



COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 16.6.2004
COM (2004) 429 definitivo

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

**Migliorare l'accesso all'informazione da parte delle autorità incaricate del
mantenimento dell'ordine pubblico e del rispetto della legge**

INDICE

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO: MIGLIORARE L'ACCESSO ALL'INFORMAZIONE DELLE AUTORITÀ INCARICATE DEL MANTENIMENTO DELL'ORDINE PUBBLICO E DEL RISPETTO DELLA LEGGE.....	3
CAPITOLO I– INTRODUZIONE, CONTESTO LOGICO E POLITICO	3
CAPITOLO II – VERSO UN MIGLIORE ACCESSO AI DATI E L'INTRODUZIONE DI UN'AZIONE DI POLIZIA E GIUDIZIARIA A LIVELLO UE FONDATA SULL'INTELLIGENCE.....	6
2.1. Obiettivi strategici.....	6
2.2. Elementi chiave per un accesso efficace ai dati ed alle informazioni e loro raccolta, conservazione, analisi e scambio	7
2.2.1. Il principio dell'accesso equivalente ai dati da parte delle autorità incaricate del mantenimento dell'ordine pubblico e del rispetto della legge.....	7
2.2.2. Delimitazione delle condizioni di accesso	8
2.2.3. Raccolta dei dati.....	10
2.2.4. Scambio e trattamento dei dati.....	10
2.2.5. Ricerca.....	11
2.3. Elementi fondamentali di un'efficace applicazione della legge fondata sull'intelligence a livello europeo	11
2.4. Instaurazione di un clima di fiducia.....	13
CAPITOLO III – INIZIATIVE LEGISLATIVE CONNESSE ALLA PRESENTE COMUNICAZIONE	14

**COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL
PARLAMENTO EUROPEO: MIGLIORARE L'ACCESSO ALL'INFORMAZIONE
DELLE AUTORITÀ INCARICATE DELL'APPLICAZIONE DELLA LEGGE
(POLITICA D'INFORMAZIONE UE)**

CAPITOLO I– INTRODUZIONE, CONTESTO LOGICO E POLITICO

Sguardo d'insieme

La dichiarazione del Consiglio europeo sulla lotta al terrorismo¹ dà mandato al Consiglio di esaminare misure legislative volte a semplificare lo scambio di informazioni e di intelligence tra le autorità degli Stati membri incaricate del mantenimento dell'ordine pubblico. La Commissione è invitata a presentare proposte al Consiglio europeo di giugno riguardo lo scambio di informazioni personali e l'uso delle informazioni sui passeggeri al fine di combattere il terrorismo. Le proposte della Commissione dovrebbero includere anche disposizioni che permettano alle autorità nazionali incaricate dell'applicazione della legge di accedere ai sistemi informativi dell'UE.

La presente comunicazione è un primo contributo della Commissione in risposta alla richiesta del Consiglio.

In questa comunicazione, la Commissione espone gli elementi critici che impediscono il raggiungimento della libera circolazione delle informazioni tra le autorità degli Stati membri incaricate dell'applicazione della legge, in modo più strutturato di quello attuale. Esistono ancora ostacoli alla libera circolazione delle informazioni, il che induce il Consiglio, tra l'altro, a dedicare la terza fase delle reciproche valutazioni ad esaminare lo "scambio di informazioni e intelligence tra Europol e gli Stati membri e tra gli Stati membri stessi". La compartimentalizzazione dell'informazione e la mancanza di una politica chiara sui canali informativi ostacola lo scambio di informazioni. Le sfide per superare la suddivisione dell'informazione tra i diversi ministeri nazionali sono esacerbate dai problemi legali, tecnici e pratici che impediscono lo scambio tra Stati membri. Allo scopo di ottenere un quadro più accurato di tali ostacoli, la Commissione propone di fare il punto completo della situazione sulle condizioni di accesso all'informazione, nonché di intraprendere un'ampia e aperta consultazione di tutti gli interessati, in particolare del Garante europeo della protezione dei dati. La comunicazione è altresì volta a fornire i mezzi per evitare le minacce maggiori, quali il terrorismo, introducendo il concetto di azione di polizia e giudiziaria basata sull'intelligence a livello UE. Essa presenta un programma che espone come raggiungere questo obiettivo ed annuncia una normativa per eliminare specifici problemi giuridici. Il fulcro di questa comunicazione è il miglioramento dell'accesso alle informazioni necessarie e rilevanti, come pure il più ampio concetto dell'introduzione di un'azione di polizia e giudiziaria fondata sull'intelligence a livello UE. Ciò avrà altresì conseguenze sul ruolo internazionale che l'UE è in grado di assumere.

¹ Consiglio europeo del 25 marzo 2004 *Dichiarazione sulla lotta al terrorismo*.

