potere di iniziativa. Il trattato di Amsterdam ha integrato i settori riguardanti il controllo alle frontiere esterne, i visti, l'asilo e l'immigrazione nel (primo) pilastro comunitario, in cui la Commissione godeva di diritto di iniziativa esclusivo. Il trattato di Lisbona ha eliminato la struttura a pilastri dell'Unione, riaffermando il diritto di iniziativa della Commissione. Tuttavia, nei settori della cooperazione di polizia e giudiziaria in materia penale (compresa la cooperazione amministrativa) un atto legislativo può essere ancora proposto su iniziativa di un quarto degli Stati membri.

– norme di conservazione dei dati,

– stato di attuazione,

– meccanismo di revisione.

2.1. Strumenti vigenti o in fase di attuazione o di esame

Strumenti dell'UE diretti a migliorare il funzionamento dello spazio Schengen e l'unione doganale

Il Sistema d'informazione Schengen (SIS) nasce dal desiderio degli Stati membri di istituire uno spazio senza controlli alle frontiere interne che faciliti nel contempo l'attraversamento delle frontiere esterne da parte delle persone[9]. Operativo dal 1995, il SIS intende preservare la sicurezza pubblica, compresa la sicurezza dello Stato, all'interno dello spazio Schengen, e facilitare la circolazione delle persone usando informazioni comunicate attraverso il sistema stesso. Il SIS è un sistema d'informazione centralizzato costituito da una sezione nazionale presso ciascuno Stato partecipante e da un'unità di supporto tecnico in Francia. Gli Stati membri possono segnalare persone ricercate per l'arresto ai fini di estradizione; cittadini di paesi terzi ai fini della non ammissione; persone scomparse; testimoni e persone citate a comparire dinanzi all'autorità giudiziaria; persone e veicoli soggetti a monitoraggio straordinario in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato; veicoli, documenti e armi da fuoco persi o rubati; banconote registrate. I dati inseriti nel SIS indicano nomi e alias, segni fisici particolari, data e luogo di nascita, cittadinanza e se l'interessato è armato o violento. Ai dati possono accedere, nell'ambito delle rispettive competenze legali, le autorità di polizia, le autorità di controllo alla frontiera, le autorità doganali e le autorità giudiziarie nei procedimenti penali. Le autorità competenti per l'immigrazione e le autorità consolari possono accedere ai dati relativi ai cittadini di paesi terzi iscritti nell'elenco delle persone soggette a divieto di ingresso e alle segnalazioni sui documenti persi e rubati. Europol ha accesso ad alcune categorie di dati SIS, comprese le segnalazioni relative alle persone ricercate per l'arresto ai fini di estradizione e le segnalazioni relative alle persone soggette a monitoraggio straordinario in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato. Eurojust può accedere alle segnalazioni relative alle persone ricercate per l'arresto ai fini di estradizione e alle segnalazioni relative ai testimoni e alle persone citate a comparire dinanzi all'autorità giudiziaria. I dati personali possono essere usati solo per le finalità delle segnalazioni specifiche per le quali sono stati forniti. I dati personali inseriti nel SIS ai fini della ricerca di persone possono essere conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti, e non oltre tre anni dopo il loro inserimento. I dati sulle persone soggette a monitoraggio straordinario in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato devono essere cancellati dopo un anno. Gli Stati membri devono adottare le disposizioni nazionali necessarie per ottenere un livello di protezione dei dati personali almeno pari a quello derivante dalla convenzione del Consiglio d'Europa del 1981 sulla protezione delle persone nei riguardi del trattamento automatizzato dei dati di natura personale e dalla raccomandazione del 1987 del comitato dei Ministri del Consiglio d'Europa

[9] Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni (GU L 239 del 22.9.2000, pag. 19).

tendente a regolare l'uso dei dati di natura personale nel settore della polizia[10]. La convenzione Schengen non prevede un meccanismo di revisione, tuttavia i firmatari possono proporre di modificarla; in tal caso il testo modificato deve essere approvato all'unanimità e ratificato dai parlamenti nazionali. Il SIS è interamente applicabile in 22 Stati membri e in Svizzera, Norvegia e Islanda. Il Regno Unito e l'Irlanda partecipano agli aspetti della cooperazione di polizia della convenzione Schengen e del SIS, fatta eccezione per le segnalazioni relative ai cittadini di paesi terzi iscritti nell'elenco delle persone soggette a divieto di ingresso. Cipro ha firmato la convenzione Schengen ma non l'ha ancora attuata. Il Liechtenstein dovrebbe attuarla nel 2010 e la Romania e la Bulgaria nel 2011. Le interrogazioni del SIS generano "hit" (segnalazioni positive) quando le indicazioni relative a una persona o a un oggetto corrispondono a quelle di una segnalazione esistente. Ottenuto un "hit", le autorità di contrasto possono chiedere informazioni supplementari sulla persona o sull'oggetto cui si riferisce la segnalazione tramite la rete di uffici SIRENE[11].

Con l'ingresso nello spazio Schengen dei nuovi Stati membri, le dimensioni della banca dati SIS sono aumentate proporzionalmente: tra gennaio 2008 e gennaio 2010 il numero totale di segnalazioni SIS è passato da 22,9 milioni a 31,6 milioni[12]. In previsione di un simile aumento del volume dei dati e di un cambiamento delle esigenze degli utenti, nel 2001 gli Stati membri avevano deciso di sviluppare un **sistema d'informazione Schengen di seconda generazione** (SIS II), affidando l'incarico alla Commissione[13]. Attualmente in fase di sviluppo, il SIS II è diretto ad assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia potenziando le funzioni del sistema di prima generazione, e ad agevolare la circolazione delle persone avvalendosi delle informazioni trasmesse tramite il sistema. Oltre alle originarie categorie di dati del sistema di prima generazione, il SIS II sarà in grado di gestire impronte digitali, fotografie, copie di mandati di arresto europei, le disposizioni per la tutela delle persone la cui identità è stata usurpata e le connessioni tra diverse segnalazioni. Il SIS II sarà in grado, ad esempio, di interconnettere le segnalazioni riguardanti una persona ricercata per sottrazione, la persona sottratta e il veicolo usato per commettere tale reato. Le norme sui diritti di accesso e sulla conservazione dei dati sono identiche rispetto al sistema di prima generazione. I dati personali possono essere usati solo per le finalità delle segnalazioni specifiche per le quali sono stati forniti. I dati personali memorizzati nel SIS II devono essere trattati conformemente alle disposizioni specifiche degli strumenti giuridici di base che disciplinano il sistema (regolamento (CE) n. 1987/2006 e decisione 2007/533/GAI del Consiglio) e che chiariscono i principi della direttiva 95/46/CE e, nel rispetto del regolamento (CE) n. 45/2001, della convenzione del Consiglio d'Europa n. 108 e della raccomandazione nel settore della polizia[14]. Il SIS II si avvarrà della rete s-TESTA, la rete di trasmissione sicura

---

10 Convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

11 SIRENE è l'acronimo di *Supplementary Information Request at National Entry* (Informazioni supplementari richieste all'atto dell'ingresso nel territorio nazionale).

12 Documenti del Consiglio n. 5441/08 del 30.1.2008 e n. 6162/10 del 5.2.2010.

13 Regolamento (CE) n. 1986/2006 (GU L 381 del 28.12.2006, pag. 1); regolamento (CE) n. 1987/2006 (GU L 381 del 28.12.2006, pag. 4); decisione 2007/533/GAI (GU L 205 del 7.8.2007, pag. 63).

14 Regolamento (CE) n. 1987/2006 (GU L 381 del 28.12.2006, pag. 4); decisione 2007/533/GAI (GU L 205 del 7.8.2007, pag. 63); direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31); regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); raccomandazione R (87) 15 del 17 settembre 1987

dei dati della Commissione[15]. Una volta in funzione, il SIS II sarà applicabile tutti gli Stati membri e in Svizzera, Liechtenstein, Norvegia e Islanda[16]. La Commissione è tenuta a presentare ogni due anni al Parlamento europeo e al Consiglio una relazione di avanzamento concernente lo sviluppo del SIS II e la potenziale migrazione dal sistema di prima generazione[17].

Lo sviluppo di **EURODAC** risale all'abolizione delle frontiere interne, quando si sono rese necessarie norme chiare per il trattamento delle domande di asilo. EURODAC è un sistema centralizzato e informatizzato di identificazione delle impronte digitali, in cui sono registrate le impronte digitali di determinati cittadini di paesi terzi. Operativo dal gennaio 2003, ha lo scopo di concorrere alla determinazione dello Stato membro competente per l'esame di una domanda di asilo ai sensi del regolamento Dublino[18]. Alle persone di età non inferiore a 14 anni che chiedono asilo in uno Stato membro e a coloro che sono fermati in relazione all'attraversamento irregolare di una frontiera esterna sono rilevate automaticamente le impronte digitali. Confrontando tali impronte con i dati registrati in EURODAC, le autorità nazionali cercano di determinare il luogo in cui l'interessato può aver presentato domanda di asilo o da cui può aver fatto ingresso per la prima volta nell'Unione europea. Possono inoltre confrontare con i dati registrati in EURODAC le impronte digitali dei cittadini di paesi terzi trovati illegalmente nel loro territorio. Gli Stati membri devono comunicare l'elenco delle autorità che hanno accesso alla banca dati EURODAC, ossia di norma le autorità competenti per l'asilo e l'immigrazione, le guardie di frontiera e la polizia. Gli Stati membri inseriscono i dati pertinenti nella banca dati centrale tramite i punti d'accesso nazionali. I dati personali registrati in EURODAC possono essere usati solo per agevolare l'applicazione del regolamento Dublino; qualunque altro uso è soggetto a sanzioni. Le impronte digitali dei richiedenti asilo sono conservate per 10 anni, mentre quelle dei migranti in situazione irregolare per due anni. I dati riguardanti i richiedenti asilo sono cancellati una volta che l'interessato ha acquistato la cittadinanza di uno Stato membro, e quelli dei migranti in situazione irregolare dopo che l'interessato ha ottenuto un permesso di soggiorno o ha acquistato la cittadinanza di uno Stato membro oppure dopo che ha lasciato il territorio degli Stati membri. Al trattamento dei dati personali ai sensi di questo strumento si applica la direttiva 95/46/CE[19]. EURODAC funziona sulla rete s-TESTA della Commissione ed è applicabile in tutti gli Stati membri e in Svizzera, Norvegia e Islanda. Per quanto riguarda il Liechtenstein, si è in attesa della conclusione di un accordo che ne autorizza la connessione. La Commissione è tenuta a trasmettere annualmente al Parlamento europeo e al Consiglio una relazione sull'attività dell'unità centrale di EURODAC.

---

del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

15 S-TESTA è l'acronimo di *Secure Trans-European Services for Telematics between Administrations* (rete di servizi transeuropei sicuri per la comunicazione telematica tra amministrazioni). È una rete di trasmissione dati finanziata dalla Commissione che consente alle amministrazioni nazionali e alle istituzioni, agenzie e organismi dell'UE di scambiare informazioni in modo sicuro e cifrato.

16 Il Regno Unito e l'Irlanda parteciperanno al SIS II fatta eccezione per le segnalazioni relative ai cittadini di paesi terzi iscritti nell'elenco delle persone soggette a divieto di ingresso.

17 Regolamento (CE) n. 1104/2008 del Consiglio (GU L 299 dell'8.11.2008, pag. 1); decisione 2008/839/GAI del Consiglio (GU L 299 del 08/11/2008, pag. 43).

18 Regolamento (CE) n. 343/2003 (GU L 50 del 25.2.2003, pag. 1) (regolamento Dublino), regolamento (CE) n. 2725/2000 (GU L 316 del 15.12.2000, pag. 1) (regolamento EURODAC). Questi strumenti si basano sulla convenzione di Dublino del 1990 (GU C 254 del 19.8.1997, pag. 1), il cui obiettivo era determinare lo Stato competente per l'esame di una domanda di asilo. Il sistema di esame di una domanda d'asilo prende il nome di "sistema di Dublino".

19 Direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31).

In seguito agli attentati dell'11 settembre 2001 gli Stati membri hanno deciso di accelerare l'attuazione della politica comune in materia di visti creando un sistema per lo scambio di informazioni sui visti per soggiorni di breve durata[20]. Con l'abolizione delle frontiere interne è diventato più facile abusare dei regimi dei visti degli Stati membri. Il **sistema d'informazione visti** (VIS) mira ad affrontare entrambi gli aspetti: il suo scopo è migliorare l'attuazione della politica comune in materia di visti agevolando l'esame delle domande di visto e i controlli ai valichi di frontiera esterni, contribuendo nel contempo a prevenire minacce alla sicurezza interna degli Stati membri[21]. Il VIS è un sistema d'informazione centralizzato costituito da una sezione nazionale presso ciascuno Stato partecipante e da un'unità di supporto tecnico in Francia, che si avvale di un sistema di confronto biometrico per garantire un confronto attendibile delle impronte digitali e verificare l'identità dei titolari del visto alle frontiere esterne. Il VIS contiene dati relativi alle domande di visto, fotografie, impronte digitali, decisioni correlate delle autorità per il visto e collegamenti tra domande connesse. Le autorità per il visto, l'asilo e l'immigrazione e le autorità di controllo alla frontiera hanno accesso alla banca dati VIS per verificare l'identità del titolare del visto e l'autenticità del visto; la polizia ed Europol possono consultarla ai fini della prevenzione e della lotta al terrorismo e ad altre forme gravi di criminalità[22]. I fascicoli relativi alla domanda possono essere conservati per cinque anni. I dati personali memorizzati nel VIS devono essere trattati in conformità delle disposizioni specifiche degli strumenti giuridici che disciplinano il sistema (regolamento (CE) n. 767/2008 e decisione 2008/633/GAI del Consiglio) e che integrano le disposizioni della direttiva 95/46/CE e, nel rispetto del regolamento (CE) n. 45/2001, della decisione quadro 2008/977/GAI del Consiglio, della convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e della raccomandazione nel settore della polizia[23]. Il VIS è applicabile in tutti gli Stati membri (esclusi il Regno Unito e l'Irlanda) e in Svizzera, Norvegia e Islanda e funziona sulla rete s-TESTA della Commissione. Tre anni dopo l'entrata in funzione del VIS, e in seguito ogni quattro anni, la Commissione effettuerà una valutazione del sistema.

Su iniziativa spagnola, nel 2004 il Consiglio ha adottato una direttiva che disciplina la **trasmissione anticipata dei dati relativi alle persone trasportate** (*Advance Passenger Information* – API) da parte dei vettori aerei alle autorità di controllo alla frontiera[24]. La direttiva intende migliorare i controlli alle frontiere e combattere l'immigrazione illegale. Su richiesta, i vettori aerei sono tenuti a comunicare alle autorità di controllo alla frontiera il nome, la data di nascita, la cittadinanza, il punto di imbarco e il valico di frontiera di ingresso

---

20 Consiglio straordinario "Giustizia e affari interni" del 29.9.2001.

21 Decisione 2004/512/GAI del Consiglio (GU L 213 del 15.6.2004, pag. 5); regolamento (CE) n. 767/2008 (GU L 218 del 13/08/2008, pag. 60); decisione 2008/633/GAI del Consiglio (GU L 218 del 13/08/2008, pag. 129). Si veda anche la dichiarazione sulla lotta al terrorismo adottata dal Consiglio europeo il 25 marzo 2004.

22 Decisione 2008/633/GAI del Consiglio (GU L 218 del 13.8.2008, pag. 129).

23 Regolamento (CE) n. 767/2008 (GU L 218 del 13.8.2008, pag. 60); decisione 2008/633/GAI del Consiglio (GU L 218 del 13.8.2008, pag. 129). direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31); regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1); decisione quadro 2008/977/GAI del Consiglio (GU L 350 del 30.12.2008, pag. 60); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181) del Consiglio d'Europa dell'8.11.2001 (protocollo addizionale n. 181); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

24 Direttiva 2004/82/CE del Consiglio (GU L 261 del 6.8.2004, pag. 24).

dei passeggeri che si recano nell'UE da paesi terzi. Di norma i dati personali sono raccolti dalla banda a lettura ottica del passaporto dei passeggeri e trasmessi alle autorità al termine delle procedure di accettazione. Dopo l'arrivo del volo, le autorità e i vettori aerei possono conservare i dati API per 24 ore. Il sistema API opera in modo decentrato tramite la condivisione di informazioni tra operatori privati e autorità pubbliche. La direttiva non consente lo scambio di dati API tra Stati membri; tuttavia, autorità di contrasto diverse dalle guardie di frontiera possono chiederne l'accesso a fini di contrasto. I dati personali possono essere usati solo dalle autorità pubbliche ai fini del controllo alla frontiera e della lotta all'immigrazione illegale, e devono essere trattati in conformità della direttiva 95/46/CE[25]. In vigore in tutta l'UE, questo strumento è usato solo da pochi Stati membri. La Commissione lo riesaminerà nel 2011.

