



Bruxelles, 7.12.2012  
COM(2012) 735 final

**COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL  
CONSIGLIO**

**Rafforzare la cooperazione in materia di applicazione della legge nell'UE:  
il modello europeo di scambio di informazioni (EIXM)**

# COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

## Rafforzare la cooperazione in materia di applicazione della legge nell'UE: il modello europeo di scambio di informazioni (EIXM)

### 1. INTRODUZIONE

Garantire un elevato livello di sicurezza nell'UE e nello spazio Schengen implica un'azione concertata a livello europeo nella lotta alle reti criminali<sup>1</sup>. Una tale azione è necessaria per affrontare non solo le forme gravi di criminalità organizzata, come la tratta di esseri umani, il traffico di droga o di armi da fuoco, ma anche reati meno gravi commessi su larga scala da gruppi criminali organizzati e mobili, così come i crimini commessi da singoli trasgressori che operano in più Stati membri.

Lo scambio di informazioni tra Stati membri è, in questo contesto, uno strumento fondamentale per le autorità di contrasto della criminalità. Gli accordi internazionali e bilaterali sono stati pertanto integrati da sistemi e strumenti a livello dell'Unione – quali il sistema di informazione Schengen e il sistema di informazione Europol – che sono predisposti in modo da garantire pienamente la tutela della riservatezza e dei dati personali, conformemente alla Carta dei diritti fondamentali. La presente comunicazione traccia un bilancio di **come funziona, oggi, nell'UE lo scambio di informazioni a livello transfrontaliero**, e formula raccomandazioni per eventuali miglioramenti.

La comunicazione giunge alla conclusione che complessivamente lo scambio di informazioni è efficiente, come dimostrano dai risultati positivi riportati di seguito a titolo d'esempio. **Pertanto, non si ravvisa la necessità – a questo stadio – di introdurre a livello dell'UE nuove banche dati o nuovi strumenti per lo scambio di informazioni nel settore della lotta alla criminalità.** Tuttavia, gli attuali strumenti dell'UE potrebbero e dovrebbero essere impiegati meglio, e gli scambi dovrebbero essere organizzati in modo più coerente.

La presente comunicazione formula pertanto raccomandazioni agli Stati membri sulle modalità di **migliorare l'applicazione degli strumenti esistenti e razionalizzare i canali di comunicazione utilizzati**, sottolineando la necessità di **assicurare un elevato livello di qualità, sicurezza e protezione dei dati**. La comunicazione spiega quale sostegno la Commissione intende fornire agli Stati membri, anche **in materia di finanziamenti ed attività di formazione**. In tal senso, propone un modello per orientare le attività dell'UE e degli Stati membri.

La presente comunicazione dà seguito al programma di Stoccolma, che invitava la Commissione a valutare la necessità di sviluppare un modello europeo di scambio delle informazioni basato sulla valutazione degli strumenti esistenti. Essa si basa sulla comunicazione della Commissione del 2010, che illustrava un "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia" (di seguito la «Comunicazione del 2010»)<sup>2</sup> e sulla strategia di gestione delle informazioni per la sicurezza

---

<sup>1</sup> La strategia di sicurezza interna dell'UE in azione, COM (2010) 673.

<sup>2</sup> COM (2010) 385.

interna dell'UE approvata nel 2009<sup>3</sup>, nonché sulle azioni intraprese dagli Stati membri, la Commissione e Europol per attuarla. Inoltre, essa si fonda su una ricognizione degli scambi di informazione a livello dell'UE che ha coinvolto esperti nazionali ed altri esperti (il garante europeo della protezione dei dati, altre agenzie dell'UE, Interpol), su uno studio degli scambi di informazione tra le autorità incaricate dell'applicazione della legge<sup>4</sup> e sulle discussioni con le parti interessate, comprese le autorità per la protezione dei dati.

## 2. LA SITUAZIONE ATTUALE

Le autorità di contrasto della criminalità si scambiano informazioni per diversi fini: lo svolgimento di indagini penali, la prevenzione del crimine, l'individuazione dei reati (per esempio mediante operazioni di intelligence criminale) e il mantenimento dell'ordine e della sicurezza pubblica. Per quanto riguarda le dimensioni degli scambi transfrontalieri, il citato studio del 2010 riporta quanto riferito dalle agenzie nazionali negli Stati membri, ovvero che in circa un quarto delle loro indagini e operazioni di intelligence in materia penale sono stati interpellati altri Stati membri dell'UE o dello spazio Schengen.

### 2.1. Strumenti

La Comunicazione del 2010 descrive tutte le misure a livello UE che disciplinano la raccolta, la conservazione o lo scambio transfrontaliero di informazioni personali a fini repressivi o di gestione dell'immigrazione. La presente comunicazione verte in particolare sugli **strumenti utilizzati per gli scambi transfrontalieri tra Stati membri**. Gli Stati membri hanno fornito esempi del modo in cui utilizzano tali strumenti.

L'**iniziativa svedese**<sup>5</sup> stabilisce le regole, comprese le scadenze, per lo scambio di informazioni e intelligence tra le autorità degli Stati membri incaricate dell'applicazione della legge ai fini dello svolgimento di indagini penali o di operazioni di intelligence criminale. L'iniziativa si basa sul principio dell'«accesso equivalente»: le informazioni devono essere fornite agli Stati membri richiedenti a condizioni che non siano più severe di quelle applicabili a livello nazionale. Le informazioni devono essere comunicate anche a Europol e Eurojust, nella misura in cui lo scambio si riferisce a reati che rientrano nell'ambito del loro mandato.

*Nel 2012 una società svedese è indotta da un noto truffatore italiano a versare 65 000 EUR su un conto italiano. Lo “sportello unico” svedese (cfr. 3.2) riceve, attraverso i canali SIRENE (cfr. infra), una richiesta dell'Italia di contattare il direttore della società per verificare se il pagamento era avvenuto, nel qual caso l'Italia avrebbe bloccare il denaro. La Svezia risponde nell'ambito dell'iniziativa svedese in meno di 24 ore. Grazie alla rapida reazione, la polizia svedese ha ricevuto notizia di una frode perpetrata ai danni di un'impresa e le autorità italiane hanno ottenuto le informazioni necessarie per intervenire e il denaro potrà probabilmente essere recuperato.*

*Nel 2012, al pronto soccorso di un ospedale nei pressi di Parigi, un uomo di origine belga racconta confusamente in che modo è stato gravemente ferito da un colpo d'arma da fuoco. Le dichiarazioni della persona che lo accompagna portano gli investigatori a seguire una pista in Belgio. Dai primi accertamenti emerge che l'uomo era schedato in Belgio, anche per*

<sup>3</sup> Conclusioni del Consiglio del 30 novembre 2009, doc. 16637/09.