Questi due elementi costituiscono le pietre miliari della politica d'informazione UE per le autorità incaricate dell'applicazione della legge. L'azione comune in questi settori sosterrà la progressiva instaurazione dell'area di libertà, sicurezza e giustizia, ove la libera circolazione delle persone resta garantita di fronte alle nuove sfide sulla sicurezza che il terrorismo e le altre forme di crimine grave e organizzato pongono a tutta l'Unione. L'efficacia delle attività connesse all'applicazione della legge dovrà costruirsi in osservanza dei diritti umani e delle libertà fondamentali protette dalle tradizioni internazionali, europee e costituzionali comuni agli Stati membri. Inoltre, nella costruzione di questa politica, la Commissione garantirà che la normativa e le politiche comunitarie siano tenute in debito conto. In particolare, tale politica non dovrà creare incertezza del diritto o indebiti oneri economici per le industrie.

La Commissione invita gli Stati membri e le parti implicate ad impegnarsi in questa audace azione di cooperazione.

In primo luogo, adottare le misure indispensabili per rendere accessibili i dati e le informazioni pertinenti e necessarie alle autorità UE incaricate della repressione del crimine, allo scopo di prevenire e combattere il terrorismo e le altre forme di criminalità grave o organizzata, come pure le minacce che da esse derivano. A tale riguardo, si deve tenere a mente che le attività criminali che pure non sembrano far parte della categoria "grave o organizzata" possono molto bene condurvi o esservi collegate.

In secondo luogo, produrre ed utilizzare intelligence penale europea di alta qualità. Il suo utilizzo nell'ambito di questo processo aiuterà le istanze politiche a stabilire le priorità nel settore della giustizia e degli affari interni, in modo concertato, e permetterà alle autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge di lottare efficacemente contro i reati e le minacce che compromettono le vite dei nostri cittadini, la loro integrità e sicurezza fisica.

In terzo luogo, migliorare la fiducia tra i servizi. L'introduzione di condizioni comuni, ad esempio per l'accesso ai sistemi di dati e la divisione del "know-how", contribuiranno ad istituire una piattaforma comune di politica dell'informazione, in particolare eliminando gli ostacoli alla condivisione efficace dell'informazione e dell'intelligence.

Un certo numero di considerazioni sono sottese alla politica europea di informazione per l'applicazione della legge. Esse sono legate alla crescente presa di coscienza della vulnerabilità dell'Unione alle minacce come quelle determinate dalle attività terroristiche e dei loro effetti destabilizzanti su tutta la società; della dipendenza dell'Unione dovuta all'interconnessione delle reti; della necessità di stabilire flussi d'informazione rafforzati tra le autorità competenti; dei vantaggi delle nuove tecnologie e dei mezzi basati su le conoscenze per aumentare l'azione delle autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge e, nello stesso tempo, all'esigenza di rafforzare la protezione dei dati, la sicurezza ed i meccanismi di controllo e di sorveglianza.

Questa comunicazione intende migliorare lo scambio di informazioni tra tutte le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge, cioè non soltanto tra le forze di polizia, ma anche tra le autorità doganali, l'intelligence finanziaria, nonché migliorare l'interazione tra le autorità giudiziarie e le procure e qualsiasi altro ente pubblico che partecipi al processo che va dall'individuazione rapida delle minacce alla sicurezza e dei reati fino alla pronuncia della condanna ed esecuzione della pena nei confronti degli autori. Il ruolo fondamentale che i servizi nazionali di intelligence e di sicurezza svolgono a tale riguardo è incontestato. Le numerose sfide interdipendenti che la politica europea dell'informazione finalizzata al mantenimento dell'ordine pubblico intende affrontare sono presentate nei paragrafi seguenti.

Da ultimo, deve essere esaminata la dimensione esterna a causa della natura internazionale della sfida del terrorismo e del crimine organizzato che intendiamo affrontare. Altri paesi hanno sviluppato o possono sviluppare in futuro la loro politica d'informazione per il mantenimento dell'ordine pubblico ed abbiamo già visto i casi in cui queste politiche hanno implicazioni per i cittadini e gli operatori economici dell'UE. Possono anche sorgere questioni di reciprocità. Soluzioni multilaterali devono ricercarsi in forum specializzati. L'impatto che la politica dell'UE potrebbe avere sui cittadini di paesi terzo dovrà anche essere esaminato in modo appropriato, per garantire che la cooperazione di polizia e giudiziaria con questi paesi non sia indebolita e che i diritti dei cittadini siano rispettati senza discriminazione.

Inizialmente, questa politica renderà accessibili dati e informazioni necessari e pertinenti per le autorità incaricate del mantenimento dell'ordine pubblico allo scopo di prevenire e combattere il terrorismo e le altre forme di crimine grave o organizzato, come pure le minacce da essi causate. In secondo luogo, ciò stimolerà la produzione e l'utilizzo a livello UE di intelligence penale di alta qualità per supportare l'assunzione di decisioni in sede politica ed aiutare le autorità di polizia a rispondere efficacemente a questi reati. In terzo luogo, ciò favorirà l'instaurazione di un clima di fiducia tra i servizi competenti. Nello sviluppo di tale politica, si terrà conto delle politiche e degli strumenti giuridici comunitari, in particolare questa politica rispetterà pienamente i diritti fondamentali.