Una parte importante del programma della Commissione del 1992, che ha istituito il mercato interno, riguardava l'abolizione di tutti i controlli e di tutte le formalità per la circolazione delle merci all'interno della Comunità[26]. Aver eliminato tali adempimenti alle frontiere interne ha fatto aumentare il rischio di frodi, rendendo così necessario per gli Stati membri istituire, da un lato, un meccanismo di mutua assistenza amministrativa con l'obiettivo di aiutare a prevenire, ricercare e perseguire le operazioni che sono contrarie alle regolamentazioni doganale o agricola e, dall'altro, una cooperazione doganale per facilitare l'accertamento e il perseguimento delle violazioni delle disposizioni doganali nazionali, in particolare potenziando lo scambio transfrontaliero di informazioni. Fatta salva la competenza dell'UE nell'unione doganale[27], la **convenzione Napoli II** relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali mira a permettere alle amministrazioni doganali di prevenire e accertare le violazioni delle disposizioni doganali nazionali, e aiutarle a perseguire e punire le violazioni delle disposizioni doganali comunitarie e nazionali[28]. Ai sensi di tale strumento, gli uffici di coordinamento centrali chiedono per iscritto assistenza ai loro omologhi negli altri Stati membri nell'ambito di indagini penali concernenti violazioni di disposizioni doganali nazionali e comunitarie. Le unità possono trattare i dati personali soltanto agli scopi della convenzione Napoli II e possono trasmetterli alle autorità doganali nazionali, alle autorità nazionali responsabili delle azioni penali, agli organi giurisdizionali nazionali e, previo consenso dello Stato membro che li ha forniti, ad altre autorità. I dati possono essere conservati soltanto per il periodo necessario agli scopi della loro comunicazione. Lo Stato membro ricevente garantisce un livello di protezione dei dati personali almeno pari a quello previsto dallo Stato membro che li ha forniti; il trattamento di tali dati deve rispettare le disposizioni della direttiva 95/46/CE e della convenzione del Consiglio d'Europa n. 108[29]. La convenzione Napoli II è stata ratificata da tutti gli Stati membri che possono proporre modifiche alla convenzione, nel qual caso il testo modificato deve essere adottato dal Consiglio dei Ministri e ratificato dagli Stati membri.

---

25 Direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31).

26 Regolamento (CEE) n. 2913/92 del Consiglio (GU L 302 del 19.10.1992, pag. 1).

27 Regolamento (CE) n. 515/97 del Consiglio, del 13 marzo 1997, relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola (GU L 82 del 22.3.1997, pag. 1), modificato dal regolamento (CE) n. 766/2008 (GU L 218 del 13.8.2008, pag. 48).

28 Convenzione stabilita in base all'articolo K.3, del trattato sull'Unione europea relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali (GU C 24 del 23.1.1998, pag. 2) (convenzione Napoli II).

29 Direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108).

Integrando la convenzione Napoli II, la convenzione SID usa il **sistema d'informazione doganale** (SID) per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali rendendo più efficace, mediante la rapida diffusione di informazioni, la cooperazione tra le amministrazioni doganali degli Stati membri[30]. Il SID è un sistema di informazione centralizzato gestito dalla Commissione e accessibile tramite terminali situati in ogni Stato membro e presso la Commissione, Europol ed Eurojust. Comprende dati personali raggruppati secondo le seguenti categorie: merci, mezzi di trasporto, imprese, persone e merci e denaro contante bloccati, sequestrati o confiscati. I dati personali consistono in nomi e alias, data e luogo di nascita, cittadinanza, sesso, segni particolari, documenti d'identità, indirizzo, segnalazione che la persona ha già fatto uso di violenza, motivo dell'inclusione dei dati nel SID, azione proposta e numero d'immatricolazione del mezzo di trasporto. Per quanto riguarda le merci e il denaro contante bloccati, sequestrati o confiscati, possono essere inseriti nel SID solo i dati anagrafici e l'indirizzo. Tali informazioni possono essere usate soltanto a fini di osservazione e rendiconto, indagini particolari, controlli specifici o analisi strategica o operativa in relazione a persone sospettate di commettere una violazione delle disposizioni doganali nazionali. Ai dati SID possono accedere le autorità nazionali doganali, tributarie, agricole, sanitarie e di polizia, Europol ed Eurojust[31]. Il trattamento dei dati personali deve rispettare le norme specifiche della convenzione SID e le disposizioni della direttiva 95/46/CE, del regolamento (CE) n. 45/2001, della convenzione del Consiglio d'Europa n. 108 e della raccomandazione nel settore della polizia[32]. I dati personali immessi nel SID possono essere copiati in altri sistemi di trattamento dei dati soltanto ai fini di gestione dei rischi o di analisi operativa e possono essere consultati soltanto dagli analisti designati dagli Stati membri. I dati personali copiati dal SID sono memorizzati soltanto per il periodo necessario al raggiungimento dello scopo per cui sono stati copiati, per un massimo di 10 anni. Il SID istituisce inoltre un **archivio d'identificazione dei fascicoli a fini doganali** (FIDE) per aiutare a prevenire, ricercare e perseguire gravi infrazioni alle leggi nazionali[33]. Il FIDE consente alle autorità nazionali preposte alle indagini doganali, quando istruiscono un fascicolo, d'individuare le altre autorità che possono aver indagato sulle persone o sulle imprese in questione. Tali autorità possono immettere nel FIDE dati provenienti dal fascicolo, quali i dati anagrafici delle persone oggetto d'indagine e la ragione sociale, la denominazione commerciale, il numero di partita IVA e l'indirizzo delle imprese oggetto d'indagine. I dati provenienti da fascicoli in cui non sono state rilevate frodi doganali possono essere conservati per un periodo massimo di tre anni; se invece sono state rilevate frodi doganali i dati possono

---

30 Convenzione elaborata in base all'articolo K.3 del trattato sull'Unione europea sull'uso dell'informatica nel settore doganale (GU C 316 del 27.11.1995, pag. 34), modificata dalla decisione 2009/917/GAI del Consiglio (GU L 323 del 10.12.2009, pag. 20).

31 Dal marzo 2011 Europol e Eurojust potranno consultare il SID ai sensi della decisione 2009/917/GAI del Consiglio (GU L 323 del 10.12.2009, p. 20).

32 Convenzione elaborata in base all'articolo K.3 del trattato sull'Unione europea sull'uso dell'informatica nel settore doganale (GU C 316 del 27.11.1995, pag. 34), modificata dalla decisione 2009/917/GAI del Consiglio (GU L 323 del 10.12.2009, pag. 20); direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31); regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

33 Il FIDE (acronimo di *Fichier d'Identification des Dossiers d'Enquêtes douanières*) si basa sul regolamento (CE) n. 766/2008 del Consiglio e sul protocollo recante modifica, per quanto attiene all'istituzione di un archivio di identificazione dei fascicoli a fini doganali, della convenzione sull'uso dell'informatica nel settore doganale, istituito ai sensi dell'articolo 34 del trattato sull'Unione europea (GU C 139 del 13.6.2003, pag. 1).

essere conservati al massimo sei anni. Qualora l'indagine abbia dato luogo a una condanna o all'applicazione di sanzioni, i dati del fascicolo possono essere conservati per un periodo massimo di 10 anni. Il SID e il FIDE usano la rete comune di comunicazione, l'interfaccia comune di sistema o l'accesso Internet protetto forniti dalla Commissione. La convenzione SID è in vigore in tutti gli Stati membri. La Commissione, in cooperazione con gli Stati membri, presenta al Parlamento europeo e al Consiglio relazioni annuali sul funzionamento del SID.

Strumenti dell'UE diretti a prevenire e combattere il terrorismo e altre forme gravi di criminalità transnazionale.

A seguito degli attentati terroristici di Madrid del marzo 2004 è stata adottata una serie di nuove iniziative a livello dell'UE. Su richiesta del Consiglio europeo, nel 2005 la Commissione ha presentato una proposta di strumento che disciplina lo scambio di informazioni in virtù del principio di disponibilità[34]. Anziché approvare la proposta, nel 2006 il Consiglio ha adottato l'**iniziativa svedese** diretta ad ottimizzare la condivisione tra Stati membri di informazioni e intelligence criminale esistenti che possono essere necessarie ai fini di indagini penali o operazioni di intelligence criminale[35]. L'iniziativa svedese si basa sul principio politico dell'"accesso equivalente", secondo cui le condizioni applicabili allo scambio transfrontaliero di dati non devono essere più severe di quelle che disciplinano l'accesso a livello nazionale. L'iniziativa funziona in modo decentrato e consente alla polizia, alle autorità doganali e altre autorità competenti a indagare sui reati (ad eccezione dei servizi di intelligence - che di norma trattano intelligence di sicurezza nazionale o statale) di condividere informazioni e intelligence criminale con i loro omologhi in tutta l'UE. Gli Stati membri devono designare punti di contatto nazionali incaricati di trattare le richieste urgenti di informazioni. L'iniziativa fissa termini precisi per lo scambio di informazioni e fa obbligo agli Stati membri di compilare formulari per richiedere i dati. Gli Stati membri sono tenuti a rispondere alle richieste di informazioni e intelligence entro otto ore se la richiesta è urgente, entro una settimana se non vi è urgenza e entro due settimane in tutti gli altri casi. L'uso delle informazioni e dell'intelligence ottenute attraverso questo strumento è soggetto alla normativa nazionale sulla protezione dei dati, e gli Stati membri non possono trattare in modo differenziato i dati di produzione nazionale e quelli provenienti da altri Stati membri. Tuttavia, lo Stato membro che trasmette le informazioni o l'intelligence può fissarne le condizioni d'uso negli altri Stati membri. I dati personali devono essere trattati in conformità della normativa nazionale in materia di protezione dei dati, della convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e della raccomandazione nel settore della polizia[36]. 12 dei 31 firmatari (Stati membri dell'UE e Norvegia, Islanda, Svizzera e Liechtenstein) hanno adottato le disposizioni nazionali di attuazione dell'iniziativa; cinque Stati compilano periodicamente il formulario per richiedere informazioni, ma solo due lo

---

34 COM(2005) 490 del 12.10.2005; conclusioni della presidenza – programma dell'Aia del 4-5.11.2004. Si veda anche la dichiarazione sulla lotta al terrorismo adottata dal Consiglio europeo il 25 marzo 2004.

35 Decisione quadro 2006/960/GAI del Consiglio (GU L 386 del 29.122006, pag. 89).

36 Convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181) del Consiglio d'Europa dell'8.11.2001 (protocollo addizionale n. 181); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

usano con una certa frequenza per scambiare le informazioni[37]. La Commissione è tenuta a presentare una relazione di valutazione al Consiglio entro la fine del 2010.

La **decisione di Prüm** si basa su un accordo concluso nel 2005 da Germania, Francia, Spagna, paesi del Benelux e Austria per potenziare la cooperazione nella lotta al terrorismo, alla criminalità transfrontaliera e alla migrazione illegale. In risposta all'interesse di vari Stati membri di aderire al trattato di Prüm, durante la presidenza tedesca del Consiglio del 2007 la Germania ha proposto di trasformare tale trattato in uno strumento dell'UE. La decisione di Prüm del 2008, che deve essere attuata entro agosto 2011, fissa le norme per lo scambio transfrontaliero di profili DNA, impronte digitali, dati di immatricolazione dei veicoli e informazioni su persone sospettate di preparare attentati terroristici[38]. Il suo obiettivo è potenziare la prevenzione dei reati, in particolare il terrorismo e la criminalità transfrontaliera, e mantenere l'ordine pubblico durante eventi di rilievo. Il sistema di Prüm funzionerà in modo decentrato, mettendo in collegamento, tramite i punti di contatto nazionali, le banche dati degli Stati partecipanti sui profili DNA, le impronte digitali e i dati di immatricolazione dei veicoli. Avvalendosi della rete s-TESTA della Commissione, i punti di contatto tratteranno le richieste ricevute e inviate per il confronto transnazionale di profili DNA, impronte digitali e dati di immatricolazione dei veicoli. I loro poteri in ordine alla trasmissione di tali dati agli utenti finali sono disciplinati dalla normativa nazionale. A partire dall'agosto 2011 il confronto dei dati sarà completamente automatizzato; gli Stati membri devono tuttavia superare un rigoroso processo di valutazione (riguardante in particolare il rispetto degli obblighi di protezione dei dati e dei requisiti tecnici) per ottenere l'autorizzazione all'avvio della condivisione automatizzata dei dati. Non sarà possibile scambiare dati personali ai sensi della decisione di Prüm fintanto che gli Stati membri non avranno garantito un livello di protezione dei dati personali corrispondente almeno a quello risultante dalla convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e dalla raccomandazione nel settore della polizia[39]. Il Consiglio deciderà all'unanimità se tale condizione è rispettata. I dati personali potranno essere usati solamente ai fini per i quali sono trasmessi, a meno che lo Stato membro che li ha forniti non ne autorizzi l'uso per altri fini. Gli interessati potranno anche rivolgersi alle rispettive autorità nazionali di protezione dei dati designate ai sensi della direttiva 95/46/CE, per far valere i propri diritti in ordine al trattamento dei dati personali in forza della decisione di Prüm. Il confronto dei profili DNA e delle impronte digitali sarà effettuato in base a un sistema "hit/no hit" (anonimo) per cui le autorità potranno chiedere informazioni personali su un interessato solo se la consultazione iniziale ha dato una risposta positiva. Tali richieste di informazioni addizionali saranno di norma trasmesse tramite l'iniziativa svedese. La decisione di Prüm è in fase di attuazione nell'UE-27; Norvegia e

---

37 Dati basati sulle risposte a un questionario il cui esito è stato presentato dalla presidenza spagnola del Consiglio in una riunione del gruppo di lavoro ad hoc del Consiglio sullo scambio di informazioni del 22 giugno 2010.

38 Decisione 2008/615/GAI del Consiglio (GU L 210 del 6.8.2008, pag. 1); decisione 2008/616/GAI del Consiglio (GU L 210 del 6.8.2008, pag. 12).

39 Convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181) del Consiglio d'Europa dell'8.11.2001 (protocollo addizionale n. 181); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

Islanda stanno aderendo[40]. La Commissione deve presentare una relazione di valutazione al Consiglio nel 2012.

In risposta agli attentati di Londra del luglio 2005, il Regno Unito, l'Irlanda, la Svezia e la Francia hanno proposto di adottare uno strumento dell'UE che armonizzi le norme nazionali sulla conservazione dei dati. La **direttiva sulla conservazione dei dati** del 2006 impone ai fornitori di servizi telefonici e Internet di conservare, a fini di indagine, accertamento e perseguimento di reati gravi, i dati relativi al traffico nelle reti di comunicazione elettronica e i dati relativi all'ubicazione, nonché informazioni sugli abbonati (tra cui il numero di telefono, l'indirizzo IP e l'identificativo dell'apparecchiatura mobile)[41]. La direttiva sulla conservazione dei dati non disciplina né l'accesso né l'uso dei dati conservati dalle autorità nazionali. Dal suo campo di applicazione è esplicitamente escluso il contenuto della comunicazione elettronica; in altre parole, questo strumento non autorizza le intercettazioni telefoniche. La misura lascia il compito di definire i "reati gravi" agli Stati membri, cui compete inoltre precisare le autorità nazionali che possono accedere ai dati caso per caso e le procedure e condizioni per avere accesso alle informazioni. I dati sono conservati per periodi che variano da sei a 24 mesi. Per quanto riguarda la protezione dei dati personali nell'ambito di questo strumento, si applicano le direttive 95/46/CE e 2002/58/CE[42]. Sei Stati membri non hanno ancora recepito integralmente la direttiva sulla conservazione dei dati e le corti costituzionali di Germania e Romania hanno dichiarato l'incostituzionalità della rispettive leggi nazionali di attuazione. La corte costituzionale tedesca ha dichiarato incostituzionali, per come sono state recepite nell'ordinamento nazionale, le norme riguardanti l'accesso e l'uso dei dati[43]. La corte costituzionale romena ha ritenuto dal canto suo che la conservazione dei dati è di per sé contraria all'articolo 8 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ne ha dichiarato l'incostituzionalità[44]. La Commissione sta valutando lo strumento e presenterà una relazione di valutazione al Parlamento europeo e al Consiglio verso la fine del 2010.

L'istituzione del **sistema europeo di informazione sui casellari giudiziari** (ECRIS) risale a un'iniziativa belga del 2004 intesa a impedire ai condannati per reati a sfondo sessuale di svolgere lavori a contatto con minori in altri Stati membri. In passato gli Stati membri si basavano sulla convenzione europea di assistenza giudiziaria in materia penale del Consiglio d'Europa per scambiarsi informazioni sulle condanne pronunciate a livello nazionale, ma il sistema si è rivelato inefficace[45]. Il Consiglio ha mosso un primo passo per una riforma adottando la decisione 2005/876/GAI del Consiglio che imponeva agli Stati membri di designare un'autorità centrale incaricata di trasmettere periodicamente agli altri Stati membri le condanne pronunciate nei confronti dei loro cittadini[46]. Il nuovo strumento consentiva inoltre agli Stati membri di ottenere, per la prima volta e fatta salva la normativa nazionale, informazioni sulle precedenti condanne penali a carico di loro cittadini in altri Stati membri

---

40 Ad oggi sono 10 gli Stati membri autorizzati ad avviare lo scambio automatizzato di profili DNA, cinque quello di impronte digitali e sette quello di dati di immatricolazione dei veicoli. La Germania, l'Austria, la Spagna e i Paesi Bassi hanno trasmesso alla Commissione statistiche parziali sull'uso di questo strumento.

41 Direttiva 2006/24/CE (GU L 105 del 13.4.2006, pag. 54).

42 Direttiva 95/46/CE (GU L 281 del 23.11.1995, pag. 31); direttiva 2002/58/CE (GU L 201 del 31.7.2002, pag. 37) (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

43 Sentenza della corte costituzionale tedesca (*Bundesverfassunggericht*) dell'11.3.2008, 1 BvR 256/08.

44 Decisione n. 1258 della corte costituzionale romena dell'8.10.2009.

45 Convenzione europea di assistenza giudiziaria in materia penale (STCE n. 30) del Consiglio d'Europa del 20.4.1959. Si veda inoltre il documento COM(2005) 10 del 25.1.2005.