<sup>4</sup> [http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm).

<sup>5</sup> Decisione quadro 2006/960/JHA del Consiglio.

*omicidio. Le autorità francesi inviano immediatamente di propria iniziativa, nell'ambito dell'iniziativa svedese, informazioni alla polizia belga che individua rapidamente il collegamento con i fatti accaduti due giorni prima in Belgio quando quattro uomini armati avevano rapito il dipendente di una gioielleria. L'intervento della polizia aveva messo in fuga i criminali, che erano riusciti a dileguarsi, ma uno di loro era rimasto ferito in una sparatoria con la polizia. Sulla base di tale informazione le autorità francesi trattengono l'uomo in attesa di un mandato di arresto europeo (MAE), che viene emesso il giorno stesso in Belgio e trasmesso alla Francia tramite SIRENE.*

La decisione **Prüm**<sup>6</sup> prevede lo scambio automatizzato di dati relativi a profili DNA, impronte digitali e immatricolazione di veicoli ai fini di indagine penale (DNA, impronte, veicoli), prevenzione di reati (impronte, veicoli) e mantenimento della pubblica sicurezza (veicoli). Il confronto dei dati biometrici (DNA, impronte) opera sulla base "riscontro positivo/riscontro negativo" ("hit/no hit"): un raffronto automatizzato produce un riscontro positivo se il DNA o l'impronta in possesso dello Stato membro richiedente corrisponde ai dati detenuti in un altro Stato membro. I dati relativi alle persone o al caso vengono forniti solo a seguito di una successiva, distinta domanda.

*Il cadavere di un uomo pugnalato a morte è trovato in un appartamento di una città tedesca. Sul telaio della porta la polizia rinviene un'impronta digitale. Una ricerca automatizzata Prüm ha un riscontro positivo nella banca dati bulgara. Le pertinenti informazioni richieste alla Bulgaria il giorno dopo vengono trasmesse in 3 ore e immediatamente inserite nel sistema d'informazione Schengen (SIS – cfr. infra). Il giorno dopo il criminale in questione viene arrestato in Austria.*

*Nel 2007, all'inizio degli scambi Prüm, da un'automobile della polizia a Vienna è sottratto del materiale. Una traccia di DNA proveniente dall'auto trova riscontro positivo nella banca dati austriaca con una traccia rilevata in un caso analogo, ma è il riscontro positivo Prüm nella base dati tedesca che porta all'individuazione di un criminale polacco responsabile di numerosi furti con scasso. Un mandato d'arresto europeo è emesso in Austria. Il sospetto è arrestato in Polonia (sulla base di un riscontro positivo su una segnalazione SIS) e successivamente condannato in Austria.*

**Europol** sostiene l'azione degli Stati membri e la cooperazione per prevenire e combattere la criminalità organizzata, il terrorismo e altre forme gravi di criminalità (quali elencate nell'allegato della decisione del Consiglio che istituisce Europol<sup>7</sup>) che interessano due o più Stati membri. Offre agli Stati membri - attraverso le unità nazionali di Europol ("UNE") — una piattaforma per lo scambio di informazioni e intelligence in materia penale. Il sistema di informazione Europol è una banca dati contenente informazioni (183 000 voci) fornite dagli Stati membri sui reati transfrontalieri che ricadono nel mandato di Europol, sulle persone coinvolte (41 000) e altri dati pertinenti. Europol lo utilizza a fini di analisi e gli Stati membri possono consultarlo a fini investigativi. Dal 2011 gli Stati membri possono designare autorità di contrasto diverse dalle UNE che possono accedere alle funzioni di ricerca su base "hit/no hit". Gli archivi di lavoro per fini di analisi consentono a Europol di fornire le analisi operative a sostegno di indagini transfrontaliere.

<sup>6</sup> Decisione 2008/615/GAI del Consiglio.

<sup>7</sup> Decisione 2009/371/GAI del Consiglio.

*In Slovenia, carte di pagamento contraffatte sono state utilizzate per ritirare ingenti somme di denaro dai distributori automatici. Due cittadini bulgari sono indagati; la consultazione del Sistema di informazione Europol (SIE) consente di dimostrare che uno di loro aveva commesso reati simili in Francia e in Italia. La Francia fornisce informazioni dettagliate al SIE. Grazie ad una rapida risposta della Francia via SIENA (cfr. infra), seguito da una verifica delle impronte digitali e dalla soppressione di una restrizione di trattamento, le autorità slovene hanno potuto utilizzare i dati come prova in giudizio. L'archivio di lavoro per fini di analisi dell'Europol ha rivelato l'esistenza di collegamenti tra casi avvenuti in SI, BG, FR, IE, IT e NO.*

Il **sistema d'informazione Schengen (SIS)** contiene le segnalazioni di persone e oggetti. Come misura compensativa per l'abolizione dei controlli alle frontiere interne, è utilizzato sia all'interno dello spazio Schengen, sia alle sue frontiere esterne, al fine di mantenere un elevato livello di sicurezza. Si tratta di un sistema su larga scala (oltre 43 milioni di segnalazioni) accessibile agli operatori sul campo su base "hit/no hit". In caso di riscontro positivo (vale a dire quando i dettagli di una persona o un oggetto corrispondono alla segnalazione), è possibile ottenere informazioni supplementari tramite gli uffici SIRENE (cfr. infra). Il SIS sarà sostituito dal **sistema d'informazione Schengen di seconda generazione (SIS II)**, che apporterà alcuni miglioramenti, quali la possibilità di collegare segnalazioni tra loro attinenti (ad esempio una segnalazione su una persona e un veicolo), nuove categorie di segnalazioni, e un archivio per conservare impronte digitali, fotografie, copie di mandati d'arresto europei. La decisione del Consiglio relativa a SIS II<sup>8</sup> definisce le categorie di segnalazioni a sostegno della cooperazione tra le autorità giudiziarie e di polizia in materia penale. A tal fine, tutti gli Stati membri dell'UE parteciperanno al SIS II, e Europol e Eurojust continueranno ad avervi accesso. La gestione delle componenti centrali del SIS II sarà trasferita all'agenzia IT<sup>9</sup>.