La politica d'informazione dovrà tenere conto dei seguenti elementi:

- La sfida della **sicurezza** rende necessaria un'azione comune e concertata ad un livello senza precedenti; le parti interessate sono gli organismi nazionali incaricati dell'applicazione della legge, i governi nazionali, i poteri esecutivo e legislativo ed altri organismi a livello europeo ed internazionale.
- La sfida della **tutela dei diritti dell'uomo** significa ricercare un adeguato equilibrio tra una protezione rigorosa dei dati e il debito rispetto degli altri diritti fondamentali da un lato e, dall'altro, un utilizzo davvero efficace delle informazioni da parte delle autorità incaricate della repressione dei reati al fine di garantire gli interessi pubblici essenziali come la sicurezza nazionale e la prevenzione, l'individuazione e il perseguimento dei reati.
- Per quanto riguarda la **tecnologia**, sono necessari sistemi d'informazione compatibili, protetti contro l'accesso illegale, che dispongano di un livello di protezione dei dati sufficiente, compreso il controllo e la sorveglianza dell'elaborazione dei dati ed il controllo delle indagini. Il lavoro sull'"analisi del rischio di esposizione al crimine" ("crime proofing") delle tecnologie dell'informazione dovrebbe includere l'esame dei punti deboli e le opportunità di utilizzare questi sistemi a fini criminali e concentrarsi sull'analisi di dati come la valutazione dei rischi ed il *profiling*.
- Per facilitare una **cooperazione** efficace, norme comuni sulla raccolta, conservazione, analisi e scambio di informazioni accresceranno notevolmente la fiducia tra i servizi competenti, sia a livello nazionale che dell'UE.
- L'**attuazione** di un approccio multifase richiederà di disporre di un'azione di cooperazione sostenuta sul lungo periodo.

CAPITOLO II – VERSO UN MIGLIORE ACCESSO AI DATI E L'INTRODUZIONE DI UN'AZIONE DI POLIZIA E GIUDIZIARIA A LIVELLO UE FONDATA SULL'INTELLIGENCE

2.1. Obiettivi strategici

L'obiettivo della presente comunicazione è istituire una politica dell'informazione UE per l'applicazione della legge, la quale contribuirà alla realizzazione degli obiettivi dell'articolo 29 TUE fornendo una migliore informazione sui canali sicuri per **la cooperazione esistente in materia di mantenimento dell'ordine pubblico e rispetto della legge** e gettando le basi dell'**istituzione di una cooperazione di polizia e giudiziaria efficace fondata sull'informazione** a livello locale, nazionale ed europeo, supportata dalla necessaria instaurazione di un **clima di reciproca fiducia**. Il piano proposto comprende misure giuridiche, tecniche e organizzative che, sinergicamente, doteranno le autorità incaricate della repressione di un quadro di cooperazione allo scopo di facilitare l'accessibilità e l'elaborazione dei dati pertinenti ai fini d'applicazione della legge e di produrre informazioni in materia penale.

Esaminando più in dettaglio la politica d'informazione, i risultati che ci si prefigge sono i seguenti:

- ottimizzare l'accesso all'informazione nel quadro di nuove attività repressive fondamentali e la produzione di informazioni in materia penale;
- garantire che i dati pertinenti raccolti a fini diversi dell'applicazione della legge siano disponibili solo fino a quando sia adeguato, necessario e proporzionato agli scopi specifici e legittimi perseguiti²;
- istituire o, qualora norme orizzontali esistano già, promuovere l'utilizzo efficace delle norme orizzontali comuni sull'accesso ai dati, l'abilitazione, la riservatezza delle informazioni, l'affidabilità, la sicurezza dei dati e la protezione dei dati, e delle norme d'interoperabilità delle basi di dati nazionali ed internazionali;
- stabilire modelli autorizzati di intelligence per assistere l'assunzione di decisioni politiche ed operative e promuovere l'elaborazione e l'utilizzo di metodi equivalenti per l'analisi in particolare delle associazioni a delinquere, delle minacce criminali, dei rischi e dei profili, da supportare ulteriormente con valutazioni dei danni economici;
- fornire la base di una definizione delle priorità della raccolta e dell'analisi delle informazioni a livello UE e, successivamente, della selezione, per le priorità così definite, della migliore via da seguire per prevenire e combattere il terrorismo ed altre forme gravi di crimine organizzato, nonché le minacce da essi causate;
- agevolare la cooperazione coordinata delle autorità competenti per l'applicazione della legge allo scopo di prevenire, indagare, o sconfiggere, in modo efficace ed appropriato, le attività terroristiche e le attività riguardanti altre forme di crimine grave o organizzato.