46 Decisione 2005/876/GAI del Consiglio (GU L 322 del 9.12.2005, pag. 33).

semplicemente compilando un modulo uniforme, senza dover ricorrere alle procedure di assistenza giudiziaria reciproca. Nel 2006 e 2007 la Commissione ha presentato un pacchetto legislativo globale composto da tre strumenti: la decisione quadro 2008/675/GAI del Consiglio che impone agli Stati membri di prendere in considerazione le precedenti decisioni di condanna in occasione di un nuovo procedimento penale; la decisione quadro 2009/315/GAI del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario; la decisione 2009/316/GAI del Consiglio che istituisce ECRIS quale strumento tecnico per lo scambio di informazioni estratte dal casellario giudiziario[47]. Le decisioni quadro 2009/315/GAI e 2009/316/GAI del Consiglio, la cui attuazione è prevista entro aprile 2012, sono dirette a definire le modalità secondo le quali lo Stato membro di condanna deve trasmettere le informazioni sulle nuove condanne allo o agli Stati membri di cittadinanza del condannato, definire gli obblighi di conservazione e fissare il quadro per un sistema informatizzato di scambio di informazioni. ECRIS è un sistema di informazione decentrato che interconnette le banche dati dei casellari giudiziari degli Stati membri tramite la rete s-TESTA della Commissione. Più autorità centrali potranno scambiarsi dati relativi alle condanne nuove e passate e informazioni estratte dai casellari giudiziari. I dati saranno cifrati e strutturati in base a un formato predeterminato e comprenderanno dati anagrafici, condanna, pena, reato e ulteriori informazioni (tra cui impronte digitali, se disponibili). A partire dall'aprile 2012, ai fini di un procedimento penale pendente occorrerà fornire le informazioni estratte dal casellario giudiziario e inviarle alle autorità giudiziarie o alle autorità amministrative competenti, quali gli organi autorizzati a svolgere controlli su persone in relazione a incarichi di natura sensibile o al possesso di armi da fuoco. I dati personali trasmessi ai fini di un procedimento penale potranno essere usati solo per questa finalità; per ogni altro uso è necessario il consenso dello Stato che li ha trasmessi. Il trattamento dei dati personali deve essere conforme alle disposizioni specifiche della decisione quadro 2009/315/GAI del Consiglio, che include le norme della decisione 2005/876/GAI del Consiglio, e della decisione quadro 2008/977/GAI del Consiglio e della convenzione del Consiglio d'Europa n. 108[48]. Al trattamento dei dati personali da parte delle istituzioni dell'Unione nell'ambito di ECRIS, ad esempio per garantire la sicurezza dei dati, si applica il regolamento (CE) n. 45/2001[49]. Questo pacchetto legislativo non contiene norme sulla conservazione dei dati, in quanto a disciplinare la conservazione delle informazioni relative alle condanne penali è la legislazione nazionale. È in corso un progetto pilota cui partecipano 15 Stati membri, nove dei quali hanno iniziato lo scambio elettronico di informazioni estratte dai casellari giudiziari. La Commissione è tenuta a presentare al Parlamento europeo e al Consiglio due relazioni di valutazione relative al funzionamento del pacchetto legislativo. La decisione quadro 2008/675/GAI deve essere riesaminata nel 2011 e la decisione quadro 2009/315/GAI nel 2015. A partire dal 2016 la Commissione è inoltre tenuta a pubblicare relazioni periodiche sul funzionamento di ECRIS.

Su iniziativa finlandese, nel 2000 il Consiglio ha adottato uno strumento che organizza lo scambio di informazioni tra le **unità di informazione finanziaria** (UIF) degli Stati membri ai

---

47 Decisione quadro 2008/675/GAI del Consiglio (GU L 220 del 15.8.2008, pag. 32); decisione quadro 2009/315/GAI del Consiglio (GU L 93 del 7.4.2009, pag. 23); decisione 2009/316/GAI del Consiglio (GU L 93 del 7.4.2009, pag. 33). Si veda inoltre il documento COM(2005) 10 del 25.1.2005.

48 Decisione quadro 2009/315/GAI del Consiglio (GU L 93 del 7.4.2009, pag. 23); decisione 2005/876/GAI del Consiglio (GU L 322 del 9.12.2005, pag. 33); decisione quadro 2008/977/GAI del Consiglio (GU L 350 del 30.12.2008, pag. 60); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108).

49 Regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1).

fini della lotta contro il riciclaggio di denaro e, successivamente, del finanziamento del terrorismo[50]. Di norma, le UIF sono istituite presso le autorità di contrasto, le autorità giudiziarie o gli organi amministrativi tenuti a riferire alle autorità finanziarie e hanno l'obbligo di scambiare con i loro omologhi nell'UE i dati finanziari o a fini di contrasto necessari, comprese le informazioni sulle operazioni finanziarie, salvo quando tale informazione risulti palesemente sproporzionata rispetto agli interessi di una persona fisica o giuridica. Le informazioni trasmesse per analisi o indagini su casi di riciclaggio di denaro o finanziamento del terrorismo possono essere usate anche per indagini o azioni penali, salvo che lo Stato membro che le ha fornite ne vieti tale uso. Il trattamento di dati personali deve rispettare le disposizioni della decisione quadro 2008/977/GAI del Consiglio, della convenzione del Consiglio d'Europa n. 108 e della raccomandazione nel settore della polizia[51]. Nel 2002 un gruppo di Stati membri ha istituito FIU.net, un'applicazione di rete decentrata che permette lo scambio di dati tra le UIF e che funziona sulla rete s-TESTA della Commissione[52]. L'iniziativa consta oggi di 20 UIF con status di membro. È al vaglio l'opportunità di usare l'applicazione protetta SIENA di Europol per il funzionamento di FIU.net[53]. Dopo aver valutato la conformità degli Stati membri allo strumento, il Consiglio, nella terza direttiva antiriciclaggio, ha autorizzato le UIF a ricevere, analizzare e comunicare le segnalazioni di operazioni sospette che riguardano casi di riciclaggio *E* di finanziamento del terrorismo[54]. Nell'ambito del piano d'azione per i servizi finanziari, dal 2009 la Commissione sta esaminando l'attuazione della terza direttiva antiriciclaggio[55].

Basandosi su un'iniziativa proposta da Austria, Belgio e Finlandia, nel 2007 il Consiglio ha adottato uno strumento diretto a rafforzare la cooperazione tra gli **uffici per il recupero dei beni** (ARO) ai fini del reperimento e dell'identificazione dei proventi di reato[56]. Come le FIU, gli ARO cooperano su base decentrata ma senza il supporto di una piattaforma online. Per scambiarsi le informazioni devono avvalersi dell'iniziativa svedese e fornire indicazioni sui beni oggetto dei provvedimenti (ad esempio conti bancari, beni immobili e veicoli) e sulle persone fisiche o giuridiche ricercate (ad esempio nomi, indirizzo, data di nascita e informazioni su azionisti o società). L'uso delle informazioni scambiate ai sensi di questo strumento è soggetto alla normativa nazionale sulla protezione dei dati e gli Stati membri non possono riservare un trattamento differenziato ai dati di produzione nazionale e a quelli provenienti da altri Stati membri. I dati personali devono essere trattati in conformità delle disposizioni della convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e della raccomandazione nel settore della polizia[57]. Ad oggi, oltre 20 Stati membri

---

50 Decisione 2000/642/GAI del Consiglio (GU L 271 del 24.10.2000, pag. 4).

51 Decisione quadro 2008/977/GAI del Consiglio (GU L 350 del 30.12.2008, pag. 60); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

52 http://www.fiu.net/

53 SIENA è l'acronimo di *Secure Information Exchange Network Application* (applicazione di rete per lo scambio di informazioni protetta).

54 Direttiva 2005/60/CE (GU L 309 del 25.11.2005, pag. 15) (terza direttiva antiriciclaggio).

55 Si veda, ad esempio, la relazione finale sulla valutazione dell'impatto economico del piano d'azione per i servizi finanziari (*Evaluation of the economic impacts of the Financial Services Action Plan — Final report*) realizzata nel marzo 2009 da CRA International per la Commissione europea, DG MARKT.

56 Decisione 2007/845/GAI del Consiglio (GU L 332 del 18.12.2007, pag. 103).

57 Convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al

hanno istituito uffici per il recupero dei beni. Considerato il carattere sensibile delle informazioni scambiate, è al vaglio l'opportunità che gli ARO usino l'applicazione SIENA di Europol per scambiarsi i dati. Nel quadro di un progetto pilota avviato nel maggio 2010, 12 ARO hanno iniziato a servirsi di SIENA per condividere informazioni utili al reperimento di beni. La Commissione è tenuta a presentare una relazione di valutazione al Consiglio nel 2010.

Nel 2008 la presidenza francese del Consiglio ha invitato gli Stati membri a istituire **piattaforme nazionali di segnalazione dei reati informatici**, e Europol a istituire una piattaforma europea di segnalazione dei reati informatici, allo scopo di raccogliere, analizzare e scambiare informazioni sui reati commessi su Internet[58]. I cittadini possono segnalare alle proprie piattaforme nazionali i contenuti o i comportamenti illeciti rilevati su Internet. La piattaforma europea in materia di criminalità informatica, gestita da Europol, fungerà da centro informativo per l'analisi e lo scambio con le autorità di contrasto nazionali di informazioni sui reati informatici rientranti nel mandato di Europol[59]. Ad oggi, quasi tutti gli Stati membri hanno istituito piattaforme nazionali di segnalazione dei reati informatici. Europol sta procedendo alla realizzazione tecnica della piattaforma europea in materia di criminalità informatica e presto potrà usare l'applicazione SIENA per potenziare la condivisione dei dati con le piattaforme nazionali. Nella misura in cui lo scambio di informazioni comporta il trattamento di dati personali da parte di Europol, si applicano le disposizioni specifiche sulla protezione dei dati della decisione Europol (decisione 2009/371/GAI del Consiglio) nonché il regolamento (CE) 45/2001, la convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e la raccomandazione nel settore della polizia[60]. Le disposizioni della decisione quadro 2008/977/GAI del Consiglio disciplinano lo scambio dei dati personali tra gli Stati membri ed Europol[61]. In mancanza di uno strumento giuridico, non esiste un meccanismo di revisione formale per le piattaforme di segnalazione dei reati informatici. Tuttavia, Europol è già competente in questo importante settore e in futuro riferirà sulle attività della piattaforma europea in materia di criminalità informatica nella relazione annuale che presenta al Consiglio per approvazione e al Parlamento europeo per informazione.

---

trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181) del Consiglio d'Europa dell'8.11.2001 (protocollo addizionale n. 181); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

58 Conclusioni del Consiglio sull'istituzione di piattaforme nazionali e di una piattaforma europea per la segnalazione dei reati rilevati su Internet, Consiglio "Giustizia e affari interni" del 24.10.2008; conclusioni del Consiglio su un piano d'azione per l'attuazione della strategia concertata di lotta alla criminalità informatica, Consiglio "Affari generali" del 26.4.10. Europol ha ribattezzato il progetto "piattaforma europea in materia di criminalità informatica".

59 L'obiettivo di Europol è prevenire e combattere la criminalità organizzata, il terrorismo e altre forme gravi di criminalità che interessano due o più Stati membri. Si veda la decisione 2009/371/GAI del Consiglio (GU L 121 del 15.5.2009, pag. 37).

60 Decisione 2009/371/GAI del Consiglio (GU L 121 del 15.5.2009, pag. 37); regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181) del Consiglio d'Europa dell'8.11.2001 (protocollo addizionale n. 181); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

61 Decisione quadro 2008/977/GAI del Consiglio (GU L 350 del 30.12.2008, pag. 60).

Agenzie e organi dell'UE incaricate di assistere gli Stati membri nella prevenzione e lotta contro le forme gravi di criminalità transnazionale

Istituito nel 1995, l'**Ufficio europeo di polizia** (Europol) ha iniziato le attività nel 1999 per diventare agenzia dell'Unione nel gennaio 2010[62]. Obiettivo di Europol è assistere gli Stati membri per prevenire e combattere la criminalità organizzata, il terrorismo e altre forme gravi di criminalità che interessano due o più Stati membri. Tra i suoi compiti principali: raccogliere, conservare, trattare, analizzare e scambiare informazioni e intelligence; facilitare le indagini; fornire intelligence e supporto analitico agli Stati membri. Il principale organo di collegamento tra Europol e gli Stati membri è costituito dalle unità nazionali di Europol (UNE) che distaccano presso quest'ultimo ufficiali di collegamento. I capi delle UNE si riuniscono regolarmente per assistere Europol in questioni operative, mentre sul funzionamento dell'agenzia vigilano il consiglio di amministrazione e il direttore. Gli strumenti di gestione delle informazioni a disposizione di Europol comprendono il sistema di informazione Europol (SIE), gli archivi di lavoro per fini di analisi (AWF) e l'applicazione SIENA. Il SIE contiene dati personali, tra cui gli identificatori biometrici, le condanne penali e i legami con la criminalità organizzata di persone indagate per reati di competenza di Europol. Al sistema possono accedere soltanto le UNE, il personale autorizzato di Europol e il direttore. Gli archivi AWF, aperti allo scopo di contribuire alle indagini penali, contengono dati personali e altre informazioni che le unità nazionali decidano di aggiungere. L'accesso è consentito agli ufficiali di collegamento ma l'immissione di dati è riservata agli analisti di Europol. Grazie a una funzione indice, le UNE e gli ufficiali di collegamento possono verificare se un archivio AWF contiene dati di interesse per i loro Stati membri. Gli Stati membri usano con frequenza sempre maggiore l'applicazione SIENA per condividere dati sensibili a fini di contrasto. Nello svolgimento delle proprie funzioni Europol può trattare informazioni e intelligence, inclusi i dati personali. Gli Stati membri possono utilizzare le informazioni estratte dagli archivi di Europol esclusivamente a fini di prevenzione e lotta alle forme gravi di criminalità transnazionale. Se lo Stato membro che fornisce le informazioni ne subordina l'uso a eventuali restrizioni, queste devono essere rispettate anche dagli utenti che estraggono i dati dagli archivi di Europol. Europol può inoltre scambiare dati personali con paesi terzi con cui ha concluso accordi operativi e che garantiscono un livello di protezione dei dati adeguato. Può conservare i dati solo per il tempo necessario per l'esercizio dei suoi compiti. Gli archivi AWF sono conservati per un periodo massimo di tre anni, prorogabili una sola volta per ulteriori tre anni. Il trattamento dei dati personali operato da Europol deve essere conforme alle disposizioni specifiche sulla protezione dei dati della decisione che disciplina Europol (decisione 2009/371/GAI del Consiglio) e del regolamento (CE) n. 45/2001, della convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e della raccomandazione nel settore della polizia[63]. Allo scambio dei dati personali tra gli Stati membri ed Europol si applicano le disposizioni della decisione quadro 2008/977/GAI

---

62 Decisione 2009/371/GAI del Consiglio (GU L 121 del 15.5.2009, pag 37) che sostituisce la convenzione basata sull'articolo K.3 del trattato sull'Unione europea che istituisce un ufficio europeo di polizia (GU C 316 del 27.11.1995, pag. 2).

63 Decisione 2009/371/GAI del Consiglio (GU L 121 del 15.5.2009, pag. 37); regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1); convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) (convenzione del Consiglio d'Europa n. 108); protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181) del Consiglio d'Europa dell'8.11.2001 (protocollo addizionale n. 181); raccomandazione R (87) 15 del 17 settembre 1987 del comitato dei Ministri del Consiglio d'Europa tendente a regolare l'utilizzazione dei dati di natura personale nel settore della polizia (raccomandazione nel settore della polizia).

del Consiglio[64]. L'autorità di controllo comune, composta da membri delle autorità di controllo nazionali, è incaricata di controllare il trattamento dei dati personali da parte di Europol e la legittimità della loro trasmissione ad altre parti, e trasmette periodicamente rapporti al Parlamento europeo e al Consiglio. Europol presenta un rapporto annuale di attività al Consiglio per approvazione e al Parlamento europeo per approvazione.

Oltre ad incidere su molti degli strumenti già descritti, gli attentati terroristici dell'11 settembre 2001 hanno indotto a istituire, nel 2002, l'**Unità di cooperazione giudiziaria dell'Unione europea** (Eurojust)[65]. Eurojust è un organo dell'Unione europea il cui obiettivo è migliorare il coordinamento delle indagini e dell'azione penali tra gli Stati membri e rafforzare la cooperazione tra le autorità nazionali competenti. Le sue competenze si estendono alle stesse forme di criminalità e agli stessi tipi di reati di cui si occupa Europol. Nell'ambito del mandato di Eurojust e ai fini dell'esercizio delle sue funzioni, i 27 membri nazionali che ne compongono il collegio sono autorizzati ad accedere ai dati personali degli indagati e degli autori dei reati, in particolare ai dati anagrafici, ai recapiti, ai dati di immatricolazione dei veicoli, ai profili DNA, alle fotografie, alle impronte digitali e ai dati messi a disposizione da fornitori di servizi di telecomunicazioni relativi al traffico, all'ubicazione e agli abbonati. Gli Stati membri dovrebbero condividere questi dati con Eurojust per consentire all'Unità di svolgere le proprie funzioni. Tutti i dati personali che si riferiscono a un caso devono essere inseriti nel sistema automatico di gestione dei fascicoli che gira sulla rete TESTA della Commissione. Un sistema di indice conserva i dati personali e non personali rilevanti per le indagini in corso. Eurojust può trattare dati personali nell'esercizio delle sue funzioni, ma queste operazioni devono avvenire in conformità delle disposizioni specifiche della decisione che disciplina Eurojust (decisione 2009/426/GAI del Consiglio), della convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale n. 181 e della raccomandazione nel settore della polizia. Allo scambio dei dati personali tra gli Stati membri ed Eurojust si applicano le disposizioni della decisione quadro 2008/977/GAI del Consiglio[66]. Eurojust può scambiare dati con autorità nazionali e paesi terzi con cui ha concluso accordi, a condizione che il membro nazionale che ha fornito i dati abbia dato il suo consenso alla trasmissione e che il paese terzo garantisca un adeguato livello di protezione dei dati personali. Questi ultimi possono essere conservati per tutto il tempo necessario a raggiungere gli obiettivi di Eurojust, ma vanno cancellati una volta chiuso il caso. Gli Stati membri devono attuare la base giuridica modificata di Eurojust entro giugno 2011 ed entro giugno 2014 la Commissione deve provvedere alla revisione, proponendo le modifiche che ritiene opportune in ordine allo scambio di informazioni tra i membri nazionali di Eurojust. Entro giugno 2013 Eurojust presenterà al Consiglio e alla Commissione una relazione sull'esperienza relativa all'accesso a livello nazionale al sistema di gestione dei fascicoli. Su questa base gli Stati membri potranno rivedere i diritti di accesso nazionali. L'autorità di controllo comune, composta da giudici nominati dagli Stati membri, controlla il trattamento dei dati personali da parte di Eurojust e riferisce ogni anno al Consiglio. Il presidente del collegio presenta al Consiglio una relazione annuale sulle attività di Eurojust, che il Consiglio trasmette al Parlamento europeo.