**Altri strumenti dell'UE** o sistemi informativi consentono lo scambio di informazioni a fini repressivi tra le autorità doganali (Convenzione Napoli II; sistema d'informazione doganale nell'ambito delle banche dati del sistema d'informazione antifrode gestite dall'Ufficio europeo per la lotta antifrode - OLAF), le unità di informazione finanziaria, gli uffici per il recupero dei beni e le piattaforme di segnalazione dei reati informatici<sup>10</sup>. L'accesso a fini repressivi di altri sistemi a livello di Unione è previsto (Sistema Informazione Visti) o è proposto (EURODAC<sup>11</sup>) a fini di prevenzione, individuazione e investigazione di atti di terrorismo o altri reati gravi. La questione relativa all'autorizzazione di accesso alle autorità di polizia e, in tal caso, a quali condizioni, rientra nei lavori preparatori attualmente in corso finalizzati alla proposta di un sistema di ingressi/uscite che sarà presentata a breve.

Si sta lavorando ad un sistema europeo di sorveglianza delle frontiere (EUROSUR) per lo scambio di informazioni e la cooperazione operativa tra i centri di coordinamento nazionali e Frontex, al fine di migliorare la conoscenza della situazione alle frontiere esterne dell'UE e la capacità di reazione per prevenire la migrazione irregolare e la criminalità transfrontaliera. Un

<sup>8</sup> Decisione 2007/533/GAI del Consiglio.

<sup>9</sup> Agenzia europea per la gestione operativa di sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (Agenzia IT).

<sup>10</sup> La prossima strategia europea in materia di sicurezza informatica offrirà l'occasione di valutare le future esigenze di scambio di informazioni tra le autorità competenti in materia di sicurezza delle reti e dell'informazione e le autorità di contrasto della criminalità, ad esempio attraverso il Centro europeo per la lotta alla criminalità informatica.

<sup>11</sup> Banca dati dell'UE delle impronte digitali dei richiedenti asilo e coloro che valicano le frontiere clandestinamente.

sistema comune per la condivisione delle informazioni (CISE) relative alla sorveglianza del settore marittimo dell'UE, inteso tra l'altro a migliorare la consapevolezza della situazione nelle operazioni marittime, è stato concepito per consentire scambi di informazioni tra autorità pubbliche di sette settori pertinenti (comprese le generiche attività di applicazione della legge) e tra paesi, e al contempo garantire l'interoperabilità tra i sistemi di sorveglianza esistenti e futuri, quali EUROSUR.

Gli Stati membri si scambiano informazioni anche in applicazione della legislazione nazionale e di accordi bilaterali. Essi sono anche tutti membri di Interpol, che consente di scambiare informazioni con paesi di tutto il mondo attraverso gli avvisi e le banche dati Interpol (ad esempio documenti di viaggio rubati o smarriti) o bilateralmente utilizzando il canale Interpol.

## 2.2. Canali e strumenti di comunicazione

**Tre canali principali** sono utilizzati per lo scambio di informazioni transfrontaliero, ciascuno basato, in ogni Stato membro, su unità nazionali che utilizzano uno specifico strumento di comunicazione:

- (1) Gli uffici **SIRENE**<sup>12</sup> possono, a seguito di riscontro positivo di una segnalazione nel SIS, ottenere informazioni supplementari dallo Stato membro che ha effettuato la segnalazione. Esse operano 24 ore su 24 e 7 giorni su 7 e seguono le procedure previste nel manuale SIRENE. Attualmente, esse scambiano informazioni utilizzando un sistema denominato SISNET, che sarà sostituito dalla rete di comunicazione SIS II entro fine marzo 2013.
- (2) Le unità nazionali di **Europol** scambiano informazioni con Europol, ma possono anche trasmettere informazioni a livello bilaterale sulla criminalità al di fuori del mandato di Europol e senza il suo coinvolgimento. Tali unità possono comunicare direttamente o per il tramite degli ufficiali di collegamento Europol, che dipendono da un'unità nazionale ma sono distaccati presso la sede centrale di Europol. Strumento di comunicazione sicuro, **SIENA**<sup>13</sup>, è stato sviluppato da Europol per gli scambi con Europol e tra Stati membri. Nel 2011, gli Stati membri hanno trasmesso 222 000 messaggi tramite SIENA; nel 53% dei casi le informazioni sono state condivise con Europol.
- (3) Gli uffici centrali nazionali **Interpol**, operanti 24 ore su 24 e 7 giorni su 7, scambiano informazioni con l'Interpol ed anche a livello bilaterale, senza il suo coinvolgimento. Gli uffici centrali nazionali utilizzano lo strumento di comunicazione I-24/7 sviluppato dall'Interpol.

**Altri canali** includono gli ufficiali di collegamento bilaterali (distaccati in altri Stati membri e generalmente coinvolti nei casi più complessi) e centri di cooperazione di polizia e doganale (istituiti da Stati membri confinanti per favorire lo scambio di informazioni e la cooperazione operativa nelle regioni di frontiera).

La **scelta del canale** è in parte disciplinato dal diritto dell'UE: le richieste di informazioni supplementari a seguito di un riscontro positivo nel SIS devono essere effettuate tramite gli uffici Sirene, mentre lo scambio di informazioni con Europol deve passare attraverso le unità nazionali. Negli altri casi la scelta spetta agli Stati membri.

---

<sup>12</sup> “Supplementary Information REquest at the National Entries”.

<sup>13</sup> “Secure Information Exchange Network Application”.

### **2.3. Interazione tra i diversi strumenti, canali e dispositivi**

Esistono vari strumenti, canali e dispositivi, ciascuno destinato ad un uso specifico. Un'indagine penale può richiedere un utilizzo contestuale o sequenziale di più di uno strumento. In un caso transfrontaliero di reato grave o di criminalità organizzata, una persona o un oggetto potrebbero essere confrontate sia con il sistema di informazione Europol sia con SIS, e qualora vi fossero riscontri positivi le richieste di follow-up possono essere trasmesse, rispettivamente, via Europol o i canali SIRENE. Una traccia biometrica potrebbe essere oggetto di uno scambio Prüm seguito da una richiesta di follow-up nell'ambito dell'iniziativa svedese attraverso lo strumento SIENA.

Qualunque sia la combinazione o la sequenza, vanno rispettate le disposizioni applicabili a ciascuno strumento. Ciò vale in particolare per le disposizioni sulla protezione dei dati, sulla sicurezza e qualità dei dati, e sullo scopo per il quale gli strumenti sono utilizzati. Il trattamento nazionale di dati per gli scambi transfrontalieri deve inoltre rispettare la legislazione dell'Unione sulla protezione dei dati personali<sup>14</sup>. Deve essere rispettato il principio di proporzionalità; ad esempio, possono essere respinte richieste nell'ambito dell'iniziativa svedese nel caso in cui fornire informazioni fosse chiaramente sproporzionato rispetto alla finalità della richiesta. Il rispetto di tali disposizioni esige che le domande e le risposte siano convalidate da personale altamente qualificato e dotato di strumenti informatici adeguati.