Un migliore accesso ai dati, all'informazione e all'intelligence aiuterà le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge in ogni Stato membro ed a livello europeo, a prevenire e combattere il terrorismo ed altre forme di

² Una proposta legislativa sulla conservazione dei dati è stata presentata da quattro Stati membri al Consiglio GAI di aprile 2004. La Commissione prevede una consultazione pubblica sulla materia.

crimine grave o organizzato, come pure le minacce da essi generate. Un valore aggiunto addizionale deriverà dall'analisi metodica dei dati al fine di produrre intelligence di prim'ordine in materia penale. A sostegno di un'applicazione della legge fondata sull'intelligence europea, occorrerebbe adottare norme minime applicabili ai sistemi nazionali di intelligence in materia penale, al fine di rendere possibili valutazioni della minaccia compatibili a livello europeo.

2.2. Elementi chiave di un accesso efficace ai dati ed alle informazioni e loro raccolta, conservazione, analisi e scambio

2.2.1. Il principio dell'accesso equivalente ai dati da parte delle autorità incaricate del mantenimento dell'ordine pubblico e del rispetto della legge

Il primo obiettivo fondamentale della politica d'informazione della struttura responsabile per il mantenimento dell'ordine pubblico e per il rispetto della legge è quello di istituire la libera circolazione dell'informazione tra le autorità responsabili, tra cui EUROPOL ed EUROJUST. Attualmente, le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge possono interrogare le basi di dati accessibili su scala nazionale. Tuttavia, l'accesso ad informazioni detenute dalle corrispondenti autorità di altri Stati membri pone delle difficoltà che, in pratica, le rendono inaccessibili.

La politica d'informazione mira a rendere accessibili in pratica queste informazioni a tutte le autorità dell'Unione competenti per l'applicazione della legge, tra cui EUROPOL ed EUROJUST, per assisterle nello svolgimento delle loro funzioni ed in conformità con i principi dello Stato di diritto.

Il diritto di accesso equivalente ai dati è il principio introdotto dalla politica d'informazione per raccogliere le sfide enunciate al capitolo precedente. Esso conferirebbe alle autorità ed agli agenti dell'Unione europea, incaricati dell'applicazione della legge, diritti equivalenti d'accesso ai dati ed alle basi di dati in altri Stati membri dell'UE a condizioni comparabili alle autorità di questo Stato membro. Il corollario di questo diritto è l'obbligo di fornire un pari accesso agli agenti di altri Stati membri nelle stesse condizioni di quelle accordate agli agenti nazionali incaricati dell'applicazione della legge.

Ciò implica un impegno degli Stati membri ad agire nell'ambito di un modello UE che comprende argomenti come la sincronizzazione della valutazione della minaccia sulla base di una metodologia comune sistematicamente sostenuta da uno studio di vulnerabilità settoriale.

Il principio dell'accesso equivalente riconosce che:

- la sicurezza dell'Unione e dei suoi cittadini è una responsabilità comune;
- gli Stati membri dipendono l'uno dall'altro nell'applicare le leggi volte a prevenire e combattere il terrorismo e altre forme di crimine grave o organizzato e nel contenere le minacce da questi generate;
- le autorità competenti per l'applicazione della legge di uno Stato membro eseguono compiti simili ed hanno necessità d'informazioni equivalenti ai loro omologhi di altri Stati membri;
- le autorità competenti per l'applicazione della legge agiscono legalmente quando accedono ai dati o quando interrogano basi di dati nell'esercizio delle loro funzioni e nei limiti fissati dalle norme comuni sulla protezione e la sicurezza dei dati.

In via di principio, il diritto di accesso equivalente non dovrà influire sugli strumenti esistenti di reciproca assistenza giudiziaria. Tuttavia, ogni conseguenza giuridica potenziale dovrà essere analizzata attentamente.

Occorre porre in essere condizioni trasparenti e semplici che disciplinino l'accesso di tutte le autorità dell'UE responsabili del mantenimento dell'ordine pubblico e del rispetto della legge a tutte le informazioni necessarie e pertinenti, sulla base di norme comuni, comprese quelle sulla protezione e la sicurezza dei dati. Gli Stati membri saranno responsabili dell'attuazione di queste condizioni. Un sistema di controllo dell'attuazione sarà realizzato dopo l'individuazione delle condizioni d'accesso nel corso dell'esercizio di bilancio (cfr. paragrafo 2.2.2).

I principali ostacoli allo scambio di informazioni tra le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge possono essere efficacemente eliminati soltanto con l'impegno fermo degli Stati membri di adottare misure concrete in vista dell'istituzione di un modello europeo di intelligence in materia penale (cfr. paragrafo 2.3).

La politica europea dell'informazione è volta all'instaurazione del principio del diritto di accesso equivalente a tutti i dati ed informazioni necessari e pertinenti per le autorità UE responsabili del mantenimento dell'ordine pubblico e del rispetto della legge. La Commissione esaminerà con gli Stati membri quali siano gli ostacoli esistenti e valuterà, su tale base, l'opportunità di presentare una proposta legislativa al Consiglio e al Parlamento europeo per la sua adozione a livello UE.