---

64 Decisione quadro 2008/977/GAI del Consiglio (GU L 350 del 30.12.2008, pag. 60).

65 Decisione 2002/187/GAI del Consiglio (GU L 63 del 6.3.2002, pag. 1), modificata dalla decisione 2009/426/GAI del Consiglio (GU L 138 del 4.6.2009, pag. 14). Si veda anche il Consiglio straordinario "Giustizia e affari interni" del 29.9.2001.

66 Decisione quadro 2008/977/GAI del Consiglio (GU L 350 del 30.12.2008, pag. 60).

Accordi internazionali diretti a prevenire e combattere il terrorismo e altre forme gravi di criminalità transnazionale

In conseguenza degli attentati terroristici dell'11 settembre 2001, gli Stati Uniti hanno adottato una legislazione che impone ai vettori aerei che operano voli per, da o attraverso il loro territorio di fornire alle autorità statunitensi i **dati del codice di prenotazione** (*Passenger Name Record*, PNR) contenuti nei loro sistemi automatizzati di prenotazione. Poco tempo dopo il Canada e l'Australia hanno deciso di seguire l'esempio degli Stati Uniti. Poiché la legislazione dell'UE in materia prevede la valutazione preventiva del livello di protezione dei dati garantito dai paesi terzi, la Commissione è intervenuta in tal senso negoziando accordi PNR con questi paesi[67]. Nel luglio 2007 è stato firmato l'accordo con gli Stati Uniti, nel giugno 2008 con l'Australia e nell'ottobre 2005 l'accordo API/PNR con il Canada[68]. Gli accordi con gli Stati Uniti e l'Australia sono applicabili in via provvisoria, mentre l'accordo con il Canada resta in vigore nonostante sia scaduta, nel settembre 2009, la decisione di adeguatezza della Commissione relativa alle norme canadesi sulla protezione dei dati[69]. Esprimendosi in termini critici sul loro contenuto, il Parlamento europeo ha invitato la Commissione a rinegoziare tutti e tre gli accordi sulla base di un'unica serie di principi[70]. Inviati con largo anticipo sulla partenza di un volo, i dati PNR sono utili alle autorità di contrasto nell'attività di controllo dei passeggeri per individuare eventuali legami con il terrorismo e con altre forme gravi di criminalità. Pertanto, scopo di ogni accordo è la prevenzione e la lotta la terrorismo e altre forme gravi di criminalità transnazionale. In cambio dei dati PNR di provenienza UE, il dipartimento per la sicurezza interna degli Stati Uniti (*Department of Homeland Security* – DHS) condivide con le autorità di contrasto dell'UE, Europol e Eurojust le "informazioni indiziarie" che risultano dalle sue analisi dei dati PNR; inoltre, sia il Canada che gli Stati Uniti si sono impegnati nei rispettivi accordi a collaborare con l'UE per assisterla nella creazione del proprio sistema PNR. Gli accordi con gli Stati Uniti e con l'Australia contengono 19 categorie di dati, tra cui dati anagrafici, di prenotazione, pagamento e informazioni aggiuntive; l'accordo con il Canada contiene 25 voci simili. Le informazioni aggiuntive comprendono, tra l'altro, dati sui biglietti di sola andata, sullo stato di "standby" e sullo stato di mancata presentazione all'imbarco. L'accordo con gli Stati Uniti consente inoltre, in presenza di condizioni particolari, di utilizzare informazioni sensibili. Il DHS può trattare queste informazioni se è a rischio la vita dell'interessato o altrui, ma deve cancellarle entro 30 giorni. I dati PNR sono inviati a una serie di unità centrali presso il DHS, l'Agenzia dei servizi di frontiera del Canada (*Canada Border Services Agency*) e l'amministrazione doganale australiana (*Australian Customs Service*), che possono trasferirli ad altre autorità di contrasto e antiterrorismo nazionali. Nell'accordo con gli Stati Uniti, il DHS si aspetta di non dover garantire nel trattamento dei dati PNR di provenienza UE che un livello di protezione "più elevato" di quello applicato dalle autorità dell'Unione nei rispettivi sistemi PNR nazionali. Non dovesse concretizzarsi quest'aspettativa, il DHS potrebbe sospendere alcune parti dell'accordo. Secondo l'UE, la condizione perché il Canada e

---

67 Direttiva 95/46/CE (direttiva sulla protezione dei dati) (GU L 281 del 23.11.1995, pag. 31).

68 Il pacchetto canadese è composto da una dichiarazione d'intenti del Canada relativa al trattamento dei dati API/PNR, dalla decisione della Commissione concernente l'adeguatezza delle norme in materia di protezione dei dati e da un accordo internazionale (vedi GU L 91 del 29.3.2006, pag. 49; GU L 82 del 21.3.2006, pag. 14). L'accordo con gli Stati Uniti è pubblicato nella GU L 204 del 4.8.2007, pag. 16, e l'accordo con l'Australia nella GU L 213 dell'8.8.2008, pag. 47.

69 Nel 2009, il Canada si è impegnato nei confronti della Commissione, della presidenza del Consiglio e degli Stati membri dell'UE a continuare a applicare i termini della precedente dichiarazione d'intenti del 2005 relativa all'uso dei dati UE PNR. La decisione di adeguatezza della Commissione era basata su tale dichiarazione d'intenti.

70 Risoluzione del Parlamento europeo P7_TA(2010)0144 del 5.5.2010.

l'Australia assicurino un livello "adeguato" di protezione dei dati PNR di provenienza UE è che osservino le condizioni contenute nei rispettivi accordi. Negli Stati Uniti, i dati PNR di provenienza UE sono conservati per sette anni in una banca dati attiva, e per altri otto anni in una banca dati dormiente. In Australia i dati sono inseriti in una banca dati attiva per tre anni e mezzo, e successivamente, per due anni, in una banca dati dormiente. In entrambi i paesi, l'accesso alla banca dati dormiente è consentito soltanto previa autorizzazione speciale. In Canada i dati vengono conservati per tre anni e mezzo, e le informazioni sono rese anonime dopo 72 ore. Ogni accordo è soggetto a verifica periodica e solo gli accordi canadese e australiano ne prevedono la denuncia. Nell'UE, soltanto il Regno Unito dispone di un sistema PNR. La Francia, la Danimarca, il Belgio, la Svezia e i Paesi Bassi hanno in alcuni casi emanato leggi in materia, in altri stanno testando l'uso dei dati PNR in vista di istituire un sistema PNR. Molti altri Stati membri stanno valutando questa ipotesi mentre tutti fanno uso, caso per caso, dei dati PNR a fini di contrasto.

Dopo gli attentati terroristici dell'11 settembre 2001, il dipartimento del Tesoro degli Stati Uniti ha sviluppato il **programma di controllo delle transazioni finanziarie dei terroristi** (TFTP) per identificare, controllare e perseguire i terroristi e i loro finanziatori. Nell'ambito del TFTP, il dipartimento del Tesoro ha emesso ordinanze amministrative per intimare alla filiale di una società belga di trasferirgli serie limitate di dati di messaggistica finanziaria che transitano sulla sua rete. Nel gennaio 2010 questa società ha modificato la sua architettura di sistema, riducendo di più della metà la quantità di dati di competenza giurisdizionale statunitense e quindi di norma soggetti alle ordinanze del Tesoro. Nel novembre del 2009, la presidenza del Consiglio dell'Unione europea e il governo degli Stati Uniti hanno firmato un accordo interinale sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del TFTP, che il Parlamento europeo non ha approvato[71]. Sulla base di un nuovo mandato, la Commissione europea ha negoziato un ulteriore progetto di accordo con gli Stati Uniti, presentando al Consiglio, il 18 giugno 2010, una proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi[72]. Il Parlamento europeo ha approvato la conclusione dell'accordo l'8 luglio 2010[73]. Ora spetta al Consiglio adottare una decisione relativa alla conclusione dell'accordo, dopodiché l'accordo entrerà in vigore mediante uno scambio di lettere tra le parti. Obiettivo dell'accordo TFTP UE-USA è la prevenzione, l'indagine, l'accertamento o l'azione penale nei confronti del terrorismo o del suo finanziamento. L'accordo obbliga i fornitori designati di servizi di messaggistica finanziaria a trasferire al dipartimento del Tesoro statunitense, sulla base di valutazioni specifiche della minaccia geografica e di richieste precise, serie di dati di messaggistica finanziaria contenenti, tra l'altro, il nome, il numero di conto, l'indirizzo e il numero d'identificazione dell'ordinante e/o del o dei beneficiari della transazione finanziaria. Il dipartimento del Tesoro può ricercare tali dati esclusivamente ai fini del TFTP e solo qualora abbia motivo di ritenere che la persona identificata ha un nesso con il terrorismo o il suo finanziamento. Sono vietati il *data mining* e il trasferimento di dati relativi a transazioni all'interno dello spazio unico dei pagamenti in euro. Gli Stati Uniti forniscono agli Stati membri dell'UE, a Europol e Eurojust le "informazioni indiziarie" riguardanti potenziali attentati terroristici nell'UE, e assisteranno l'Unione nell'istituire un sistema proprio equivalente al TFTP. Nell'ipotesi che l'UE decida di

---

71 Risoluzione del Parlamento europeo P7_TA(2010)0029, 11.2.2010.

72 COM(2010) 316 definitivo/2 del 18.6.2010.

73 Risoluzione del Parlamento europeo P7_TA-PROV(2010)0279 dell'8.7.2010.

istituire un tale programma, le due parti potrebbero riadattare le condizione dell'accordo. Prima di qualsiasi trasferimento di dati, ogni richiesta d'informazioni da parte degli Stati Uniti deve essere esaminata da Europol per garantire che rispetti le condizioni dell'accordo. Le informazioni estratte dai dati di messaggistica finanziaria possono essere conservate solo per il tempo necessario alle indagini o azioni penali specifiche; i dati non estratti possono essere conservati per un massimo di cinque anni. Qualora necessario per l'indagine, la prevenzione o l'azione penale nei confronti del terrorismo o del suo finanziamento, il dipartimento del Tesoro può trasferire alle autorità di contrasto, di pubblica sicurezza o antiterrorismo statunitensi, agli Stati membri UE e a Europol o Eurojust i dati personali estratti dai messaggi FIN. Può inoltre condividere con paesi terzi le informazioni indiziarie relative a cittadini e residenti UE, previo consenso dello Stato membro interessato. Il rispetto della rigorosa limitazione delle finalità al controterrorismo e delle altre salvaguardie è oggetto di monitoraggio e supervisione indipendenti, anche di una personalità nominata dalla Commissione. L'accordo è stato siglato per una durata di cinque anni e ciascuna parte può denunciarlo o sospenderlo. Dopo sei mesi dall'entrata in vigore dell'accordo, un gruppo diretto dalla Commissione e composto da rappresentanti di due autorità di protezione dei dati e da una persona con esperienza in campo giudiziario procederà alla verifica dello stesso, valutando in particolare l'attuazione, da parte dei firmatari, delle disposizioni relative alla limitazione delle finalità e alla proporzionalità e il rispetto degli obblighi di protezione dei dati. La relazione della Commissione sarà presentata al Parlamento europeo e al Consiglio.

2.2. Iniziative ai sensi del piano d'azione per l'attuazione del programma di Stoccolma

Proposte legislative che presenterà la Commissione

Nel programma di Stoccolma il Consiglio europeo ha invitato la Commissione a presentare tre proposte che riguardano direttamente la presente comunicazione: un sistema PNR dell'UE per la prevenzione, l'accertamento e l'azione penale nei confronti del terrorismo e dei reati gravi, un sistema di registrazione ingressi/uscite e un programma per viaggiatori registrati. Come ha sottolineato il Consiglio europeo, gli ultimi due dovrebbero essere presentati "il prima possibile". La Commissione ha inserito tutte e tre le richieste nel piano d'azione per l'attuazione del programma di Stoccolma[74] e punta ora ad attuarle e, in futuro, a valutare questi strumenti sulla base dei principi di elaborazione delle politiche esposti nella sezione 4.

Nel novembre 2007 la Commissione ha presentato una proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione nelle attività di contrasto[75]. Questa iniziativa ha avuto l'appoggio del Consiglio ed è stata successivamente rimaneggiata in funzione degli emendamenti del Parlamento europeo e del parere del Garante europeo della protezione dei dati, ma è decaduta con l'entrata in vigore del trattato di Lisbona. Come indicato nel piano d'azione per l'attuazione del programma di Stoccolma, attualmente la Commissione sta lavorando per presentare, a inizi 2011, un **pacchetto relativo al codice di prenotazione** così composto: una comunicazione relativa a una strategia esterna dell'UE in ambito PNR che enuclei i principi fondamentali da seguire per negoziare accordi con paesi terzi; direttive di negoziato per rinegoziare gli accordi PNR con gli Stati Uniti e l'Australia;

---

[74] Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini, documento del Consiglio n. 5731/10 del 3.3.2010; COM(2010) 171 del 20.4.2010 (Piano d'azione per l'attuazione del programma di Stoccolma).

[75] COM(2007) 654 del 6.11.2007.

direttive di negoziato per un nuovo accordo con il Canada. La Commissione sta inoltre preparando una nuova proposta di PNR dell'UE.

Nel 2008 la Commissione ha presentato una serie di suggerimenti per sviluppare la gestione integrata delle frontiere dell'Unione europea facilitando gli spostamenti dei cittadini di paesi terzi e rafforzando nel contempo la sicurezza interna[76]. Avendo constatato che i soggiornanti "fuoritermine" (cosiddetti overstayer) rappresentano la principale categoria di immigrati irregolari nell'UE, la Commissione ha suggerito l'eventuale introduzione di un **sistema di ingresso/uscita** per i cittadini di paesi terzi ammessi nell'UE per soggiorni di breve durata fino a tre mesi. Questo sistema registrerebbe la data e il luogo d'ingresso, la durata del soggiorno autorizzato e segnalerebbe automaticamente alle autorità competenti i fuoritermine. Basato sulla verifica dei dati biometrici, userebbe lo stesso sistema di confronto biometrico e la stessa strumentazione operativa dei sistemi SIS II e VIS. Al momento la Commissione sta effettuando una valutazione d'impatto e, come indicato nel piano d'azione per l'attuazione del programma di Stoccolma, farà in modo di presentare una proposta legislativa nel 2011.

La terza proposta all'esame era il **programma per viaggiatori registrati**[77], grazie al quale alcune categorie di persone che viaggiano di frequente da paesi terzi verso l'UE potrebbero usufruire, previo adeguato preesame, di verifiche di frontiera semplificate attraverso porte automatiche. Il programma per viaggiatori registrati sarebbe inoltre fondato sulla verifica dell'identità mediante l'uso di dati biometrici e consentirebbe un passaggio graduale dall'attuale approccio incentrato su controlli di frontiera generici a uno basato sul rischio individuale. La Commissione ha effettuato una valutazione d'impatto e, in linea con il piano d'azione per l'attuazione del programma di Stoccolma, prevede di presentare una proposta legislativa nel 2011.

Iniziative per cui la Commissione deve realizzare studi

Nel programma di Stoccolma, il Consiglio europeo ha invitato la Commissione a svolgere studi su tre iniziative che riguardano la presente comunicazione: possibilità di tracciamento del finanziamento del terrorismo nell'UE; fattibilità e utilità di un sistema europeo di autorizzazione di viaggio e necessità e valore aggiunto di un indice europeo dei casellari giudiziali. Anche queste iniziative fanno parte del piano d'azione per l'attuazione del programma di Stoccolma, e la Commissione ne valuterà la fattibilità e deciderà se e come portarle avanti sulla base dei principi di elaborazione delle politiche esposti nella sezione 4.

L'accordo TFTP UE-USA invita la Commissione europea a realizzare uno studio sull'introduzione eventuale di un **sistema UE di controllo delle transazioni finanziarie dei terroristi** equivalente al TFTP statunitense che consenta un trasferimento dei dati più mirato dall'UE agli USA. Il progetto di decisione del Consiglio relativa alla conclusione dell'accordo invita altresì la Commissione a presentare al Parlamento europeo e al Consiglio, entro un anno dalla data di entrata in vigore dell'accordo TFTP UE-USA, un quadro giuridico e tecnico per l'estrazione di dati sul territorio UE[78]. Entro tre anni dalla data di entrata in vigore dell'accordo la Commissione dovrà presentare una relazione sui progressi nello sviluppo di tale sistema UE equivalente. Se cinque anni dopo la data di entrata in vigore dell'accordo non è stato istituito il sistema UE equivalente, l'Unione potrà decidere di non rinnovare l'accordo.