### **2.4. Interfaccia con la cooperazione giudiziaria**

Il processo della giustizia penale coinvolge sia le autorità di contrasto della criminalità sia le autorità giudiziarie, ma esistono differenze tra gli Stati membri anche sulla misura in cui l'autorità giudiziaria (compreso il pubblico ministero) dirige o controlla l'indagine. Se sono le autorità giudiziarie a condurre l'indagine, così come quando le informazioni sono necessarie come elementi di prova, si deve generalmente far ricorso alle procedure di assistenza giudiziaria reciproca in materia di cooperazione giudiziaria.

Per contro, le informazioni direttamente accessibili alle autorità di contrasto in uno Stato membro possono essere soggette all'autorizzazione giudiziaria in un altro. L'iniziativa svedese stabilisce che, qualora le informazioni richieste siano fornite solo previa autorizzazione giudiziaria, l'autorità richiedente deve rivolgersi all'autorità giudiziaria, la quale è tenuta ad applicare le medesime regole valide per i casi di dimensione esclusivamente nazionale.

L'esercizio di ricognizione ha constatato, tuttavia, che gli esperti nel campo del contrasto della criminalità percepiscono la diversità delle norme applicabili come fonte di ritardi nelle indagini transfrontaliere. Anche se esula dalla finalità della presente comunicazione, giova osservare che Eurojust è disponibile per facilitare la cooperazione giudiziaria. Anche l'ordine europeo di indagine, attualmente in discussione, potrebbe essere utile e potrebbe sostituire le norme esistenti per l'acquisizione di mezzi di prova basandosi sul principio del reciproco riconoscimento. L'ordine dovrebbe essere riconosciuto ed eseguito con la stessa rapidità riservata ai casi simili a livello nazionale e, in ogni caso, entro i termini definiti.

---

<sup>14</sup> Decisione quadro 2008/977/GAI del Consiglio.

## 2.5. Principi

Nella sua Comunicazione del 2010 la Commissione ha esposto principi sostanziali e principi orientati al processo per lo sviluppo di nuove iniziative e la valutazione degli strumenti in vigore.

I principi sostanziali sono:

- (1) *Salvaguardia dei diritti fondamentali, in particolare del diritto al rispetto della vita privata e alla protezione dei dati.* Si tratta dei diritti sanciti agli articoli 7 e 8 della Carta e all'articolo 16 del trattato sul funzionamento dell'Unione europea.
- (2) *Necessità.* Una restrizione del diritto al rispetto della vita privata può essere giustificato soltanto se prevista per legge, persegue un obiettivo legittimo e se è necessario in una società democratica.
- (3) *Sussidiarietà.*
- (4) *Attenta gestione del rischio.* La verifica della necessità e la limitazione delle finalità sono presupposti essenziali.

I principi orientati al processo sono:

- (1) *Efficacia economica.* Ciò significa che si deve tener conto delle soluzioni preesistenti e valutare se un uso ottimale degli strumenti esistenti possa conseguire gli obiettivi di una proposta.
- (2) *Elaborazione delle politiche "dal basso".* Un esempio in proposito è dato dall'esercizio di ricognizione al quale hanno partecipato esperti incaricati dell'applicazione della legge per la preparazione della presente comunicazione.
- (3) *Ripartizione chiara delle responsabilità.* La Comunicazione del 2010 ha constatato che gli Stati membri non dispongono di un capo progetto al quale rivolgersi per consulenze in materia di attuazione della decisione Prüm. La relazione sull'attuazione della decisione Prüm della Commissione osserva che questa lacuna è oggi in parte coperta dal sostegno offerto da Europol. Per quanto concerne l'idea, espressa nella Comunicazione del 2010, che l'Agenzia IT possa fornire consulenza tecnica, si deve riscontare che le attuali priorità dell'Agenzia risiedono altrove. Un'occasione per riesaminare quest'opzione sarà la valutazione triennale prevista entro la fine del 2015.
- (4) *Clausole di revisione e caducità.* La Commissione ha pubblicato le relazioni sull'applicazione dell'iniziativa svedese e della decisione Prüm. La presente comunicazione tiene conto di entrambe.

## 3. VALUTAZIONE E RACCOMANDAZIONI

La presente sezione verte sull'iniziativa svedese, sulla decisione Prüm e sul canale Europol. Anche se SIS e il canale SIRENE vantano un elevato volume di scambi di informazioni, non vengono definite raccomandazioni in proposito perché sono già in corso estese modifiche dei due canali, in particolare con il passaggio imminente al SIS II.



### 3.1. Migliorare l'uso degli strumenti esistenti

Al di fuori della futura riforma di Europol, la Commissione non intende, a breve termine, proporre modifiche ai citati strumenti dell'Unione, né risultano necessari nuovi strumenti nel contesto attuale. **Prima di tutto occorre dare piena attuazione agli strumenti esistenti.**

Ciò vale in special modo per la decisione Prüm. La relazione sull'applicazione della decisione Prüm della Commissione che accompagna la presente comunicazione ritiene che lo scambio di dati in ambito Prüm sia molto apprezzato ai fini investigativi, ma che l'attuazione della decisione abbia subito un grave ritardo. **Molti Stati membri non scambiano ancora dati in ambito Prüm, benché la scadenza di recepimento della decisione fosse fissata al 26 agosto 2011**<sup>15</sup>. Le ragioni principali sono difficoltà di natura tecnica e la mancanza di risorse umane e finanziarie negli Stati membri. Tuttavia, tenuto conto delle possibilità di sostegno dell'UE (finanziamenti, Mobile Competence Team, helpdesk), sembrerebbe piuttosto che manchi la volontà politica di dare attuazione allo strumento. Come indicato nella relazione, la Commissione continuerà ad offrire sostegno attraverso i finanziamenti dell'UE. Tuttavia, la situazione è destinata a cambiare nel dicembre 2014, quando la Commissione sarà in grado di avviare procedimenti di infrazione. Fino a tale data, infatti, non si può far ricorso alle norme in materia di controllo dell'applicazione a livello nazionale giacché la decisione Prüm, così come l'iniziativa svedese, è stata adottata in base al vecchio terzo pilastro.