2.2.2. Delimitazione delle condizioni di accesso

La Commissione propone di procedere ad una valutazione completa sulla base delle informazioni disponibili e di quelle fornite a tal fine dagli Stati membri per raccogliere gli elementi seguenti:

- quali dati o basi di dati sono accessibili alle autorità competenti per l'applicazione della legge negli stati membri e quali sono accessibili all'estero, compresi gli indici delle basi di dati (*contenuto*);
- quale è l'obiettivo della base di dati (*definizione dell'obiettivo*);
- quale tipo d'autorità responsabile del mantenimento dell'ordine pubblico e del rispetto della legge ha accesso a questi dati (*utenti*);
- a quali condizioni queste autorità hanno accesso a tali dati e basi di dati (*protocollo d'accesso*);
- quali sono i requisiti tecnici per l'accesso a questi dati e basi di dati (*protocolli tecnici*);
- quale è la frequenza d'interrogazione di questi dati e basi di dati (*pertinenza*);
- quali dati o basi di dati presentano un interesse per le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge, ma non sono loro accessibili; quali sono le disposizioni applicabili in materia di protezione dei dati (*determinazione delle necessità*).

La Commissione intende:

- *lanciare un esercizio di valutazione entro la fine 2004, per individuare l'ambito di applicazione, le esigenze e le restrizioni all'accesso ai dati e alle basi di dati da parte delle autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge.*
- *lanciare uno studio sulle disposizioni giuridiche, sulle condizioni, comprese le soluzioni legate alle tecnologie dell'informazione, destinate o meno all'applicazione della legge e sulle procedure relative alle disposizioni in materia di protezione e sicurezza dei dati.*

2.2.3. Raccolta dei dati

Le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge nell'UE ricorrono ad approcci divergenti per raccogliere e catalogare i dati e le informazioni. Non esiste attualmente un forum unico per la classificazione della riservatezza delle varie fonti d'informazione.

I dati raccolti dalle autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge sono la fonte d'informazione per eccellenza. L'accesso ai dati che non sono raccolti a fini repressivi è un'altra questione politica. Essa richiede una consultazione ampia ed aperta con tutti gli interessati, tenuto conto delle sue implicazioni possibili sugli operatori e sulle normative e politiche comunitarie.

Un sistema di gestione dei vari diritti d'accesso quali *Norme europee comuni per l'autorizzazione d'accesso all'informazione classificata*, un sistema comune di *profili d'accesso degli utenti* per gestire i numerosi diritti d'accesso, ed un metodo autenticato di registrazione degli utenti autorizzati (cfr. *account* degli utenti) costituirebbero la base di una gestione d'accesso efficace. I profili di utenti potrebbero anche essere utilizzati per garantire un controllo sistematico e verificare l'accesso ai dati ed il loro trattamento, ai fini di conservazione in sistemi di *log files* e di pista di controllo.

La Commissione intende lanciare studi per sostenere l'elaborazione di iniziative legislative e non concernenti norme minime per la raccolta dei dati, delle norme procedurali comuni per classificare la riservatezza dei dati e la loro affidabilità, delle norme comuni sull'autorizzazione d'accesso alle informazioni classificate ed i profili d'accesso degli utenti.

La Commissione organizzerà anche consultazioni e seminari pluridisciplinari, sotto l'egida del Forum UE sulla prevenzione del crimine organizzato, per esaminare i partenariati privati/pubblici riguardanti, in particolare, l'accesso ai dati non raccolti ai fini d'applicazione della legge.

2.2.4. Scambio e trattamento dei dati

Oltre alle varie modalità di accesso ai dati e alle basi di dati sulla base del principio del pari accesso, un'altra opzione per migliorare l'accesso ai dati ed alle basi di dati esistenti passa per la loro messa in rete o per la creazione di basi di dati centrali. In questo contesto, il Consiglio europeo³ ha invitato la Commissione “a presentare proposte per migliorare l'interoperabilità fra le varie basi di dati europee e a vagliare la possibilità di sinergie tra i sistemi d'informazione attuali e futuri (SIS II, VIS ed EURODAC) per sfruttarne il valore aggiunto,

³ Consiglio europeo del 25 marzo 2004 *Dichiarazione sulla lotta al terrorismo.*

nel rispettivo ambito giuridico e tecnico, ai fini della prevenzione e del contrasto del terrorismo”⁴. Il miglioramento dell'interoperabilità richiederà la considerazione delle disposizioni legali applicabili in materia di protezione dei dati.

La Commissione ritiene che la sola opzione valida in futuro sia la creazione di sistemi compatibili ed interconnessi nell'UE. Un'architettura informatica basata su un concetto globale che integri interconnessioni nazionali, europee ed internazionali offre a lungo termine economie, sinergie ed opportunità d'azione considerevoli, tanto nel settore dell'intelligence in materia penale che nel contesto più ampio di una strategia europea di sicurezza in via di evoluzione.