---

76 COM(2008) 69 del 13.2.2008.

77 COM(2008) 69 del 13.2.2008.

78 Documento del Consiglio n. 11222/1/10 REV 1 del 24.6.2010; documento del Consiglio n. 11222/1/10 REV1 COR1 del 24.6.2010.

L'accordo TFTP UE-USA impegna inoltre gli USA a cooperare con l'UE prestando assistenza e consulenza qualora questa decida di istituire un tale sistema. Fatta salva la decisione finale, la Commissione ha già iniziato a esaminare le implicazioni pratiche e in termini di risorse e protezione dei dati che questo impegno comporta. Come indicato nel piano d'azione per l'attuazione del programma di Stoccolma, la Commissione prevede di presentare nel 2011 una comunicazione sulla fattibilità di istituire un programma europeo di controllo delle transazioni finanziarie dei terroristi (TFTP dell'UE).

Nella comunicazione del 2008 relativa alla gestione integrata delle frontiere, la Commissione ha suggerito l'eventuale introduzione di un **sistema elettronico di autorizzazione di viaggio** per cittadini di paesi terzi senza obbligo di visto[79]. Secondo il programma, i cittadini dei paesi terzi in possesso di questo requisito dovrebbero presentare domanda elettronica fornendo i propri dati prima della partenza e specificando i particolari del passaporto e del viaggio. Rispetto alla procedura per il rilascio del visto, il sistema elettronico di autorizzazione di viaggio sarebbe un metodo più semplice e rapido per verificare se una persona soddisfa le condizioni di ingresso necessarie. Attualmente la Commissione sta conducendo uno studio su vantaggi, svantaggi e implicazioni pratiche dell'introduzione di tale sistema e, come specificato nel piano d'azione per l'attuazione del programma di Stoccolma, nel 2011 intende presentare una comunicazione sulla sua fattibilità.

Nel ricoprire la presidenza del Consiglio nel 2007, la Germania ha avviato una discussione sull'eventuale introduzione di un **indice europeo dei casellari giudiziari** (EPRIS)[80]. Con EPRIS il personale di polizia sarà in grado di reperire più agevolmente le informazioni nell'UE, in particolare quelle riguardanti i collegamenti tra persone sospettate di appartenere alla criminalità organizzata. Nel 2010 la Commissione presenterà al Consiglio il suo progetto di mandato per lo studio di fattibilità su EPRIS e, come indicato nel piano d'azione per l'attuazione del programma di Stoccolma, nel 2012 prevede di presentare una comunicazione sulla sua fattibilità.

3. ANALISI DEGLI STRUMENTI VIGENTI O IN FASE DI ATTUAZIONE O DI ESAME

La panoramica precedente invita alle seguenti osservazioni preliminari.

Struttura decentrata

Dei vari strumenti attualmente vigenti o in fase di attuazione o di esame, solo sei comportano la raccolta o la conservazione di dati personali a livello UE, ovvero il SIS (e SIS II), il VIS, EURODAC, il SID, Europol e Eurojust. Tutte le altre misure disciplinano lo scambio decentrato e transfrontaliero o il trasferimento verso paesi terzi di dati personali raccolti a livello nazionale da autorità pubbliche o imprese private. La maggioranza dei dati personali è raccolta e conservata a livello nazionale; l'UE cerca di apportare un valore aggiunto rendendo possibile, a determinate condizioni, lo scambio di questi dati con partner UE e paesi terzi. La Commissione ha presentato di recente al Parlamento europeo e al Consiglio una proposta modificata che istituisce un'agenzia per la gestione operativa dei sistemi di tecnologia dell'informazione su larga scala del settore della libertà, della sicurezza e della giustizia[81]. Il compito della nuova agenzia IT sarà assicurare la gestione operativa del SIS II, del VIS, di

[79] COM(2008) 69 del 13.2.2008.
[80] Si veda il documento del Consiglio n. 15526/1/09 del 2.12.2009.
[81] COM(2010) 93 del 19.3.2010.

EURODAC e di ogni altro futuro sistema IT nel settore della libertà, della sicurezza e della giustizia, in modo da garantirne il funzionamento costante assicurando così un flusso di informazioni ininterrotto.

Limitazione delle finalità

La maggioranza degli strumenti analizzati in precedenza persegue un obiettivo unitario: EURODAC è diretto a migliorare il funzionamento del sistema Dublino, il sistema API a migliorare i controlli di frontiera, l'iniziativa svedese a promuovere le indagini penali e le operazioni di intelligence, la convenzione Napoli II a contribuire a prevenire, accertare, perseguire e punire le frodi doganali, il SID ad aiutare a prevenire, ricercare e perseguire gravi infrazioni alle leggi nazionali aumentando l'efficienza della cooperazione tra le amministrazioni doganali nazionali, ECRIS, le UIF e gli ARO ad agevolare la condivisione transfrontaliera di dati in determinate aree, e la decisione di Prüm, la direttiva sulla conservazione dei dati, il TFTP e i PNR a lottare contro il terrorismo e le forme gravi di criminalità. Il SIS, il SIS II e il VIS sono le principali eccezioni alla regola: in origine l'obiettivo del VIS era agevolare lo scambio transfrontaliero di dati sui visti, ma lo strumento è stato successivamente esteso alla prevenzione e alla lotta al terrorismo e altre forme gravi di criminalità. L'obiettivo del SIS e del SIS II è assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia e agevolare la circolazione delle persone grazie alle informazioni comunicate attraverso il sistema. Ad accezione di questi sistemi di informazione centralizzati, la limitazione delle finalità risulta essere un fattore primario nel predisporre le misure di gestione delle informazioni a livello UE.

Potenziali sovrapposizioni di funzioni

Più strumenti diversi possono raccogliere gli stessi dati personali ma possono usarli solo per finalità limitate nel proprio stretto ambito (salvo il VIS, il SIS e il SIS II). Ad esempio, i dati anagrafici di una persona, compreso nome, data e luogo di nascita, cittadinanza, possono essere trattati nell'ambito del SIS, del SIS II, del VIS, del sistema API, del SID, dell'iniziativa svedese, della decisione di Prüm, di ECRIS, delle UIF, degli ARO, di Europol, Eurojust e degli accordi PNR e TFTP. Eppure, nel caso del sistema API questi dati possono essere trattati solo a fini di controllo di frontiera, nel caso del SID per prevenire, ricercare e perseguire le frodi doganali, nel caso dell'iniziativa svedese per le indagini penali e le operazioni di intelligence, nel caso della decisione di Prüm per la prevenzione del terrorismo e della criminalità transfrontaliera, nel caso di ECRIS per esaminare i precedenti penali di una persona, nel caso delle UIF per svolgere indagini in ordine ai legami di una persona con la criminalità organizzata e le reti terroristiche, nel caso degli ARO per il recupero dei beni, nel caso di Europol e Eurojust ai fini di indagine e prevenzione della lotta a forme gravi di criminalità, nel caso dei PNR per prevenire e combattere il terrorismo e altre forme gravi di criminalità transnazionale e nel caso del TFTP per identificare e perseguire i terroristi e i loro finanziatori. I dati biometrici quali impronte digitali e fotografie possono essere trattati nell'ambito del SIS II, del VIS, di EURODAC, dell'iniziativa svedese, della decisione di Prüm, di ECRIS, Europol e Eurojust – di nuovo, per le finalità limitate di ciascuno strumento. La decisione di Prüm è l'unico strumento che consente lo scambio transfrontaliero di profili DNA anonimi (che possono però essere trasmessi anche a Europol e Eurojust). Altri strumenti trattano dati personali altamente specializzati che pertengono al loro unico obiettivo: il sistema PNR tratta i dati di prenotazione del volo dei passeggeri; il FIDE i dati rilevanti per le indagini nelle frodi doganali; la direttiva sulla conservazione dei dati gli indirizzi di protocollo Internet (IP) e gli identificatori delle apparecchiature di comunicazione mobili; ECRIS i casellari giudiziali; gli ARO i beni privati e indicazioni sulle imprese, le piattaforme in

materia di criminalità informatica i reati a mezzo Internet; Europol i collegamenti alle reti criminali e il TFTP i dati di messaggistica finanziaria. Lo scambio transfrontaliero di informazioni e di intelligence per le indagini penali costituisce l'unico esempio di una sostanziale sovrapposizione di funzioni. Sul piano giuridico, l'iniziativa svedese sarebbe sufficiente per lo scambio di *qualsiasi* tipo di informazioni rilevanti per tali indagini (purché lo scambio dei dati personali sia ammesso ai sensi della legge nazionale). Da un punto di vista operativo però, la decisione di Prüm potrebbe rivelarsi preferibile per condividere profili DNA e dati relativi alle impronte digitali, in quanto il suo sistema "hit/no hit" assicura risposte istantanee e il metodo di condivisione dei dati automatizzato ne garantisce un livello di sicurezza elevato[82]. Allo stesso modo, può rivelarsi più efficace per le UIF, gli ARO e le piattaforme in materia di criminalità informatica mettersi in contatto diretto con le controparti dell'UE, senza dover compilare i moduli per la richiesta di informazioni previsti dall'iniziativa svedese.

Diritti di accesso controllati

I diritti di accesso agli strumenti ispirati alla logica dell'antiterrorismo e della lotta alle forme gravi di criminalità sono tendenzialmente limitati a un'accezione ristretta di autorità di contrasto (polizia, autorità di frontiera e doganali). I diritti di accesso per strumenti che rispondono alla logica Schengen sono di norma accordati alle autorità competenti per l'immigrazione e, a certe condizione, alla polizia e alle autorità di frontiera e doganali. Il flusso d'informazioni è controllato da interfacce nazionali nel caso dei sistemi centralizzati SIS e VIS e avviene tramite punti di contatto nazionali o unità di coordinamento centrali nel caso di strumenti decentrati quali la decisione di Prüm, l'iniziativa svedese, la convenzione Napoli II, ECRIS, il TFTP, gli accordi PNR, le UIF, gli ARO e le piattaforme in materia di criminalità informatica.

Norme divergenti sulla conservazione dei dati

I dati sono conservati per periodi che variano ampiamente a seconda degli obiettivi dei vari strumenti. L'accordo PNR con gli USA prevede il periodo di conservazione più esteso (15 anni), il sistema API il più breve (24 ore). Gli accordi PNR introducono una distinzione interessante tra uso attivo e passivo dei dati: dopo un determinato periodo, i dati devono essere archiviati e possono essere "sbloccati" solo con una speciale autorizzazione. Ne è un ottimo esempio l'uso canadese dei dati PNR provenienti dall'UE: i dati devono essere resi anonimi dopo 72 ore, ma rimangono a disposizione di funzionari autorizzati per 3 anni e mezzo.

Gestione efficace dell'identità

Molti degli strumenti analizzati finora, compresi il futuro SIS II e il VIS, mirano a consentire la verifica dell'identità tramite i dati biometrici. L'attuazione del SIS dovrebbe rafforzare la sicurezza nello spazio di libertà, sicurezza e giustizia agevolando, ad esempio, l'identificazione di persone per le quali è stato emesso un mandato d'arresto europeo, di coloro a cui è negato l'ingresso nello spazio Schengen e di coloro che sono ricercati per altri motivi

---

[82] Alla decisione di Prüm (decisione 2008/615/GAI del Consiglio, GU L 210 del 6.8.2008, pag. 1) corrisponde una decisione di attuazione (decisione 2008/616/GAI del Consiglio, GU L 210 del 6.8.2008, pag. 12) diretta a garantire l'impiego di tecnologie di punta per assicurare la protezione e la sicurezza dei dati, oltre all'uso della cifratura e di procedure di autorizzazione per accedere ai dati, e contenente norme specifiche che disciplinano l'ammissibilità delle consultazioni.

specifici legati a indagini in corso (persone scomparse o testimoni in giudizio) indipendentemente dalla disponibilità o dall'autenticità dei documenti d'identificazione. L'attuazione del VIS dovrebbe agevolare la procedura di rilascio e gestione dei visti.

Soluzioni dell'UE per la sicurezza dei dati

Per scambiare dati sensibili attraverso i confini europei, gli Stati membri prediligono soluzioni a livello dell'UE. Numerosi strumenti di dimensione, struttura e finalità diverse ricorrono, per la condivisione di dati sensibili, alla rete di trasmissione dati s-TESTA finanziata dalla Commissione. Tra questi, i sistemi centralizzati SIS II, VIS e EURODAC, gli strumenti decentrati Prüm, ECRIS e UIF, Europol e Eurojust. Il SID e il FIDE usano la rete comune di comunicazione, l'interfaccia comune di sistema o l'accesso Internet protetto forniti dalla Commissione. Nel contempo, l'applicazione di rete per lo scambio di informazioni di Europol (SIENA) è diventata l'applicazione preferita per alcune iniziative recenti basate sul trasferimento sicuro di dati: sono in corso discussioni sull'opportunità di rendere operativi la rete FIU.net, gli ARO e le piattaforme di segnalazione dei reati informatici sulla base di tale applicazione.

Meccanismi di revisione diversi

Gli strumenti analizzati contengono una serie di meccanismi di revisione diversi. Nel caso di sistemi d'informazione complessi come il SIS II, il VIS e EURODAC, la Commissione deve presentare al Parlamento europeo e al Consiglio relazioni annuali o biennali sul loro funzionamento o stato di attuazione. Gli strumenti decentrati per lo scambio d'informazioni prevedono invece che la Commissione presenti alle altre istituzioni un'unica relazione di valutazione qualche anno dopo l'attuazione: la direttiva sulla conservazione dei dati, l'iniziativa svedese e gli strumenti ARO devono essere valutati nel 2010, la decisione di Prüm nel 2012 e ECRIS nel 2016. I tre accordi PNR dispongono verifiche periodiche ad hoc, e due di essi contengono anche clausole di caducità. Europol e Eurojust presentano relazioni annuali al Consiglio, che le trasmette per informazione al Parlamento europeo. Queste considerazioni suggeriscono che l'attuale struttura di gestione delle informazioni nell'UE non si presta all'adozione di un meccanismo di valutazione unico per tutti gli strumenti. Proprio per via di questa diversità è fondamentale che eventuali modifiche future degli strumenti nel campo della gestione delle informazioni tengano conto del loro eventuale impatto su tutte le altre misure che disciplinano la raccolta, la conservazione e lo scambio di dati personali nello spazio di libertà, sicurezza e giustizia.

4. PRINCIPI DI ELABORAZIONE DELLE POLITICHE

La sezione 2 descrive le numerose iniziative che la Commissione europea ha attuato, presentato o preso in considerazione negli ultimi anni. Tante idee nuove e un corpus legislativo sempre più vasto nel settore della sicurezza interna e della gestione dell'immigrazione rendono necessario definire un nucleo di principi cardine che presiedano al varo e alla valutazione delle proposte di azione negli anni a venire. Questi principi si reggono, cercando di completarli, sui principi generali sanciti dai trattati, sulla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo e sugli accordi interistituzionali pertinenti tra il Parlamento europeo, il Consiglio e la Commissione europea. Quest'ultima propone di sviluppare e attuare nuove iniziative e di valutare gli strumenti esistenti sulla base delle due serie di principi seguenti.

Principi sostanziali

Salvaguardia dei diritti fondamentali, in particolare del diritto al rispetto della vita privata e alla protezione dei dati

La salvaguardia dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata e alla protezione dei dati personali, sarà la priorità della Commissione nell'elaborare nuove proposte che comportano trattamento di dati personali nel settore della sicurezza interna e della gestione dell'immigrazione. Gli articoli 7 e 8 della Carta proclamano il diritto di ogni persona al "rispetto della propria vita privata e familiare" e alla "protezione dei dati di carattere personale che la riguardano"[83]. L'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE), vincolante nei confronti degli Stati membri, delle istituzioni, degli organi e degli organismi dell'Unione nell'esercizio delle loro attività, riafferma il diritto di ogni persona alla "protezione dei dati di carattere personale che la riguardano"[84]. Nello sviluppare nuovi strumenti basati sull'uso delle tecnologie dell'informazione, la Commissione si impegnerà a seguire l'approccio *privacy by design* (tutela della vita privata fin dalla progettazione). Per questo sarà necessario integrare la protezione dei dati personali nella base tecnologia dello strumento proposto, limitando il trattamento a quanto necessario per conseguire l'obiettivo proposto e garantendo l'accesso solo a determinati organismi in funzione della "necessità di conoscere"[85].

Necessità

L'ingerenza di un'autorità pubblica nel diritto di ciascuno al rispetto della vita privata può essere una misura necessaria alla sicurezza nazionale, alla pubblica sicurezza e alla prevenzione dei reati[86]. La giurisprudenza della Corte europea dei diritti dell'uomo stabilisce tre condizioni che giustificano tali restrizioni: se sono previste dalla legge, se perseguono un obiettivo legittimo e se sono necessarie in una società democratica. L'ingerenza nell'esercizio del diritto al rispetto della vita privata è considerata necessaria se risponde a un'esigenza sociale impellente, se è proporzionata all'obiettivo perseguito e se le ragioni avanzate dall'autorità pubblica per giustificarla risultano pertinenti e sufficienti[87]. In tutte le proposte future, la Commissione valuterà l'impatto stimato dell'iniziativa sul diritto di ciascuno al rispetto della vita privata e alla protezione dei dati personali e preciserà perché tale impatto è necessario e per quale motivo la soluzione proposta è proporzionata all'obiettivo legittimo del mantenimento della sicurezza interna nell'Unione europea, della prevenzione dei reati o della gestione dell'immigrazione. In ogni caso, il rispetto delle norme sulla protezione dei dati personali sarà subordinato al controllo di un'autorità indipendente a livello nazionale o a livello dell'UE.