Per quanto riguarda **l'iniziativa svedese**, la Commissione ha riferito nel 2011 che lo strumento non aveva ancora realizzato pienamente il suo potenziale, ma che la sua importanza era destinata a crescere<sup>16</sup>. Tale valutazione resta valida; non tutti gli Stati membri si sono conformati all'obbligo di attuazione<sup>17</sup>. La maggior parte degli Stati membri ha notificato il recepimento degli strumenti nel diritto interno<sup>18</sup>, mentre alcuni hanno dichiarato che ciò non era necessario poiché la loro normativa nazionale è già conforme a detti strumenti<sup>19</sup>. Tuttavia, nonostante i vantaggi che comporta, segnatamente il principio dell'accesso equivalente e le scadenze, lo strumento rimane in pratica ancora poco utilizzato. Le motivazioni addotte includono, tra l'altro, l'esistenza di alternative adeguate e la difficoltà di compilare il modulo di richiesta (anche nella sua versione semplificata del 2010<sup>20</sup>).

È stato chiesto alla Commissione di valutare la sua utilità per le richieste di follow-up a seguito di riscontri positivi in ambito Prüm<sup>21</sup>. Se è necessario disporre di informazioni di follow-up come elemento di prova dinanzi a un giudice, è generalmente necessaria una richiesta di cooperazione giudiziaria. Tuttavia, nel caso in cui l'utilizzazione come elementi di prova non sia o non sia ancora necessaria, l'uso sistematico dell'iniziativa svedese come base giuridica e di SIENA come canale di comunicazione dovrebbe essere promosso in modo da sfruttare appieno i vantaggi di ciascuno e allineare gli Stati membri sulla medesima buona pratica.

---

<sup>15</sup> I seguenti Stati membri si sono conformati all'obbligo di attuazione:  
DNA: BG/CZ/DE/ES/EE/FR/CY/LV/LT/LU/HU/NL/AT/PT/RO/SI/SK/FI;  
Impronte digitali: BG/CZ/DE/EE/ES/FR/CY/LT/LU/HU/NL/AT/SI/SK;  
Immatricolazione di veicoli: BE/DE/ES/FR/LT/LU/NL/AT/PL/RO/SI/FI/SE.  
Per ulteriori informazioni, si rimanda alla relazione Prüm

<sup>16</sup> SEC (2011) 593.

<sup>17</sup> I seguenti Stati membri devono ancora adottare la normativa di attuazione: BE/EL/IT/LU.

<sup>18</sup> BG/CZ/DK/DE/EE/ES/FR/CY/HU/LT/LV/NL/PL/PT/RO/SI/SK/FI/SE.

<sup>19</sup> IE/MT/AT/UK.

<sup>20</sup> Doc. 9512/1/10.

<sup>21</sup> Conclusioni del Consiglio del 27 e 28 ottobre 2011, doc. 15277/11.

Per quanto riguarda **Europol**, una valutazione del 2012<sup>22</sup> fornisce ulteriori riscontri del fatto che gli Stati membri non condividono le informazioni con Europol (e quindi reciprocamente) in misura adeguata. La Commissione affronterà questo aspetto in una proposta di modifica della base giuridica di Europol. Da parte sua, il Consiglio ha invitato gli Stati membri a fare maggiore uso del sistema di informazione Europol<sup>23</sup>.

In linea con il programma di Stoccolma, la Commissione ha ordinato uno studio su un eventuale **Indice europeo dei casellari giudiziari (EPRIS)**<sup>24</sup>. Dato l'aumento dei reati di natura transfrontaliera, l'idea è di rispondere alla necessità avvertita dai funzionari di polizia in uno Stato membro di sapere se il sospetto è noto alla polizia di un altro. In linea con il principio del buon rapporto costo/efficacia, la Commissione ritiene che la creazione di un **EPRIS non sia al momento giustificato** dato che gli strumenti e i mezzi esistenti, che potrebbero offrire, in parte o del tutto, lo stesso servizio grazie ad un utilizzo migliore o rafforzato, non sono pienamente sfruttati. Ciò riguarda in particolare il sistema di informazione Europol (caricamento dati pertinenti e ampliamento dell'accesso a livello nazionale), il SIS II (uso crescente di segnalazioni di persone o veicoli ai fini di controllo per la repressione di infrazioni penali e per prevenire minacce alla sicurezza pubblica), SIENA (ulteriore miglioramento dell'accesso a livello nazionale, l'interconnessione con i sistemi nazionali e, eventualmente, l'automatizzazione di alcune funzioni), e di Prüm (piena attuazione al fine di migliorare l'identificazione dei criminali che operano in diversi Stati membri).

#### ***Gli Stati membri sono invitati a***

- attuare pienamente l'iniziativa svedese, compreso il principio dell'accesso equivalente;
- dare piena attuazione alla decisione Prüm, avvalendosi delle possibilità di sostegno dell'UE;
- a seguito delle richieste di follow-up successive a riscontri positivi in ambito Prüm, avvalersi dell'iniziativa svedese e dello strumento SIENA.

#### ***La Commissione intende:***

- continuare a fornire finanziamenti dell'UE per sostenere l'attuazione della decisione Prüm;
- entro dicembre 2014: prepararsi ad applicare in questo settore le disposizioni che assicurino l'attuazione nazionale del diritto dell'Unione.

### **3.2. Razionalizzare e gestire i canali**

**Scelta del canale.** Una delle conseguenze della libertà di scelta del canale da parte degli Stati membri (con l'eccezione delle disposizioni vincolanti concernenti gli uffici SIRENE e gli uffici nazionali di Europol) è che essi tendono ad utilizzare i diversi canali in diversa misura. Il manuale di buone prassi riguardanti la cooperazione internazionale tra forze di polizia a

<sup>22</sup> [https://www.europol.europa.eu/sites/default/files/publications/rand\\_evaluation\\_report.pdf](https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf)

<sup>23</sup> Conclusioni del Consiglio del 7 e 8 giugno 2012.

<sup>24</sup> [http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm).

livello nazionale (“Manuale del 2008”)<sup>25</sup>, messo a punto sotto l’egida dei capi della polizia europei, contiene dei criteri<sup>26</sup>, che tuttavia non sono vincolanti e non hanno portato alla convergenza delle pratiche nazionali. Alcuni Stati membri sono passati a un ricorso più sistematico del canale Europol. Altri continuano a basarsi ampiamente sul canale Interpol, la cui attrattiva sembra risiedere in parte nel suo tradizionale ruolo centrale nella cooperazione internazionale di polizia e in parte nella sua facilità d’uso. SISNET è utilizzato da alcuni Stati membri per le questioni non attinenti al SIS, ad esempio le richieste nell’ambito dell’iniziativa svedese.