Occorre concepire un approccio graduale, basato sulla messa a punto di modelli armonizzati di codifica di dati e di norme di accesso per i vari sistemi. Le prime consultazioni condotte dalla Commissione europea con le parti interessate⁵ hanno già permesso di identificare un certo numero di punti suscettibili di ostacolare la condivisione di informazioni. Si tratta in particolare dell'assenza dei seguenti elementi:

- norme e condizioni comuni per l'elaborazione dei dati;
- norme comuni d'accessibilità ai dati;
- definizioni penali e statistiche criminali compatibili;
- tecnologie dell'informazione compatibili in uso nelle amministrazioni incaricate dell'applicazione della legge;
- culture di cooperazione delle autorità responsabili con il mantenimento dell'ordine pubblico e del rispetto della legge al di là delle frontiere istituzionali;
- cooperazione tra soggetti dei settori pubblici e privati;
- consapevolezza delle norme comuni di protezione e assenza di un quadro comune di sicurezza dei dati.

La Commissione prevede di presentare una comunicazione che individui mezzi efficaci per eliminare i principali ostacoli alla condivisione dei dati e che, se necessario, sarà sostenuta dalle rispettive iniziative legislative.

2.2.5. Ricerca

I programmi di ricerca europei attuali affrontano la questione della sicurezza dell'informazione, dei sistemi di comunicazione e delle infrastrutture. La Commissione ha già ritenuto la necessità di accelerare la preparazione del programma europeo di ricerca sulla sicurezza per migliorare la sicurezza dei cittadini europei lanciando un'azione preparatoria nel campo della ricerca in materia di sicurezza⁶. L'azione preparatoria nel campo della ricerca in materia di sicurezza, per gli anni 2004-2006, (budget 65 milioni di euro) sosterrà e finanzierà attività volte a sondare il terreno al fine di istituire un programma globale europeo di ricerca sulla sicurezza dal 2007 in poi.

Il terrorismo ed il crimine organizzato sono identificati come le due preoccupazioni principali dei cittadini europei (l'80% dei cittadini UE considera il terrorismo ed il crimine organizzato come i loro principali motivi di preoccupazione). Attualmente, le attività di ricerca che riguardano i sistemi di intelligence in materia penale o di applicazione della legge non sono

⁴ Una distinta comunicazione della Commissione sarà approntata sull'argomento.

⁵ Dichiarazione di Dublino e conclusioni degli incontri del Forum sulla prevenzione del crimine organizzato.

⁶ COM (2004) 72 definitivo.

sufficientemente coperte dai programmi di ricerca. Di conseguenza, occorre definire azioni specifiche di ricerca in aggiunta ai programmi esistenti. Inoltre, il cofinanziamento delle attività di ricerca è possibile anche nel quadro del programma AGIS.

- *promuovere la ricerca sui canali di comunicazione sicuri e confidenziali tramite il programma AGIS;*
- *intraprendere lo sviluppo di norme applicabili ad un sicuro scambio di informazioni, particolarmente da parte delle autorità competenti per l'applicazione della legge e tra esse;*
- *lanciare ricerche specifiche sull'utilizzo e l'attuazione di sistemi europei di intelligence in materia penale, compresi quelli relativi agli standard comuni per i metadati, la protezione degli scambi di dati, il miglioramento degli strumenti di protezione dei dati, l'analisi automatizzata, la valutazione della minaccia e dei rischi ed i metodi di profiling.*

2.3. Elementi fondamentali di un'efficace applicazione della legge fondata sull'intelligence a livello europeo

Il secondo obiettivo fondamentale della politica d'informazione consiste nel proporre misure tendenti a sviluppare nell'UE un'applicazione della legge fondata sulle informazioni. L'intelligence in materia penale aiuta le autorità competenti a svolgere le loro missioni strategiche o operative, per prevenire e combattere il terrorismo e altre forme di crimine grave o organizzato, come pure le minacce da essi generate⁷. L'introduzione di un modello europeo di intelligence in materia penale renderebbe effettiva un'azione di polizia e giudiziaria fondata sulle informazioni e permetterebbe una cooperazione rafforzata. Esso dovrebbe comprendere temi come la sincronizzazione della valutazione della minaccia basata su una metodologia comune sistematicamente sostenuta da uno studio di vulnerabilità per settori, nonché le risorse umane e finanziarie necessarie.

La politica europea d'informazione ai fini dell'applicazione della legge mira a **rendere disponibili le informazioni necessarie ad una rete europea di intelligence in materia penale** allo scopo di creare un'intelligence in materia penale di prim'ordine a livello UE, che si focalizzi sulla produzione regolare di valutazioni strategiche ed operative UE. Anche la disponibilità del sistema d'informazione EUROPOL svolgerà un ruolo importante nello sviluppo di questa capacità europea di informazioni.

Le misure descritte qui di seguito dovrebbero condurre ad una situazione nella quale le valutazioni strategiche siano facilmente accessibili per le istanze decisionali ai fini della revisione delle priorità politiche, tutte le volte che ciò sia necessario. Inoltre, le valutazioni operative sarebbero a disposizione della task-force dei capi di polizia (TFCP) ed offrirebbero il migliore stato delle conoscenze tattiche disponibili per prevenire o combattere le minacce o la criminalità, compreso il terrorismo, conformemente alle priorità stabilite dal Consiglio.