---

83 Carta dei diritti fondamentali dell'Unione europea (GU C 83 del 30.3.2010, pag. 389).

84 Versioni consolidate del trattato sull'Unione europea e del trattato sul funzionamento dell'Unione europea (GU C 83 del 30.3.2010.2008, pag. 1).

85 Per una descrizione esaustiva del principio della "privacy by design" si veda il parere del Garante europeo della protezione dei dati relativo alla promozione della fiducia nella società dell'informazione mediante il rafforzamento della protezione dei dati e della privacy (*Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*) del 18.3.2010.

86 Si veda l'articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (STE n. 5), Consiglio d'Europa, 4.11.1950.

87 Si veda la sentenza *Marper v United Kingdom* della Corte europea dei diritti dell'uomo, Strasburgo, 4.12.2008.

Sussidiarietà

La Commissione provvederà a motivare le sue nuove proposte alla luce dei principi di sussidiarietà e di proporzionalità, in linea con l'articolo 5 del protocollo n. 2 allegato al trattato sull'Unione europea. Ogni nuova proposta legislativa sarà accompagnata da una scheda contenente elementi circostanziati che consentano di valutare il rispetto dei principi di sussidiarietà, come prevede l'articolo 5 del trattato sull'Unione europea. Tale scheda fornirà elementi che consentiranno di valutare l'impatto finanziario, economico e sociale della proposta e le conseguenze, quando si tratta di una direttiva, sulla regolamentazione che sarà attuata dagli gli Stati membri[88]. Le ragioni che hanno portato a concludere che un obiettivo dell'Unione può essere conseguito meglio a livello UE saranno confortati da indicatori qualitativi. Le proposte legislative terranno conto della necessità che gli oneri che ricadono sull'UE, sui governi nazionali, sugli enti regionali, sugli operatori economici e sui cittadini il meno gravosi possibile e commisurati all'obiettivo da conseguire. Nel caso di proposte di nuovi accordi internazionali, tale scheda prenderà in considerazione l'impatto stimato della proposta sui rapporti con i paesi terzi interessati.

Attenta gestione del rischio

Di norma le informazioni nel settore della libertà, della sicurezza e della giustizia vengono scambiate per analizzare le minacce alla sicurezza, identificare i trend delle attività criminali o valutare i rischi nei settori correlati[89]. Spesso, ma non necessariamente, il rischio è legato a persone il cui comportamento o schema di comportamento nel passato è indice di un rischio che permane nel futuro. Tuttavia, il rischio dovrebbe basarsi su elementi di fatto e non su ipotesi. Qualsiasi misura di gestione dell'informazione presuppone una verifica della necessità e la limitazione delle finalità. L'elaborazione di profili di rischio – da non confondersi con la profilazione su base razziale o altrimenti discriminatoria, incompatibile con i diritti fondamentali – assume particolare importanza. Detti profili possono rivelarsi utili per concentrare le risorse su determinate persone allo scopo di individuare minacce alla sicurezza e proteggere le vittime della criminalità.

Principi orientati al processo[90]

Efficacia economica

I servizi pubblici basati sulla tecnologia dell'informazione dovrebbero consentire di prestare ai contribuenti servizi migliori e a prezzi più convenienti. Alla luce dell'attuale situazione economica, tutte le nuove proposte, specie quelle per la creazione o l'upgrade dei sistemi d'informazione, tenderanno a garantire la maggiore efficacia economica possibile. Questo approccio terrà conto delle soluzioni preesistenti in modo da ridurre al minimo le sovrapposizioni e massimizzare le eventuali sinergie. La Commissione valuterà se sia possibile conseguire gli obiettivi di una proposta tramite un uso ottimale degli strumenti esistenti e se sia opportuno aggiungere funzioni ausiliarie agli attuali sistemi d'informazione prima di proporne di nuovi.

---

88 I principi fondamentali delle valutazioni d'impatto figurano negli orientamenti per la valutazione d'impatto della Commissione europea (*Impact Assessment Guidelines* - SEC(2009)92 del 15.1.2009).

89 Esempi pratici di rischi gestiti con successo: impedire a chi è stato espulso per avere commesso un reato grave in uno Stato membro di rientrare nello spazio Schengen passando da un altro Stato membro (SIS); impedire di presentare domanda di asilo in più Stati membri (EURODAC).

90 Questi principi si ispirano alle conclusioni del Consiglio relative a una strategia di gestione delle informazioni per la sicurezza interna dell'UE, Consiglio "Giustizia e affari interni" del 30.11.2009.

Elaborazione delle politiche "dal basso"

Nell'elaborare nuove iniziative è essenziale tenere conto, sin dalle primissime fasi, del contributo di tutte le parti interessate, a cominciare dalle autorità nazionali competenti per l'attuazione, dagli operatori economici e dalla società civile. Sviluppare politiche che tengano conto degli interessi dei destinatari finali richiede una riflessione orizzontale e una consultazione di ampio respiro[91]. Per questo motivo, la Commissione intende allacciare contatti permanenti con funzionari e professionisti nazionali nell'ambito delle strutture del Consiglio, di comitati di gestione e formazioni ad hoc.

Ripartizione chiara delle responsabilità

In considerazione della complessità tecnica dei progetti di raccolta e scambio d'informazioni nel settore della libertà, della sicurezza e della giustizia, occorre prestare particolare attenzione alla configurazione iniziale delle strutture di governance. L'esperienza del progetto SIS II ha dimostrato che se non si definiscono sin dall'inizio obiettivi generali, regole e responsabilità chiare e stabili, si rischia di andare incontro a sovraccosti e ritardi nell'attuazione. Da una prima valutazione dell'attuazione della decisione di Prüm risulta che una struttura di governance decentrata non è sempre la soluzione, in quanto non esiste un responsabile di progetto cui gli Stati membri possano rivolgersi per consulenze sugli aspetti finanziari o tecnici dell'attuazione. Probabilmente la nuova agenzia IT sarà in grado di offrire ai gestori dei sistemi d'informazione nello spazio di libertà, sicurezza e giustizia questa consulenza tecnica e anche una piattaforma per una più ampia partecipazione delle parti interessate alla gestione operativa e allo sviluppo dei sistemi IT. Per ovviare ai sovraccosti e ritardi dovuti alla modifica dei requisiti, prima di sviluppare qualsiasi nuovo sistema d'informazione nello spazio di libertà, sicurezza e giustizia, in particolare se è un sistema IT su larga scala, bisognerà attendere l'adozione definitiva degli strumenti giuridici fondamentali che ne definiscono l'obiettivo, l'ambito di applicazione, le funzioni e le caratteristiche tecniche.

Clausole di revisione e caducità

La Commissione valuterà ogni strumento descritto in questa comunicazione. Tale valutazione riguarderà tutta la gamma di strumenti esistenti nel campo della gestione delle informazioni e traccerà un quadro affidabile delle modalità con cui i singoli strumenti si inseriscono nel panorama più ampio della sicurezza interna e della gestione dell'immigrazione. Le proposte future prevedranno, dove opportuno, l'obbligo di presentare relazioni annuali, revisioni periodiche ad hoc e clausole di caducità. Gli attuali strumenti saranno mantenuti solo se continueranno a perseguire l'obiettivo legittimo per cui sono stati ideati. Per ogni strumento oggetto della presente comunicazione, l'allegato II fissa la data e il meccanismo di revisione.

5. PROSPETTIVE FUTURE

La presente comunicazione è la prima sintesi, chiara e completa, delle misure dell'UE, vigenti o in fase di attuazione o di esame, che disciplinano la raccolta, la conservazione o lo scambio transfrontaliero di informazioni personali a fini di contrasto o di gestione dell'immigrazione.

---

[91] I principi generali e i requisiti minimi per la consultazione pubblica sono esposti nel documento COM(2002)704 dell'11.12.2002.

È una panoramica, a uso dei cittadini, del tipo di dati personali raccolti, conservati o scambiati e del fine per cui vengono effettuate queste operazioni, e da chi. È uno strumento di riferimento trasparente per quanti intendano partecipare al dibattito sulla direzione che dovrà prendere in futuro la politica dell'UE in questo settore. La presente comunicazione è però anche una prima risposta all'invito del Consiglio europeo a sviluppare strumenti di gestione delle informazioni a livello UE in conformità della strategia di gestione delle informazioni per la sicurezza interna dell'UE[92] e a riflettere sulla necessità di adottare un modello europeo di scambio delle informazioni[93].

La Commissione intende dare seguito al presente documento con una comunicazione sul modello europeo di scambio delle informazioni nel 2012[94]. Per questo ha lanciato, nel gennaio 2010, una "mappatura delle informazioni" partendo dalle basi giuridiche e dal funzionamento pratico dello scambio tra Stati membri di informazioni e intelligence in materia penale, di cui dovrà riferire al Consiglio e al Parlamento europeo nel 2011[95].

Per finire, con la presente comunicazione la Commissione espone, per la prima volta, il suo punto di vista sui principi generali cui intende attenersi nello sviluppo futuro degli strumenti di raccolta, conservazione e scambio di dati, principi che varranno altresì per la valutazione degli strumenti esistenti. La Commissione ritiene infatti che, applicando un approccio di elaborazione e valutazione delle politiche basato su principi, aumenteranno la coerenza e l'efficacia degli strumenti attuali e futuri nel pieno rispetto dei diritti fondamentali dei cittadini.

---

92 Conclusioni del Consiglio su una strategia di gestione delle informazioni per la sicurezza interna dell'UE, Consiglio "Giustizia e affari interni" del 30.11.2009 (*EU Information Management Strategy*).

93 Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini, documento del Consiglio n. 5731/10 del 3.3.2010, punto 4.2.2.

94 Come indicato nel piano d'azione per l'attuazione del programma di Stoccolma (COM(2010) 171 del 20.4.2010).

95 Questa mappatura delle informazioni è effettuata in stretta collaborazione con un gruppo ad hoc composto da rappresentanti degli Stati membri dell'UE e dell'EFTA, di Europol, Eurojust, Frontex e del Garante europeo della protezione dei dati.

ALLEGATO I

I dati e gli esempi seguenti illustrano il funzionamento pratico delle attuali misure di gestione delle informazioni.

Sistema d'informazione Schengen (SIS)

Numero complessivo di segnalazioni SIS introdotte nella banca dati SIS centrale (C.SIS)[96]

Categorie di segnalazioni	**2007**	**2008**	**2009**
Banconote	177,327	168,982	134,255
Documenti vergini	390,306	360,349	341,675
Armi da fuoco	314,897	332,028	348,353
Documenti emessi	17,876,227	22,216,158	25,685,572
Veicoli	3,012,856	3,618,199	3,889,098
Persone ricercate (alias)	299,473	296,815	290,452
Persone ricercate (nome principale)	859,300	927,318	929,546
di cui:			
persone ricercate per arresto ai fini di estradizione	19 119	24 560	28 666
cittadini di paesi terzi colpiti da divieto di ingresso	696,419	746,994	736 868
adulti scomparsi	24 594	23 931	26 707
minori scomparsi	22 907	24 628	25 612
testimoni o persone citate a comparire dinanzi all'autorità giudiziaria	64 684	72 958	78 869
persone soggette a monitoraggio straordinario per prevenire minacce alla pubblica sicurezza	31 568	34 149	32 571
persone soggette a monitoraggio straordinario per prevenire minacce alla sicurezza dello Stato	9	98	253
Totale	**22 933 370**	**27 919 849**	**31 618 951**

[96] Documenti del Consiglio n. 6162/10 del 5.2.2010, n. 5764/10 del 28.1.2009 e n. 5441/08 del 30.1.2008.

EURODAC – Movimenti di richiedenti asilo che hanno presentato nuove domande nello stesso o in altri Stati membri (2008)

Stati membri che hanno inviato impronte digitali ai fini di confronto e ottenuto risposte pertinenti da Stati membri (colonne) in cui l'interessato aveva già presentato domanda d'asilo	Stato membro in cui è stata presentata la prima domanda[97]																													Totale seconde domande	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	Risposte pertinenti locali	Totale risposte pertinenti
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Totale prime domande	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

[97] COM(2009) 494 del 25.9.2009. "Risposta pertinente locale" indica la presentazione di una nuova domanda d'asilo nello stesso Stato membro in cui è stata introdotta la domanda precedente.

Sistema di trasmissione anticipata dei dati relativi alle persone trasportate (API)

Ricorso del Regno Unito al sistema API per migliorare il controllo alle frontiere e lottare contro l'immigrazione illegale[98]	
Numero di azioni nel 2009	
Antecedenti sfavorevoli (ingresso rifiutato)	379
Passaporti persi, rubati o annullati (documento ritirato)	56

[98] Informazioni fornite alla Commissione, ai fini della presente comunicazione, dalla *UK Border Agency* (Agenzia britannica per le frontiere).

Sistema d'informazione doganale (SID)

Numero totale di casi registrati nella banca dati SID (2009)[99]	
Azione	**SID (in base alla convenzione SID)**
Casi aperti	2 007
Casi in corso	274
Casi consultati	11 920
Casi cancellati	1 355

[99] Informazioni fornite dalla Commissione.

Iniziativa svedese

Esempi di ricorso all'iniziativa svedese per indagare su reati[100]	
Omicidio	Nel 2009 un tentativo di omicidio ha luogo nella capitale di uno Stato membro. La polizia raccoglie un campione biologico da un bicchiere da cui il sospetto ha bevuto. La scientifica ne estrae il DNA e stabilisce un profilo genetico ma dal confronto con altri profili di riferimento nella banca dati DNA nazionale non emerge nessun riscontro positivo. Gli investigatori, attraverso il loro punto di contatto Prüm, inviano una domanda di confronto con altri profili DNA di riferimento conservati in altri Stati membri autorizzati a scambiare tali dati in base alla decisione di Prüm o all'accordo di Prüm. Il confronto transfrontaliero dà una segnalazione positiva (hit). In base all'iniziativa svedese, gli investigatori chiedono altri dati sul sospetto. Il loro punto di contatto nazionale riceve le risposte da altri Stati membri nell'arco di 36 ore e la polizia riesce a identificare il sospetto.
Stupro	Nel 2003 un sospetto non identificato stupra una donna. La polizia raccoglie campioni dalla vittima ma il profilo DNA ricostruito non corrisponde ad alcun profilo di riferimento nella banca dati DNA nazionale. Una richiesta di confronto di DNA, inviata dal punto di contatto Prüm ad altri Stati membri autorizzati a scambiare profili DNA di riferimento in base alla decisione di Prüm o all'accordo di Prüm, dà una segnalazione positiva. Gli investigatori chiedono altre informazioni sul sospetto in base all'iniziativa svedese. Il loro punto di contatto nazionale riceve le risposte nell'arco di otto ore, cosa e la polizia riesce a identificare il sospetto.

[100] Informazioni fornite alla Commissione, ai fini della presente comunicazione, dalle forze di polizia di uno Stato membro.

Risposte positive, per tipo di reato, ottenute dalla Germania nell'ambito del confronto transfrontaliero di profili DNA (2009)[101]

Risposte positive per tipo di reato	**Austria**	**Spagna**	**Lussemburgo**	**Paesi Bassi**	**Slovenia**
Reati contro il pubblico interesse	32	4	0	5	2
Reati contro la libertà personale	9	3	5	2	0
Reati sessuali	40	22	0	31	4
Reati contro la persona	49	24	0	15	2
Altri reati	3 005	712	18	1 105	71

[101] Risposta del governo tedesco all'interrogazione parlamentare di Ulla Jelpke, Inge Höger e Jan Korte (riferimento n. 16/14120), Bundestag, 16a sessione, riferimento n. 16/14150 del 22.10.2009. Le cifre riguardano il periodo che va a quando lo Stato membro ha cominciato lo scambio di dati con la Germania fino al 30 settembre 2009.

Esempi di reati gravi scoperti negli Stati membri grazie alla conservazione dei dati[102]	
Omicidio premeditato	Le autorità di polizia di uno Stato membro riescono a risalire ai responsabili dell'omicidio di sei persone per motivi razziali. Gli autori del reato cercano di sottrarsi alla cattura cambiando le rispettive carte SIM ma sono traditi dall'elenco delle chiamate e dall'identificativo dei cellulari.
Omicidio	Le autorità di polizia riescono a dimostrare il coinvolgimento di due persone sospettate d'omicidio analizzando i dati relativi al traffico del cellulare della vittima. Gli investigatori ricostruiscono infatti, sulla base di questi dati, il percorso fatto insieme dalla vittima e dai due sospetti.
Furto con scasso	Le autorità risalgono all'autore di 17 furti con scasso analizzando i dati del traffico della sua carta SIM prepagata, anonima. Identificandone la ragazza, localizzano anche il ladro.
Frode	Gli investigatori sventano la truffa di una gang che vende macchine di lusso "in contanti" su Internet e sistematicamente rapina gli acquirenti al momento della consegna dell'auto. Grazie a un indirizzo IP la polizia rintraccia l'abbonato e arresta i truffatori.

[102] Gli esempi riportati sono anonimi e mutuati dalle risposte date dagli Stati membri a un questionario della Commissione del 2009 riguardante il recepimento della direttiva 2006/24/CE (direttiva sulla conservazione dei dati).

Cooperazione tra unità di informazione finanziaria (UIF)

Totale delle richieste di informazioni inoltrate dalle UIF nazionali via FIU.net[103]		
Anno	**Richieste di informazioni**	**Utilizzatori attivi**
2007	3 133	12 Stati membri
2008	3 084	13 Stati membri
2009	3 520	18 Stati membri

[103] Dati forniti alla Commissione dall'ufficio FIU.net ai fini della presente comunicazione.