La Commissione ritiene che sia giunto il momento di procedere all’interno dell’UE a un approccio più coerente, che conferisca al canale Europol un ruolo centrale. In tal senso, quando la scelta del canale non è giuridicamente definita, **il canale Europol, tramite lo strumento SIENA, dovrebbe diventare il canale prescelto**, tranne quando ragioni particolari impongano di utilizzarne un altro. Così, ad esempio, le richieste di cooperazione di polizia attualmente effettuate utilizzando la rete SISNET (che giungerà a termine non appena SIS II diventerà operativo<sup>27</sup>) dovrebbero in futuro essere effettuate tramite SIENA.

Alcuni Stati membri privilegiano un approccio che lascia ampia flessibilità di utilizzare i diversi canali. La Commissione non è d’accordo. La definizione da parte di tutti gli Stati membri di norme nazionali applicabili alla scelta dei canali e la convergenza verso un unico approccio comune risulterebbero più efficaci rispetto all’attuale approccio dispersivo. La scelta del canale Europol è giustificabile in base ai suoi vantaggi. Gli ufficiali di collegamento Europol possono essere chiamati a intervenire in caso di necessità. Lo strumento SIENA, utilizzato per gli scambi bilaterali diretti, può anche favorire lo scambio di informazioni con Europol conformemente ai requisiti della decisione Europol e dell’iniziativa svedese. I messaggi SIENA sono strutturati, possono gestire grandi volumi di dati e sono trasmessi con un livello elevato di sicurezza. La protezione dei dati è rafforzata dallo scambio di informazioni in un formato strutturato, ad esempio tramite SIENA. L’approccio suggerito è pienamente in linea con la proposta della Commissione di riforma di Europol e con gli orientamenti strategici definiti dal Consiglio europeo nel programma di Stoccolma, che afferma che “Europol dovrebbe diventare il punto nodale dello scambio di informazioni tra le autorità di contrasto degli Stati membri, un fornitore di servizi e una piattaforma per i servizi di applicazione della legge”.

**Gestione dei canali.** Un unico punto di contatto (SPOC) è uno “sportello unico” per la cooperazione internazionale tra le forze di polizia, che operano 24 ore su 24 e 7 giorni su 7, in cui uno Stato membro riunisce il proprio ufficio SIRENE, l’unità nazionale Europol e gli uffici centrali nazionali Interpol, e i punti di contatto per altri canali. La creazione da parte di ciascuno Stato membro, di un punto di contatto unico (anche se questo termine non è sempre utilizzato) figurava nel 2007 tra le conclusioni della terza tornata di visite<sup>28</sup> di valutazione reciproca e tra le raccomandazioni del manuale del 2008. La maggior parte degli Stati membri dispone di un dipartimento per la cooperazione internazionale tra forze di polizia, ma solo alcuni sono dotati delle caratteristiche di un autentico “sportello unico”. Nel 2012, il Consiglio ha invitato gli Stati membri ad esaminare le possibilità di istituire uno “sportello unico”<sup>29</sup>. La Commissione andrebbe oltre: per migliorare lo scambio di informazioni in

---

<sup>25</sup> Doc. 7968/08.

<sup>26</sup> Ripetuti negli Orientamenti sull’attuazione dell’iniziativa svedese, doc. 9512/1/10.

<sup>27</sup> La rete di comunicazione SIS II è giuridicamente limitata ai dati SIS II e alle informazioni supplementari.

<sup>28</sup> Doc. 13321/3/07.

<sup>29</sup> Conclusioni del Consiglio del 7 e 8 giugno 2012, doc. 10333/12.

materia di applicazione della legge nell'UE nel suo insieme, **tutti gli Stati membri dovrebbero istituire uno “sportello unico”** con determinate caratteristiche minime.

Per le richieste rivolte a un altro Stato membro, il fatto di riunire i vari canali in un'unica struttura organizzativa che segua le norme nazionali applicabili alla scelta del canale, garantirà la corretta e coerente scelta dei canali, nonché la qualità delle richieste. La qualità è garantita dal fatto che lo “sportello unico” convalida le richieste per confermare se siano necessarie e appropriate. Quando le informazioni non vengono scambiate mediante uno “sportello unico” (ma passano, ad esempio, per i Centri di cooperazione di polizia e doganale (CCPD) o tramite le agenzie nazionali che effettuano scambi diretti tramite SIENA), uno “sportello unico” può garantire un coordinamento nazionale. Per le richieste in arrivo, gli “sportelli unici” dovrebbero, se la legge lo consente, avere accesso diretto alle banche dati nazionali per rispondere alle richieste rapidamente, in particolare entro i termini prescritti dall'iniziativa svedese. Le regole del Manuale SIRENE (ad esempio in materia di sicurezza, sistemi di flusso di lavoro, la qualità dei dati e il personale) potrebbero costituire una base per organizzare tutti i canali in modo coerente. La condivisione delle risorse, ad esempio relative al personale e alle infrastrutture, può contribuire alla riduzione dei costi o almeno a un uso migliore delle risorse.

Gli “sportelli unici” dovrebbero comprendere tutte le autorità di contrasto della criminalità, comprese le dogane. Si dovrebbe instaurare una cooperazione tra “sportelli unici” e i centri nazionali di coordinamento (CNC) per la sorveglianza delle frontiere. Se compatibile con i sistemi giuridici nazionali, dovrebbero essere instaurati collegamenti con le autorità giudiziarie, in particolare laddove queste dirigono le indagini penali.

Un numero crescente di CCPD<sup>30</sup> effettuano soddisfacenti scambi di informazioni a livello locale e regionale. Le conferenze annuali a livello dell'UE consentono di condividere le esperienze e di discutere approcci comuni. Sebbene il numero generalmente elevato di scambi non riguardi per lo più i casi più gravi di criminalità organizzata, una delle sfide consiste nel garantire che le informazioni nei casi in questione raggiunga il livello nazionale (“sportello unico”) e, se del caso, Europol. In questo contesto, la Commissione attende con impazienza i risultati di un progetto pilota in corso (nell'ambito di un'azione relativa alla strategia di gestione dell'informazione) che utilizza SIENA in un centro di cooperazione di polizia e doganale.

La **piattaforma di scambio delle informazioni** è un'azione relativa alla strategia di gestione delle informazioni condotta da Europol intesa a sviluppare un portale comune per accedere ai canali e ai sistemi esistenti, nel pieno rispetto delle rispettive norme di sicurezza e della protezione dei dati. La Commissione ritiene che sia vantaggioso facilitare l'utilizzo dei canali e dei sistemi esistenti, ma che sia necessario un'ulteriore valutazione del rapporto costi/benefici di una piattaforma di scambio di informazioni, di riflettere sulle fonti di finanziamento, e sulla conduzione del progetto. Tale valutazione dovrebbe coinvolgere anche l'Agenzia IT<sup>31</sup>.