Attualmente, le autorità responsabili del mantenimento dell'ordine pubblico e del rispetto della legge nell'UE non sono guidate da un'intelligence in materia penale che consideri globalmente la sicurezza dell'UE. Esiste oggi la necessità urgente di proteggere i cittadini dell'Unione contro nuovi rischi e minacce per la sicurezza. Di conseguenza, è imperativo

⁷ L'intelligence penale si suddivide in intelligence strategica e operativa (o tattica). L'intelligence strategica accerta *quali* siano le minacce ed i reati da considerare e l'intelligence operativa fornisce l'orientamento tattico per determinare *come* trattarli nel miglior modo possibile e classificarli per ordine di priorità.

disporre rapidamente di valutazioni strategiche ed operative europee. Inoltre, lo scambio di informazioni dovrebbe essere assoggettato al principio dello Stato di diritto ed al rispetto dei diritti fondamentali degli individui.

Si prevede quindi un approccio in due fasi:

- A breve termine, i servizi di intelligence penale degli Stati membri dovrebbero riunirsi su base mensile sotto la possibile egida di EUROPOL e discutere delle loro valutazioni strategiche ed operative nazionali. EUROPOL dovrebbe fornire tutte le informazioni di cui può disporre. L'intelligence risultante dovrebbe essere collazionata per produrre valutazioni strategiche europee, ad esempio due volte all'anno, e valutazioni operative europee ogni mese. Le valutazioni strategiche europee permetterebbero al Consiglio di fissare priorità in materia d'applicazione della legge. La TFCP dovrebbe trasmettere le valutazioni operative a livelli operativi nelle Comunità nazionali responsabili per il mantenimento dell'ordine pubblico e per il rispetto della legge.

Ciò dovrebbe, nella prima fase, basarsi sulle informazioni alle quali i servizi di intelligence penale degli Stati membri ed EUROPOL possono legalmente accedere ai sensi della legislazione attuale ed utilizzare strumenti analitici disponibili.

- A più lungo termine, i servizi nazionali di intelligence penale potranno iniziare a produrre intelligence penale per mezzo di strumenti analitici standardizzati sulla base dei dati pertinenti all'applicazione della legge disponibili all'interno dell'Unione.

L'importanza di EUROPOL ne verrebbe accresciuta, in quanto i dati e le procedure diverrebbero più europei. Ciò comporterebbe un'intelligence penale di migliore qualità poiché sarebbe più standardizzata e di conseguenza maggiormente comprensibile. Le relazioni tra EUROPOL, il Consiglio e la TFCP dovranno adattarsi al mutamento di circostanze. A quel punto, l'UE sarà in grado di affermarsi sulla scena internazionale come un partner in materia di mantenimento dell'ordine pubblico dotato di caratteristiche e qualità proprie.

La Commissione prevede di studiare le misure necessarie per istituire, in tempo utile, un sistema di produzione di valutazioni affidabili in materia di intelligence penale e presentare una relazione al Consiglio entro la fine del 2005.

Le priorità saranno stabilite dal Consiglio sulla base delle valutazioni strategiche sviluppate dal Gruppo di intelligence penale. Queste valutazioni operative dovrebbero permettere di ottenere risultati specifici, come arresti, sequestri o confische di beni provenienti da attività criminali o lo spiegamento di sforzi miranti a smantellare un'organizzazione criminale.

I metodi di intelligence generalmente utilizzati dovrebbero essere ridisegnati in modo da essere utilizzabili non soltanto a livello UE, ma anche per entrare in relazione con istanze sopranazionali o regionali specifiche (ad esempio la task-force del Mar Baltico sul crimine organizzato). La Commissione ed EUROPOL dovrebbero intraprendere uno studio dei diversi metodi utilizzati negli organismi di intelligence penale degli Stati membri e proporre entro la fine del 2005 una metodologia analitica europea di intelligence penale. Parallelamente, il CEPOL potrebbe essere invitato a chiedere ai suoi membri di stabilire un programma di formazione per insegnare agli analisti criminali ad utilizzare questi metodi ed ai dirigenti a

trarre il migliore vantaggio dalle valutazioni operative. I metodi analitici generalmente usati⁸ dovrebbero generare risultati che possano servire a produrre valutazioni strategiche ed operative a livello UE.