Cooperazione tra gli uffici per il recupero dei beni (ARO)

Richieste di reperimento di beni presentate dagli Stati membri e trattate da Europol[104]

Anno	**2004**	**2005**	**2006**	**2007**
Richieste	5	57	53	133
di cui:				
casi di frode				29
casi di riciclaggio di denaro				26
casi legati agli stupefacenti				25
casi legati ad altri reati				18
casi legati agli stupefacenti e al riciclaggio di denaro				19
casi legati alla frode e al riciclaggio di denaro				7
casi legati a una combinazione di più reati				9

Casi di confisca di beni trattati da Eurojust (2006-2007)[105]

Tipi di casi		**Casi avviati da**	
Reati contro l'ambiente	1	Germania	27%
Partecipazione ad organizzazioni criminali	5	Paesi Bassi	21%
Traffico di stupefacenti	15	Regno Unito	15%
Frode fiscale	8	Finlandia	13%
Frode	8	Francia	8%
Frode all'IVA	1	Spagna	6%
Riciclaggio di denaro	9	Portogallo	4%
Corruzione	1	Svezia	2%
Reati contro il patrimonio	2	Danimarca	2%
Traffico d'armi	1	Lettonia	2%
Contraffazione e pirateria	2		
Frode sui pagamenti anticipati	2		
Falsificazione di atti amministrativi	1		
Traffico di autoveicoli rubati	1		
Terrorismo	1		
Falsificazione	2		
Traffico di esseri umani	1		

104 *Assessing the effectiveness of EU Member States' practices in the identification, tracing, freezing and confiscation of criminal assets – Final Report* (per la Commissione europea, DG JLS), Matrix Insight, giugno 2009.

105 Ibid.

Piattaforme di segnalazione dei reati informatici

Esempi di indagini della piattaforma francese di segnalazione dei reati informatici Pharos[106]	
Pedopornografia	Un utente di Internet informa Pharos dell'esistenza di un blog contenente fotografie e immagini tipo disegno animato di sfruttamento sessuale di minori. L'editore del blog, che appare nudo in una foto, si serve del blog per adescare minori. Gli investigatori individuano come principale sospetto un insegnante di matematica nella cui abitazione sono rinvenuti, a seguito di una perquisizione, 49 video contenenti immagini pedopornografiche. Dalle indagini emerge inoltre che il sospetto sta organizzando lezioni a domicilio. L'indagato è riconosciuto colpevole e condannato a una pena di reclusione con condizionale.
Sfruttamento sessuale di minori	La polizia francese riceve la segnalazione di un individuo che offre denaro su Internet in cambio di rapporti sessuali con minori. Un investigatore Pharos, facendosi passare per un minorenne, stabilisce un contatto con il sospetto che effettivamente gli propone denaro in cambio di prestazioni sessuali. La successiva chat su Internet permette a Pharos di individuare l'indirizzo IP del sospetto e di localizzarlo in una città nota per l'alto tasso di sfruttamento sessuale dei minori. L'indagato è riconosciuto colpevole ed condannato a una pena di reclusione con la condizionale.

[106] Pharos sta per *Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*.

Europol

Esempi del contributo di Europol alla lotta contro le forme gravi di criminalità transfrontaliera[107]	
Operazione Andromeda	Nel dicembre 2009 Europol partecipa a una vasta operazione di polizia transfrontaliera contro una rete di traffico di stupefacenti con addentellati in 42 paesi. La rete ha base in Belgio e in Norvegia e smercia droga dal Perù, attraverso i Paesi Bassi, in Belgio, Regno Unito, Italia ed altri Stati. La cooperazione di polizia è coordinata da Europol; la cooperazione giudiziaria da Eurojust. Le autorità partecipanti predispongono un ufficio mobile a Pisa, ed Europol organizza un centro operativo all'Aia. Europol procede a confronti incrociati di informazioni fra i sospetti e stila un rapporto che descrive la rete criminale.
Partecipanti	Italia, Paesi Bassi, Germania, Belgio, Regno Unito, Lituania, Norvegia ed Eurojust.
Risultati	Le forze di polizia che partecipano all'operazione sequestrano 49 kg di cocaina, 10 kg di eroina, 6 000 pasticche di ecstasy, due armi da fuoco, cinque documenti di identità falsi e 43 000 euro in contanti, e procedono all'arresto di 15 persone.
Operazione Typhoon	Fra l'aprile 2008 e il febbraio 2010 Europol fornisce supporto analitico alle forze di polizia di 20 paesi partecipanti all'operazione Typhoon. In questa azione su larga scala contro una rete di pedofili che diffonde immagini a contenuto pedopornografico attraverso un sito web austriaco, Europol si incarica del supporto tecnico e dell'analisi di intelligence criminale in base alle immagini ricevute dall'Austria, quindi valuta l'affidabilità dei dati e li ristruttura prima di preparare il proprio materiale di intelligence. Procedendo a confronti incrociati dei dati con le informazioni contenute nel suo archivio di lavoro per fini di analisi, produce 30 relazioni d'intelligence dando il via ad indagini in vari paesi.
Partecipanti	Austria, Belgio, Bulgaria, Canada, Danimarca, Francia, Germania, Ungheria, Italia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Romania, Slovacchia, Slovenia, Spagna, Svizzera e Regno Unito.
Risultati	Le forze di polizia identificano 286 sospetti e arrestano 118 presunti pedofili, salvando cinque vittime di abusi in quattro paesi.

[107] Informazioni di Europol alla Commissione ai fini della presente comunicazione. Ulteriori dati sull'operazione Andromeda all'indirizzo http://www.eurojust.europa.eu/.

Esempi del coordinamento di Eurojust di vaste operazioni giudiziarie transfrontaliere contro forme gravi di criminalità[108]	
Tratta di esseri umani e finanziamento del terrorismo	Nel maggio 2010 Eurojust coordina un'operazione transfrontaliera che sfocia nell'arresto di cinque membri di una rete di criminalità organizzata attiva in Afghanistan, Pakistan, Romania, Albania e Italia. Il gruppo procura documenti falsi a cittadini afgani e pakistani e li fa arrivare in Italia dall'Iran, dalla Turchia e dalla Grecia. Dall'Italia gli immigrati sono poi mandati in Germania, Svezia, Belgio, Regno Unito e Norvegia. I proventi della tratta sono destinati al finanziamento del terrorismo.
Frodi a carte bancarie	Coordinando la cooperazione di polizia e giudiziaria transfrontaliera, Europol e Eurojust contribuiscono a smantellare una rete di frodi con carte bancarie in Irlanda, Italia, Paesi Bassi, Belgio e Romania. La rete possiede gli identificativi di circa 15 000 carte di pagamento, causando perdite per 6,5 milioni di euro. In previsione di questa operazione, che nel luglio del 2009 porta a 24 arresti, magistrati belgi, irlandesi, italiani, olandesi e rumeni collaborano per l'emissione di mandati d'arresto europei e l'autorizzazione di intercettazione telefonica dei sospetti.
Tratta di esseri umani e traffico di stupefacenti	A seguito di una riunione di coordinamento organizzata da Eurojust nel marzo 2009, le autorità italiane, olandesi e colombiane arrestano 62 individui sospettati di tratta di esseri umani e traffico di stupefacenti. La rete fa arrivare donne vulnerabili dalla Nigeria nei Paesi Bassi, obbligandole poi a prostituirsi in Italia, Francia e Spagna. Con i proventi della prostituzione la rete acquista cocaina in Colombia, destinata al consumo nell'UE.

[108] Esempi tratti da http://www.eurojust.europa.eu/.

Dati del codice di prenotazione (PNR)

Esempi di analisi PNR che hanno permesso di ottenere informazioni nell'ambito di indagini relative a forme gravi di criminalità transfrontaliera[109]	
Tratta di minori	Da analisi PNR emerge che tre minori non accompagnati sono in viaggio da uno Stato membro dell'UE verso un paese terzo senza indicazione dell'adulto che dovrà accoglierli all'arrivo. Allertate dalla polizia dello Stato membro dopo la partenza, le autorità del paese terzo arrestano la persona che si presenta per prendere in consegna i bambini: un delinquente sessuale schedato nello Stato membro.
Tratta di esseri umani	Analisi PNR permettono di smascherare un gruppo di trafficanti di esseri umani attivo sempre sulla stessa rotta che si serve di documenti falsi per il check-in di un volo intra-UE e di documenti autentici per effettuare in contemporanea il check-in su un altro volo a destinazione di un paese terzo. Una volta nella sala d'attesa dell'aeroporto, la prassi era imbarcarsi sul volo interno UE.
Frodi a carte di credito	Più famiglie viaggiano a destinazione di uno Stato membro esibendo biglietti acquistati con carte di credito rubate. Dalle indagini emerge che un'organizzazione criminale usa queste carte per acquistare biglietti che rivende successivamente nei call-center. Grazie ai dati PNR è stato possibile ricollegare i viaggiatori alle carte di credito e ai venditori.
Traffico di stupefacenti	Le autorità di polizia di uno Stato membro hanno informazioni su un uomo che sarebbe implicato nel traffico di stupefacenti da un paese terzo senza però riuscire mai a coglierlo in flagrante al suo arrivo nell'UE. Da analisi PNR emerge che l'uomo viaggia sempre con un socio. Questi viene perquisito e trovato in possesso di grosse quantità di stupefacenti.

[109] Esempi resi anonimi per proteggere le fonti di informazione.

Esempi di informazioni raccolte nell'ambito del TFTP a fini di indagini relative ad attentati terroristici[110]	
Attentato terroristico di Barcellona (2008)	Nel gennaio 2008 a Barcellona dieci persone sono arrestate a seguito di un tentativo di attentato sventato ai trasporti pubblici della città. Per individuare i legami dei sospetti con l'Asia, l'Africa e il Nord America sono utilizzati dati TFTP.
Attentato con esplosivi liquidi su voli transatlantici (2006)	Vengono usate informazioni TFTP per le indagini e la condanna di persone implicate nel tentativo, sventato, di far esplodere, nell'agosto del 2006, dieci voli per gli USA e il Canada in partenza dal Regno Unito.
Attentati di Londra (2005)	Vengono usati dati TFTP per fornire nuove piste agli investigatori, confermare le identità dei sospetti e mettere in luce i rapporti fra i responsabili degli attacchi.
Attentati di Madrid (2004)	A vari Stati membri vengono trasmessi dati TFTP per aiutarli nelle indagini avviate a seguito degli attentati.

[110] Seconda relazione sul trattamento dei dati personali provenienti dall'UE da parte del Dipartimento del Tesoro degli Stati Uniti per fini di antiterrorismo, giudice Jean-Louis Bruguière, gennaio 2010.