---

<sup>30</sup> 38 a fine 2011.

<sup>31</sup> Agenzia europea per la gestione operativa di sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (Agenzia IT).

***Gli Stati membri sono invitati a:***

- utilizzare, per gli scambi in cui il canale non è giuridicamente definito, il canale Europol utilizzando lo strumento SIENA come canale prescelto, a meno che esistano ragioni particolari di utilizzarne un altro;
- elaborare istruzioni nazionali per la scelta del canale;
- in particolare, quando il SIS II sarà operativo e SISNET sarà dismesso, utilizzare il canale Europol e lo strumento SIENA per gli scambi nel settore della cooperazione di polizia che attualmente sono effettuati utilizzando la rete SISNET;
- creare, se non già esistente, un punto di contatto unico (Single Point of Contact - SPOC) per tutti i principali canali, disponibile 24/7, che riunisca tutte le autorità di contrasto della criminalità, con accesso alle banche dati nazionali;
- garantire che le informazioni scambiate attraverso i centri di cooperazione di polizia e doganale siano, come opportuno, trasmesse al più alto livello nazionale, e, se del caso, a Europol;
- instaurare una cooperazione tra gli sportelli unici e i centri nazionali di contatto EUROSUR.

***Il Consiglio è invitato a:***

- modificare le raccomandazioni a livello UE al fine di tener conto degli orientamenti relativi alla scelta di canali di cui sopra.

***La Commissione intende:***

- partecipare ai lavori volti a valutare la fattibilità di una piattaforma di scambio di informazioni.

### **3.3. Garantire la qualità dei dati, la sicurezza e la protezione**

Le garanzie in materia di protezione dei dati contenute negli strumenti esistenti devono essere scrupolosamente osservate. Ai sensi della proposta della Commissione, del 25 gennaio 2012, relativa a una direttiva applicabile al trattamento dei dati personali fini di prevenzione, indagine, accertamento e perseguimento di reati<sup>32</sup>, vanno rivedute le norme di protezione dei dati contenute negli strumenti esistenti al fine di valutare la necessità di renderli coerenti con la direttiva.

**Un elevato livello di sicurezza dei dati** è necessario per proteggere l'integrità dei dati personali scambiati e per garantire la fiducia degli Stati membri nello scambio di informazioni. La solidità di una catena è quella del suo anello più debole. Gli Stati membri e le agenzie dell'UE devono garantire lo scambio dei dati tramite reti che presentano un alto grado di sicurezza. La menzionata proposta di direttiva contiene norme in materia di sicurezza

---

<sup>32</sup> COM (2012) 10.

dei dati<sup>33</sup>, e a livello dell'UE esistono dettagliate norme di sicurezza per la protezione delle informazioni classificate UE<sup>34</sup>.

**Un elevato livello di qualità dei dati** è altrettanto importante. In questo contesto rivestono grande importanza le “procedure operative”, ossia il modo in cui lo scambio di informazioni avviene nella pratica. Si tratta ad esempio, ove sia possibile e opportuno, di **automatizzare determinati compiti**. Ad esempio, trattare una richiesta di informazioni proveniente da un altro Stato membro richiede che i dati registrati in un sistema nazionale vengano reinseriti nel mezzo di comunicazione utilizzato. Una procedura manuale comporta il rischio dell'introduzione di errori ed è dispendiosa in termini di tempo. Automatizzare tali compiti sarà reso possibile dal progetto **UMF II**<sup>35</sup>, un'altra azione relativa della strategia di gestione delle informazioni. Questo progetto finanziato dall'UE e condotto da Europol mira a normalizzare il formato dei messaggi utilizzati per chiedere informazioni e fornire risposte. Ciò consentirebbe l'automazione del trasferimento di dati tra i diversi sistemi nazionali, ad esempio i sistemi di gestione dei dossier nazionali e SIENA. Oltre ai potenziali risparmi sui costi, o almeno un migliore utilizzo delle risorse, l'eliminazione del reinserimento manuale dei dati comporterebbe duplici vantaggi. Da un lato, il personale che si rende così disponibile può essere impiegato in compiti di convalida, e, dall'altro, riducendo gli errori di copiatura e facilitando lo scambio di informazioni in formati strutturati, la gestione e la protezione dei dati risulteranno migliorati.

L'automatizzazione dei compiti non implica che ogni funzionario di polizia nell'UE debba avere accesso a tutte le informazioni di polizia nell'UE. Gli scambi devono essere limitati a quanto necessario e opportuno e devono essere gestiti in modo da garantire che rimangano all'interno di tali limiti. **Le ricerche automatizzate, intese a superare i problemi di capacità, funzionano quindi nell'ambito dei vigenti strumenti dell'UE di scambio di informazioni su base “hit/no hit”** (ad esempio, SIS, DNA e impronte digitali in ambito Prüm), oppure sono limitate a determinati tipi di dati (ad esempio dati di immatricolazione dei veicoli in ambito Prüm). Alcuni compiti non possono e non devono essere automatizzati, in particolare la convalida delle domande e delle risposte. Ciò è particolarmente importante nel contesto dell'iniziativa svedese, che prevede che le richieste siano giustificate.

Infine, **l'interoperabilità** tra i diversi sistemi nazionali e strutture amministrative può generare benefici in termini di coerenza delle procedure, rapidità dei tempi di risposta, migliore qualità dei dati e semplificazione di progettazione e sviluppo. Il quadro europeo di interoperabilità<sup>36</sup> individua quattro livelli di interoperabilità: tecnico, linguistico, organizzativo e giuridico. Il progetto UMF II svilupperà il livello semantico<sup>37</sup>. L'allineamento verso pratiche comuni (sportelli unici, scelta dei canali) promuoverà il livello organizzativo. In ogni caso, le informazioni saranno sempre scambiate e utilizzate solo se consentito per legge.

***Europol e gli Stati membri sono invitati a:***

- proseguire lo sviluppo degli standard UMF II.

<sup>33</sup> Articoli da 27 a 29 della proposta.

<sup>34</sup> Decisione 2011/292/UE del Consiglio.

<sup>35</sup> Universal Message Format (formato del messaggio universale).

<sup>36</sup> COM (2010) 744.