- *Le idee di questa comunicazione dovrebbero essere approvate dal Consiglio ai fini dell'adozione di misure idonee per la loro attuazione.*
- *Sotto l'egida di Europol, i rappresentanti dei servizi di intelligence penale degli Stati membri dovrebbero assemblare le valutazioni strategiche ed operative nazionali.*
- *Il Consiglio potrebbe invitare gli Stati membri a mettere a disposizione di Europol l'intelligence e dare mandato ad Europol di elaborare una valutazione globale della minaccia. I servizi delle dogane e le autorità responsabili dei controlli alle frontiere potrebbero essere incaricati di coordinare con Europol l'elaborazione della loro intelligence.*
- *Dovrebbero essere elaborate definizioni comuni in materia di statistiche criminali e norme comuni di resoconto, sulla base di proposte adeguate.*
- *Dovrebbero essere messi a punto, eventualmente sotto l'egida di Europol, metodi comuni d'analisi in previsione della produzione di informazioni a livello UE.*

2.4. Instaurazione di un clima di fiducia

Il terzo obiettivo chiave della politica dell'informazione è contribuire all'instaurazione di un clima di fiducia tra le autorità europee incaricate dell'applicazione della legge, funzionari e collaboratori istituendo una piattaforma comune di valori condivisi, standard normativi e orientamenti politici.

L'introduzione di standard normativi comuni è cruciale per creare un ambiente fidato per la raccolta, l'accesso e lo scambio di informazioni (vedasi in particolare la sezione 2.2). Le norme comuni sull'accesso ai dati ed il loro trattamento, così come metodologie compatibili in materia di valutazione della minaccia, rischi e profili diventeranno una base indispensabile per l'effettiva condivisione di informazioni e intelligence a livelli strategici ed operativi. Queste misure saranno efficaci soltanto a condizione di un appoggio politico duraturo all'attuazione **di uno spazio comune di applicazione della legge** nell'UE, basato su sistemi nazionali compatibili di intelligence penale che formeranno insieme un modello europeo d'intelligence penale concettualmente integrato.

Di conseguenza, occorre sviluppare i rapporti formali ed informali di lavoro per garantire il funzionamento del sistema. La formazione del personale responsabile del mantenimento dell'ordine pubblico e del rispetto della legge al fine di condividere una comprensione comune dell'intelligence penale contribuirà a sviluppare questi aspetti. Il CEPOL dovrebbe svolgere un ruolo importante in questo contesto, in particolare attraverso i seguenti elementi: seguenti:

- istituzione di corsi di formazione su base regolare per potenziali futuri responsabili politici ed amministratori di alto livello;

⁸ I metodi sono: le analisi nel settore dei risultati, gli schemi criminali, i mercati criminali, le reti criminali, i rischi (utilizzati come strumento di gestione in quanto tale), i profili obiettivi (spesso detto "profiling"), i profili di attività criminali e le tendenze demografiche e sociali.

- elaborazione di un piano di studi tipo per la formazione dei quadri intermedi nelle questioni di intelligence penale europea a livello nazionale;
- attuazione di misure di formazione connesse a tutti gli elementi della politica d'informazione UE.

Altre misure rafforzeranno gli sforzi di collaborazione, compresi quelli basati su strumenti già esistenti come le valutazioni reciproche, progetti dedicati nell'ambito del programma AGIS o attività svolte sotto gli auspici del Forum sulla prevenzione del crimine organizzato.

Infine, il ruolo delle autorità nazionali di supervisione dei dati dovrebbe essere tenuto in debito conto, in quanto esse contribuiscono a porre le necessarie garanzie a sostegno dello Stato di diritto e svolgono un effettivo controllo democratico.

Misure e tecniche atte a costituire un clima di fiducia sono di fondamentale importanza (standard normativi comuni e metodologie). La Commissione prevede di presentare proposte entro la fine del 2005.

Nel contempo, il Consiglio invita il CEPOL ad intraprendere lo sviluppo di un piano di studi comune per la formazione dei funzionari addetti all'intelligence.

CAPITOLO III – INIZIATIVE LEGISLATIVE CONNESSE ALLA PRESENTE COMUNICAZIONE

La Commissione continuerà a sviluppare la sua politica, comprese le iniziative legislative, nelle aree collegate della protezione dei dati personali nell'ambito del terzo pilastro e l'uso delle informazioni sui passeggeri, quest'ultimo in conformità ai principi esposti nella comunicazione della Commissione del dicembre 2003⁹.

La proposta relativa ad una decisione quadro sui dati istituirà standard comuni per il trattamento dei dati personali scambiati nell'ambito del titolo VI del trattato sull'Unione europea allo scopo di permettere l'accesso a tutti i dati rilevanti per l'applicazione della legge da parte della polizia e delle autorità giudiziarie nel rispetto dei diritti fondamentali. Questa decisione quadro fornirà un quadro unico generale per la protezione dei dati per prevenire, scoprire, indagare e perseguire i reati e le minacce alla sicurezza. Esso stabilirà un quadro per le disposizioni più specifiche contenute nei vari strumenti giuridici adottati a livello UE e ridurrà ulteriormente le differenze nella prassi dello scambio di informazioni tra Stati membri, da un lato, e tra Stati membri e paesi terzi, dall'altro, inserendola in un meccanismo che assicuri la protezione dei diritti fondamentali.

⁹ COM (2003) 826 definitivo del 16.12.03 Comunicazione della Commissione al Consiglio e al Parlamento europeo - Trasferimento di dati di identificazione delle pratiche (PNR): un approccio globale dell'UE.