ALLEGATO II

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Sistema d'informazione Schengen (SIS)	Iniziativa degli Stati membri	Preservare la sicurezza pubblica, compresa la sicurezza dello Stato, all'interno dello spazio Schengen, e facilitare la circolazione delle persone usando informazioni comunicate attraverso lo stesso sistema.	Centralizzata: N.SIS (sistema nazionale) collegato da un'interfaccia al C.SIS (sistema centrale)	Nomi e alias, segni fisici particolari, data e luogo di nascita, cittadinanza e se la persona è armata o violenta. Le segnalazioni SIS riguardano diversi gruppi di persone.	La polizia, la polizia di frontiera e le autorità doganali e giudiziarie hanno accesso a tutti i dati. Le autorità competenti per l'immigrazione e le autorità consolari hanno accesso all'elenco delle persone soggette a divieto d'ingresso e alle segnalazioni sui documenti persi o rubati. Europol e Eurojust possono accedere ad alcuni dati.	Convenzione del Consiglio d'Europa (CdE) n. 108 e raccomandazione R (87) 15 del CdE nel settore della polizia.	I dati personali inseriti nel SIS ai fini della ricerca di persone possono essere conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti, e non oltre tre anni dopo il loro inserimento. I dati sulle persone soggette a monitoraggio straordinario in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato devono essere cancellati dopo un anno.	Il SIS è pienamente applicabile in 22 Stati membri, più Svizzera, Norvegia e Islanda. Il Regno Unito e l'Irlanda partecipano al SIS, fatta eccezione per le segnalazioni relative ai cittadini di paesi terzi iscritti nell'elenco delle persone soggette a divieto di ingresso. Bulgaria, Romania e Liechtenstein dovrebbero attuare il sistema prossimamente.	I firmatari possono proporre di modificare la convenzione Schengen. Il testo modificato deve essere adottato all'unanimità e ratificato dai parlamenti.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Sistema d'informazione Schengen II (SIS II)	Iniziativa della Commissione	Assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia e agevolare la circolazione delle persone grazie alle informazioni comunicate attraverso il sistema.	Centralizzata: N.SIS II (sistema nazionale) collegato da un'interfaccia al C.SIS (sistema centrale). Il SIS II funzionerà sulla rete protetta s-TESTA.	Le categorie di dati del SIS più impronte digitali e fotografie, copie di mandati di arresto europei, segnalazioni di identità usurpate e connessioni fra diverse segnalazioni. Le segnalazioni SIS II riguardano gruppi di persone diversi.	La polizia, la polizia di frontiera e le autorità doganali e giudiziarie avranno accesso a tutti i dati. Le autorità competenti per l'immigrazione e le autorità consolari avranno accesso all'elenco delle persone soggette a divieto d'ingresso e alle segnalazioni sui documenti persi o rubati. Europol e Eurojust potranno accedere ad alcuni dati.	Norme specifiche stabilite negli strumenti giuridici che disciplinano il SIS II, e direttiva 95/46/CE, regolamento (CE) n. 45/2001, decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e raccomandazione R (87) 15 del CdE nel settore della polizia.	I dati personali inseriti nel SIS ai fini della ricerca di persone possono essere conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti, e non oltre tre anni dopo il loro inserimento. I dati sulle persone soggette a monitoraggio straordinario in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato devono essere cancellati dopo un anno.	Il SIS II è in fase di attuazione. Una volta in funzione, sarà applicabile nell'UE-27, in Svizzera, Liechtenstein, Norvegia e Islanda. Il Regno Unito e l'Irlanda parteciperanno al SIS II, fatta eccezione per le segnalazioni relative ai cittadini di paesi terzi iscritti nell'elenco delle persone soggette a divieto di ingresso.	La Commissione deve presentare ogni due anni al Parlamento europeo (PE) e al Consiglio una relazione di avanzamento concernente lo sviluppo del SIS II e la potenziale migrazione dal SIS.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
EURODAC	Iniziativa della Commissione	Concorrere alla determinazione dello Stato membro competente per l'esame di una domanda d'asilo.	Centralizzata, consistente in punti d'accesso nazionali collegati da un'interfaccia all'unità centrale EURODAC. EURODAC funziona sulla rete s-TESTA.	Impronte digitali, sesso, luogo e data della domanda d'asilo, numero di riferimento usato dallo Stato membro d'origine e data in cui le impronte digitali sono state rilevate, trasmesse e inserite nel sistema.	Gli Stati membri devono comunicare l'elenco delle autorità che hanno accesso ai dati, ossia di norma le autorità competenti per l'asilo e l'immigrazione, le guardie di frontiera e la polizia.	Direttiva 95/46/CE	Impronte digitali dei richiedenti asilo: 10 anni. Impronte digitali di cittadini di paesi terzi fermati in relazione all'attraversamento irregolare di una frontiera esterna: 2 anni.	Il regolamento EURODAC è in vigore in tutti gli Stati membri e in Norvegia, Islanda e Svizzera. Per quanto riguarda il Liechtenstein, si è in attesa della conclusione di un accordo che ne autorizza la connessione.	La Commissione deve inviare annualmente al PE e al Consiglio una relazione sull'attività dell'unità centrale di EURODAC.
Sistema d'informazione visti (VIS)	Iniziativa della Commissione	Migliorare l'attuazione della politica comune in materia di visti e prevenire minacce alla sicurezza interna.	Centralizzata, costituita da sezioni nazionali che saranno collegate da un'interfaccia alla sezione centrale. Il VIS funzionerà sulla rete s-TESTA.	Domande di visto, impronte digitali, fotografie, decisioni correlate relative ai visti e collegamenti tra domande connesse.	Le autorità per il visto, l'asilo e l'immigrazione e le autorità di controllo alla frontiera hanno accesso a tutti i dati. La polizia ed Europol possono consultare il VIS ai fini di prevenzione, ricerca e accertamento di forme gravi di criminalità.	Norme specifiche stabilite negli strumenti giuridici che disciplinano il VIS, e direttiva 95/46/CE, regolamento (CE) n. 45/2001, decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e relativo protocollo addizionale n. 181 e raccomandazione R (87) 15 del CdE nel settore della polizia.	5 anni	Il VIS è in fase di attuazione e sarà applicabile in tutti gli Stati membri (tranne il Regno Unito e l'Irlanda), in Norvegia, Islanda e Svizzera.	La Commissione deve riferire al PE e al Consiglio in merito al funzionamento del VIS tre anni dopo la sua entrata in funzione e in seguito ogni quattro anni.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Sistema di trasmissione anticipata dei dati relativi alle persone trasportate (API)	Iniziativa della Spagna	Migliorare i controlli alle frontiere e combattere l'immigrazione illegale.	Decentrata	Dati personali figuranti sul passaporto; punto d'imbarco e valico d'ingresso nell'UE.	Autorità di controllo alla frontiera e, su richiesta, autorità di contrasto.	Direttiva 95/46/CE	I dati devono essere cancellati entro le 24 ore seguenti l'arrivo del volo nell'UE.	API è in vigore in tutti gli Stati membri, ma solo in pochi lo usano.	La Commissione valuterà il sistema API nel 2011.
Convenzione Napoli II	Iniziativa degli Stati membri	Permettere alle autorità doganali nazionali di prevenire e accertare le violazioni delle disposizioni doganali nazionali, e aiutarle a perseguire e punire le violazioni delle disposizioni doganali comunitarie e nazionali.	Decentrata, funziona con una serie di uffici di coordinamento centrali.	Qualsiasi informazione concernente una persona identificata o identificabile.	Gli uffici di coordinamento centrali trasmettono i dati alle autorità doganali nazionali, alle autorità nazionali responsabili delle azioni penali e agli organi giurisdizionali nazionali e, previo consenso dello Stato membro che li ha forniti, ad altre autorità.	Direttiva 95/46/CE e convenzione n. 108 del CdE. Lo Stato membro ricevente deve garantire un livello di protezione dei dati almeno equivalente a quello previsto dallo Stato membro che li ha forniti.	I dati possono essere conservati soltanto per il periodo necessario agli scopi della loro comunicazione.	Convenzione ratificata da tutti gli Stati membri.	I firmatari possono proporre di modificare la convenzione Napoli II. Il testo modificato deve essere adottato dal Consiglio e ratificato dagli Stati membri.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Sistema d'informazione doganale (SID)	Iniziativa degli Stati membri	Facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi doganali nazionali.	Centralizzato, accessibile tramite terminali situati in ogni Stato membro e presso la Commissione. Il SID e FIDE funzionano in base ad AFIS, che usa la rete comune di comunicazione, l'interfaccia comune di sistema o l'accesso Internet protetto forniti dalla Commissione.	Nomi e alias, data e luogo di nascita, cittadinanza, sesso, segni particolari, documenti d'identità, indirizzo, segnalazione che la persona ha già fatto uso di violenza, motivo dell'inclusione dei dati nel SID, azione proposta e numero d'immatricolazione del mezzo di trasporto.	Ai dati SID possono accedere le autorità doganali nazionali, Europol ed Eurojust.	Norme specifiche della convenzione SID, direttiva 95/46/CE, regolamento (CE) n. 45/2001, convenzione n. 108 del CdE e raccomandazione R (87) 15 del CdE nel settore della polizia.	I dati personali copiati dal SID in altri sistemi ai fini di gestione dei rischi o di analisi operativa sono memorizzati soltanto per il periodo necessario al raggiungimento dello scopo per cui sono stati copiati, per un massimo di dieci anni.	In vigore in tutti gli Stati membri	La Commissione, in cooperazione con gli Stati membri, presenta al PE e al Consiglio relazioni annuali sul funzionamento del SID.
Iniziativa svedese	Iniziativa della Svezia	Ottimizzare lo scambio di informazioni ai fini di indagini penali ed operazioni di intelligence criminale.	Decentrata: gli Stati membri devono designare punti di contatto nazionali incaricati di trattare le richieste urgenti di informazioni.	Informazioni e intelligence criminale esistenti e accessibili alle autorità di contrasto.	Polizia, autorità doganali e altre autorità competenti a indagare sui reati (ad eccezione dei servizi di intelligence).	Norme nazionali di protezione ei dati, convenzione n. 108 del CdE e relativo protocollo addizionale n. 181 e raccomandazione R (87) 15 del CdE nel settore della polizia.	Le informazioni e l'intelligence ottenute attraverso questo strumento possono essere usate solo per gli scopi per cui sono state fornite e a specifiche condizioni stabilite dallo Stato membro che le ha trasmesse.	12 dei 31 firmatari (Stati UE e EFTA) hanno adottato leggi nazionali di attuazione di questo strumento; cinque compilano periodicamente il modulo per richiedere dati; due lo usano frequentemente per scambiare le informazioni.	La Commissione deve presentare al Consiglio una relazione di valutazione nel 2010.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Decisione di Prüm	Iniziativa degli Stati membri	Potenziare la prevenzione dei reati, in particolare il terrorismo, e mantenere l'ordine pubblico.	Decentrata, interconnessa attraverso la rete s-TESTA. I punti di contatto nazionali trattano le richieste ricevute e inviate per confronto di dati.	Profili DNA anonimi e impronte digitali, dati di immatricolazione veicoli e informazioni su persone sospettate di legami col terrorismo.	I punti di contatto trasmettono le richieste; l'accesso a livello nazionale è disciplinato dalla legislazione nazionale.	Norme specifiche della decisione di Prüm, convenzione n. 108 del CdE e relativo protocollo addizionale n. 181, e raccomandazione R (87) 15 del CdE nel settore della polizia. Gli interessati possono rivolgersi alla rispettive autorità nazionali di protezione dei dati per far valere i propri diritti in ordine al trattamento dei dati personali.	I dati personali devono essere cancellati quando non sono più necessari ai fini per i quali sono stati forniti. Il periodo massimo di conservazione dei dati, a livello nazionale, dello Stato che li fornisce è vincolante per lo Stato che li riceve.	La decisione di Prüm è in fase di attuazione. 10 Stati membri sono stati autorizzati a scambiare dati sul DNA, cinque a scambiare impronte digitali, sette a scambiare dati di immatricolazione veicoli. La Norvegia e l'Islanda stanno aderendo a questo strumento.	La Commissione deve presentare al Consiglio una relazione di valutazione nel 2012.
Direttiva sulla conservazione dei dati	Iniziativa degli Stati membri	Rafforzare l'indagine, l'accertamento e il perseguimento di reati gravi grazie alla conservazione dei dati di telecomunicazione relativi al traffico e all'ubicazione.	Decentrata: questo strumento impone ai fornitori di servizi di telecomunicazioni obblighi in materia di conservazione dei dati.	Numeri di telefono, indirizzi IP e identificativi dell'apparecchiatura mobile.	Le autorità con diritto di accesso sono determinate a livello nazionale.	Direttiva 95/46/CE e direttiva 2002/58/CE.	Dai sei ai 24 mesi	Sei Stati membri non hanno ancora recepito la direttiva e le corti costituzionali di Germania e Romania hanno dichiarato l'incostituzionalità delle leggi nazionali di attuazione.	La Commissione deve presentare al PE e al Consiglio una relazione di valutazione nel 2010.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Sistema europeo di informazione sui casellari giudiziari (ECRIS)	Iniziativa del Belgio e proposta dalla Commissione	Migliorare la condivisione transfrontaliera dei dati relativi ai casellari giudiziari dei cittadini dell'UE.	Decentrata: interconnessione attraverso più autorità centrali che si scambieranno informazioni estratte dai casellari giudiziari usando la rete s-TESTA.	Dati anagrafici, condanna, pena, reato e ulteriori informazioni, tra cui le impronte digitali (se disponibili).	Autorità giudiziarie e autorità amministrative competenti.	Norme specifiche della decisione quadro 2009/315/GAI del Consiglio, che include le norme della decisione 2005/876/GAI del Consiglio, e decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e regolamento (CE) n. 45/2001.	Si applicano le norme nazionali di conservazione dei dati, poiché questo strumento disciplina solo lo scambio di dati.	ECRIS è in fase di attuazione. Nove Stati membri hanno iniziato lo scambio elettronico di informazioni	La Commissione deve presentare al PE e al Consiglio due relazioni di valutazione: una sulla decisione quadro 2008/675/GAI nel 2011; l'altra sulla decisione quadro 2009/315/GAI nel 2015. A partire dal 2016 la Commissione è tenuta a pubblicare relazioni periodiche sul funzionamento della decisione quadro 2009/315/GAI del Consiglio (ECRIS).
Cooperazione fra unità di informazione finanziaria (FIU.net)	Iniziativa dei Paesi Bassi	Scambio delle informazioni necessarie per analisi e indagini su casi di riciclaggio di denaro e finanziamento del terrorismo.	Decentrata: le UIF si scambiano dati attraverso FIU.net, che funziona sulla rete s-TESTA. L'applicazione SIENA di Europol può a breve venire a rafforzare FIU.net.	Tutti i dati pertinenti per analisi o indagini su riciclaggio di denaro e finanziamento del terrorismo.	Unità di informazione finanziaria (presso le autorità di contrasto, le autorità giudiziarie o gli organi amministrativi tenuti a riferire alle autorità finanziarie).	Decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e raccomandazione R (87) 15 del CdE nel settore della polizia.	Si applicano le norme nazionali di conservazione dei dati, poiché questo strumento disciplina solo lo scambio di dati.	20 Stati membri partecipano a FIU.net, un'applicazione on-line per lo scambio di dati che funziona su s-TESTA.	Nell'ambito del piano d'azione per i servizi finanziari, la Commissione sta esaminando l'attuazione della direttiva 2005/60/CE dal 2009.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Cooperazione tra gli uffici per il recupero dei beni (ARO)	Iniziativa degli Stati membri	Scambio delle informazioni necessarie ai fini del reperimento e identificazione dei proventi di reato.	Decentrata: per scambiarsi le informazioni gli ARO devono avvalersi dell'iniziativa svedese. L'applicazione SIENA di Europol potrà presto venire a rafforzare la cooperazione fra gli ARO.	Indicazioni sui beni oggetto dei provvedimenti (ad esempio conti bancari, beni immobili e veicoli) e sulle persone fisiche o giuridiche ricercate (come nomi, indirizzi, informazioni sugli azionisti o sulla società).	Uffici per il recupero dei beni	Convenzione n. 108 del CdE e relativo protocollo addizionale n. 181, e raccomandazione R (87) 15 del CdE nel settore della polizia.	Si applicano le norme nazionali di conservazione dei dati, poiché questo strumento disciplina solo lo scambio di dati.	Oltre 20 Stati membri hanno istituito uffici per il recupero dei beni; 12 stanno partecipando a un progetto pilota che usa l'applicazione SIENA di Europol per scambiare dati utili per il reperimento di beni.	La Commissione deve presentare al Consiglio una relazione di valutazione nel 2010.
Piattaforme nazionali ed europee in materia di criminalità informatica	Iniziativa della Francia	Raccogliere, analizzare e scambiare informazioni sui reati commessi su Internet.	Decentrata: il sistema riunisce le piattaforme nazionali di segnalazione e la piattaforma europea in materia di criminalità informatica di Europol. L'applicazione SIENA di Europol potrà presto venire a rafforzare lo scambio di dati fra le piattaforme di segnalazione.	Contenuti o comportamenti illeciti rilevati su Internet.	Le piattaforme nazionali ricevono le segnalazioni dai cittadini; la piattaforma europea in materia di criminalità informatica di Europol riceve le segnalazioni relative alle forme gravi di reati informatici transfrontalieri dalle autorità di contrasto.	Norme specifiche della decisione Europol e della decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e relativo protocollo addizionale n. 181, raccomandazione R (87) 15 del CdE nel settore della polizia e regolamento (CE) n. 45/2001.	Si applicano le norme nazionali di conservazione dei dati, poiché questo strumento disciplina solo lo scambio di dati.	Quasi tutti gli Stati membri hanno istituito le piattaforme nazionali di segnalazione; Europol sta lavorando alla sua piattaforma europea in materia di criminalità informatica.	In materia di criminalità informatica è competente Europol, che in futuro riferirà delle attività della piattaforma europea in materia di criminalità informatica nella relazione annuale che presenta al Consiglio per approvazione e al Parlamento europeo per informazione.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Europol	Iniziativa degli Stati membri	Assistere gli Stati membri per prevenire e combattere la criminalità organizzata, il terrorismo e altre forme gravi di criminalità che interessano due o più Stati membri.	Europol è un'agenzia UE con sede all'Aia. Sta sviluppando SIENA, la sua applicazione di rete per lo scambio di informazioni protetta.	Il sistema d'informazione Europol (SIE) contiene dati personali, tra cui gli identificatori biometrici, le condanne penali e i legami con la criminalità organizzata di persone indagate per reati di competenza di Europol. Gli archivi di lavoro per fini di analisi (AWF) contengono tutti i dati personali pertinenti.	Possono accedere al SIE le unità nazionali di Europol, gli ufficiali di collegamento, il personale di Europol e il direttore. Agli archivi AWF hanno accesso gli ufficiali di collegamento. I dati personali possono essere scambiati con paesi terzi che hanno concluso accordi con Europol.	Norme specifiche della decisione Europol e della decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e relativo protocollo addizionale n. 181, raccomandazione R (87) 15 del CdE nel settore della polizia e regolamento (CE) n. 45/2001.	Gli archivi AWF possono essere conservati per un periodo massimo di tre anni, prorogabili una sola volta per ulteriori tre anni.	Ricorrono attivamente ad Europol tutti gli Stati membri, così come i paesi terzi con cui ha concluso accordi operativi. La nuova base giuridica di Europol è stata attuata in tutti gli Stati membri.	L'autorità di controllo comune è incaricata di monitorare il trattamento dei dati personali da parte di Europol e la legittimità della loro trasmissione ad altre parti, e trasmette periodicamente rapporti al PE e al Consiglio. Europol presenta inoltre per approvazione al Consiglio e per informazione al PE una relazione annuale sulle proprie attività.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Eurojust	Iniziativa degli Stati membri	Migliorare il coordinamento delle indagini e delle azioni penali tra gli Stati membri e rafforzare la cooperazione tra le autorità nazionali competenti.	Eurojust è un organo dell'UE con sede all'Aia. Per lo scambio di dati usa s-TESTA.	Dati personali di indagati e di autori di reati in caso di forme gravi di criminalità che interessano due o più Stati membri, fra cui dati anagrafici, recapiti, profili DNA, impronte digitali, fotografie, e dati di telecomunicazione relativi al traffico e all'ubicazione.	I 27 membri nazionali di Eurojust, che possono condividere i dati con autorità nazionali e paesi terzi se la fonte delle informazioni è d'accordo.	Norme specifiche della decisione Eurojust e della decisione quadro 2008/977/GAI del Consiglio, convenzione n. 108 del CdE e relativo protocollo addizionale n. 181, e raccomandazione R (87) 15 del CdE nel settore della polizia.	Le informazioni devono essere cancellate una volta raggiunto l'obiettivo per il quale sono fornite e una volta chiuso il caso.	La base giuridica modificata di Eurojust è in fase d'attuazione negli Stati membri.	Entro giugno 2014 la Commissione deve riesaminare gli scambi di dati tra i membri nazionali di Eurojust. Entro giugno 2013 Eurojust dovrà presentare al Consiglio e alla Commissione una relazione sull'esperienza relativa all'accesso a livello nazionale al sistema di gestione dei fascicoli. L'autorità di controllo comune controlla il trattamento dei dati personali da parte di Eurojust e riferisce ogni anno al Consiglio. Il presidente del collegio presenta al Consiglio una relazione annuale sulle attività di Eurojust, che il Consiglio trasmette al PE.

Panorama generale degli strumenti vigenti o in fase di attuazione o di esame

Strumento	Contesto	Finalità	Struttura	Dati personali interessati	Accesso ai dati	Protezione dei dati	Conservazione dei dati	Stato d'attuazione	Revisione
Accordi PNR con Stati Uniti e Australia; accordo API/PNR con il Canada	Iniziativa della Commissione	Prevenire e combattere il terrorismo e altre forme gravi di criminalità transnazionale.	Accordi internazionali	Gli accordi con gli USA e l'Australia contengono 19 categorie di dati, tra cui dati anagrafici, di prenotazione, pagamento e informazioni aggiuntive; l'accordo con il Canada contiene 25 voci simili.	Dipartimento per la sicurezza interna degli Stati Uniti, Agenzia dei servizi di frontiera del Canada e amministrazione doganale australiana, che possono trasferire i dati ad altre autorità di contrasto e antiterrorismo nazionali.	Le norme di protezione dei dati sono stabilite negli specifici accordi internazionali.	Stati Uniti: sette anni di uso attivo, otto anni di uso passivo. Australia: tre anni e mezzo di uso attivo, due anni di uso passivo. Canada: 72 ore di uso attivo, tre anni e mezzo di uso passivo.	Gli accordi USA e Australia sono applicabili in via provvisoria; l'accordo con il Canada è in vigore. La Commissione rinegozierà questi accordi. Sei Stati membri hanno adottato leggi che consentono l'uso dei dati PNR a fini di contrasto.	Ogni accordo è soggetto a verifica periodica; gli accordi canadese e australiano prevedono la denuncia.
Accordo TFTP UE-USA	Iniziativa della Commissione	Prevenzione, indagine, accertamento o azione penale nei confronti del terrorismo o del suo finanziamento.	Accordo internazionale	Dati di messaggistica finanziaria contenenti, tra l'altro, il nome, il numero di conto, l'indirizzo e il numero d'identificazione dell'ordinante e dei beneficiari della transazione finanziaria.	Il Tesoro USA può trasferire i dati personali estratti dai messaggi finanziari alle autorità di contrasto, di pubblica sicurezza o antiterrorismo statunitensi, agli Stati membri UE, a Europol o Eurojust. Il trasferimento a paesi terzi necessita del consenso degli Stati membri.	L'accordo contempla clausole rigorose di limitazione delle finalità e di proporzionalità.	I dati personali estratti dai messaggi finanziari possono essere conservati solo per il tempo necessario a specifiche indagini o azioni penali; i dati non estratti possono essere conservati per un massimo di cinque anni.	Il PE ha approvato la conclusione dell'accordo TFTP UE-USA l'8 luglio 2010. Ora spetta al Consiglio adottare una decisione relativa alla conclusione dell'accordo, dopodiché l'accordo entrerà in vigore mediante uno scambio di lettere tra le parti.	Dopo sei mesi dall'entrata in vigore la Commissione deve procedere alla verifica dell'accordo e presentare al PE e al Consiglio una relazione di valutazione.