<sup>37</sup> UMF II tiene conto di altri lavori sulla semantica, quali i modelli di dati comuni elaborati nell'ambito del programma UE sulle soluzioni di interoperabilità per le pubbliche amministrazioni europee.

### 3.4. Migliorare la formazione e la sensibilizzazione

Per dotare i funzionari delle autorità di contrasto della criminalità delle conoscenze e delle competenze necessarie per cooperare in modo efficace, la Commissione sta elaborando un programma di formazione europea in materia di applicazione della legge. Uno studio dell'UE ha dimostrato che il tema degli strumenti di scambio di informazioni è trattato nella formazione iniziale del personale delle autorità incaricate dell'applicazione della legge, senza però dare una valutazione qualitativa della formazione. I funzionari specializzati, ad esempio, coloro che lavorano presso uno "sportello unico", devono ricevere una formazione approfondita. Sono stati riconosciuti proficui anche gli scambi di tale personale<sup>38</sup>, che dovrebbero essere incoraggiati.

#### *Gli Stati membri sono invitati a:*

- assicurare che tutti i funzionari delle autorità di contrasto della criminalità ricevano una formazione appropriata in materia di scambio di informazioni transfrontaliero;
- organizzare scambi di personale degli "sportelli unici";

#### *La Commissione intende:*

- garantire che il programma di formazione europea nel settore del contrasto della criminalità includa una formazione in materia di scambio di informazioni transfrontaliero.

### 3.5. Finanziamento

Nell'ambito del Fondo per la prevenzione e la lotta contro la criminalità (ISEC), l'Unione ha finanziato progetti nel settore dello scambio di informazioni, quali il progetto UMF II (830 000 EUR) e l'attuazione della decisione Prüm (11,9 milioni di EUR). Il fondo sarà sostituito nel periodo 2014-2020 da un Fondo europeo per la sicurezza interna dell'UE, di cui potranno beneficiare anche i progetti di scambio di informazioni.

Parte del Fondo per la sicurezza interna sarà amministrato dagli Stati mediante la "gestione concorrente", conformemente ai **programmi pluriennali. Tali programmi dovrebbero tenere conto delle pertinenti priorità nazionali in materia di scambio di informazioni**, in linea con le raccomandazioni formulate nella presente comunicazione. La Commissione intende parallelamente considerare come alcune parti del Fondo per la sicurezza interna sottoposte a gestione diretta possono sostenere in particolare dei progetti pilota, ad esempio lo sviluppo ulteriore di UMF II.

Per quanto riguarda la spesa degli Stati membri, altre raccomandazioni (in tema di "sportelli unici", UMF II) potrebbero, come indicato, contribuire alla riduzione dei costi o almeno a un uso migliore delle risorse.

#### *Gli Stati membri sono invitati a:*

- tener conto di determinate priorità in materia di scambio di informazioni nei programmi pluriennali nazionali nell'ambito del Fondo per la sicurezza interna dell'UE 2014-2020.

<sup>38</sup> Doc. 10333/12.

***La Commissione intende:***

- integrare le regole in materia di scambi di informazioni nel dialogo con gli Stati membri relativo alla programmazione del Fondo per la sicurezza interna;
- avviare un bando per il finanziamento diretto (Commissione) di progetti pilota pertinenti.

### **3.6. Statistiche**

Le statistiche esistenti, benché pertinenti in alcuni settori (ad esempio SIS, SIENA), non sono complete. Migliorare le statistiche potrebbero migliorare la conoscenza della reale applicazione dell'iniziativa svedese (per la quale si conoscono solo le cifre trasmesse via SIENA) e della decisione Prüm.

La rilevazione statistica implica tuttavia un notevole impiego di risorse, in particolare se non rientra nel normale flusso di lavoro. Le esercitazioni ad hoc devono essere evitate. È preferibile privilegiare un approccio progressivo, basandosi sulle procedure già in essere quali, come descritto nella relazione Prüm, la ricognizione dei riscontri positivi che hanno contribuito all'avanzamento delle indagini. Un maggiore uso di SIENA per le richieste nell'ambito dell'iniziativa svedese, come sopra raccomandato, si tradurrà in un aumento delle statistiche relative allo strumento SIENA.

***Gli Stati membri sono invitati a:***

- migliorare le statistiche relative alla decisione Prüm.

## **4. CONCLUSIONI**

Migliorare lo scambio di informazioni transfrontaliero non un fine in se stesso, bensì mira a rendere più efficace la lotta contro la criminalità e quindi a ridurre i danni subiti dalle vittime e dall'economia dell'UE.

Lo scambio di informazioni a livello transfrontaliero in generale funziona bene e, come dimostrano gli esempi precedenti, apporta un contributo prezioso nella lotta contro le forme gravi di criminalità transfrontaliera nell'UE. Esiste tuttavia un margine di miglioramento. La normativa adottata deve essere pienamente applicata da tutti gli Stati membri. In futuro, gli Stati membri dovrebbero, in particolare, convergere verso un uso più sistematico del canale Europol e istituire punti di contatto unici a livello nazionale, completi di tutte le caratteristiche necessarie.

Da parte sua, la Commissione continuerà ad esaminare l'attuazione e l'utilizzo degli strumenti, a fornire finanziamenti dell'UE e a riunire tutti i diversi elementi indispensabili per garantire la coerenza generale. La Commissione non propone un nuovo strumento a questo stadio. Se ciò si renderà necessario in futuro, applicherà i principi sostanziali enunciati nella Comunicazione del 2010: salvaguardia dei diritti fondamentali, garanzia della necessità, sussidiarietà e un'attenta gestione del rischio.

Sono necessari sforzi considerevoli per garantire che le informazioni pertinenti siano condivise con Europol, in modo da creare un quadro completo a livello dell'UE della criminalità transfrontaliera. La proposta della Commissione relativa alla riforma di Europol



permetterà di rispondere a tali esigenze. Tuttavia, l'applicazione delle raccomandazioni contenute nella presente comunicazione per un ricorso più sistematico al canale Europol e al suo mezzo di comunicazione sicura SIENA permetterebbe già da ora di facilitare la trasmissione di informazioni a Europol .

Per dare seguito alla presente comunicazione, la Commissione continuerà a lavorare con gli Stati membri nel contesto della strategia di gestione delle informazioni dell'UE per la sicurezza interna, e invita il Consiglio a organizzare un dibattito annuale nell'ambito del suo comitato permanente per la sicurezza interna. La Commissione invita inoltre il Parlamento europeo a discutere le raccomandazioni proposte, anche in seno alla commissione speciale sulla criminalità organizzata, la corruzione e il riciclaggio di denaro.