



Strasburgo, 16.5.2017
COM(2017) 261 final

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

**Settima relazione sui progressi compiuti verso un'autentica ed efficace Unione della
sicurezza**

I. INTRODUZIONE

La presente è la settima relazione mensile sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza, e verte sugli sviluppi attinenti a due pilastri principali: affrontare il problema del terrorismo, della criminalità organizzata e dei relativi mezzi di sostegno e rafforzare le nostre difese e la nostra resilienza contro tali minacce. La presente relazione si concentra sui lavori svolti per rendere interoperabili i sistemi d'informazione per la gestione della sicurezza, delle frontiere e della migrazione al fine di aumentare l'efficacia e l'efficienza della gestione dei dati nell'UE, nel pieno rispetto dei requisiti in materia di protezione dei dati, onde proteggere meglio le frontiere esterne e rafforzare la sicurezza interna, a beneficio di tutti i cittadini. La presente relazione inoltre aggiorna sui progressi compiuti in merito ai principali fascicoli legislativi e non legislativi.

Il recente attacco informatico ransomware globale, che ha disattivato migliaia di sistemi informatici, ha messo nuovamente in luce l'urgenza di rafforzare la resilienza informatica dell'UE e le azioni di sicurezza, considerato il rapido e crescente aumento della criminalità organizzata nel cibernazio, come indicato nell'ultima relazione sui progressi dell'Unione della sicurezza¹ e sottolineato nella valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità effettuata da Europol². La Commissione sta accelerando i lavori in materia di cibersicurezza, in particolare attraverso la revisione della strategia dell'UE per la cibersicurezza del 2013³, annunciata nella revisione intermedia dell'attuazione della strategia per il mercato unico digitale⁴, al fine di dare una risposta attuale ed efficace a tali minacce.

Il discorso del presidente Juncker sullo stato dell'Unione del settembre 2016⁵ e le conclusioni del Consiglio europeo del dicembre 2016⁶ hanno sottolineato l'importanza di colmare le attuali lacune nella gestione dei dati e di migliorare l'interoperabilità dei sistemi d'informazione esistenti. I recenti attentati terroristici hanno messo ancora più in rilievo questa esigenza, evidenziando l'urgente necessità di rendere interoperabili i sistemi d'informazione e di eliminare le attuali zone d'ombra che permettono alle persone sospettate di terrorismo di essere registrate sotto nomi diversi in banche dati diverse non collegate tra loro. La presente relazione illustra l'approccio della Commissione **per garantire l'interoperabilità dei sistemi d'informazione per la gestione della sicurezza, delle frontiere e della migrazione entro il 2020** affinché le guardie di frontiera, i funzionari delle autorità di contrasto, compresi quelli delle amministrazioni doganali, i funzionari dei servizi per l'immigrazione e le autorità giudiziarie possano disporre delle informazioni necessarie. La presente relazione si situa su una linea di continuità con la comunicazione della Commissione "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza"⁷ dell'aprile 2016 e i lavori del gruppo di esperti ad alto livello sui sistemi d'informazione e l'interoperabilità, istituito dalla Commissione in seguito a tale comunicazione.

¹ COM(2017) 213 final del 12.4.2017.

² <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>.

³ JOIN(2013) 1 final del 7.2.2013.

⁴ COM(2017) 228 final del 10.5.2017. Cfr. anche la quarta relazione sui progressi dell'Unione della sicurezza, COM(2017) 41 final del 25.1.2017.

⁵ Stato dell'Unione 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_it.

⁶ Conclusioni del Consiglio europeo del 15.12.2016, http://www.consilium.europa.eu/it/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

⁷ COM(2016) 205 final del 6.4.2016.

II. SISTEMI D'INFORMAZIONE PIÙ SOLIDI E INTELLIGENTI

1. *Comunicazione della Commissione dell'aprile 2016 e iniziative intraprese finora*

La comunicazione "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza", pubblicata nell'aprile 2016, ha individuato una serie di carenze strutturali connesse ai sistemi d'informazione:

- funzionalità non ottimali di alcuni sistemi d'informazione esistenti;
- lacune informative nell'architettura della gestione dei dati dell'UE;
- complessità dovuta all'esistenza di sistemi d'informazione gestiti in maniera diversa;
- architettura frammentata della gestione dei dati per il controllo delle frontiere e la sicurezza, in cui le informazioni sono archiviate separatamente in sistemi non interconnessi, con conseguenti zone d'ombra.

Per porre rimedio a tali lacune **la Commissione ha proposto di intervenire in tre settori**, sottolineando che le disposizioni della Carta dei diritti fondamentali e, soprattutto, il quadro globale per la protezione dei dati personali nell'UE, guideranno i lavori della Commissione.

In primo luogo, la comunicazione indica possibili opzioni per **massimizzare i benefici dei sistemi d'informazione esistenti, sottolineando che gli Stati membri devono usare appieno questi sistemi**. Nel dicembre 2016 la Commissione ha presentato proposte legislative per rafforzare il sistema d'informazione Schengen (SIS)⁸, attualmente lo strumento più utile per la cooperazione tra le guardie di frontiera, le autorità doganali, i funzionari di polizia e le autorità giudiziarie. Nel maggio 2016 aveva presentato una proposta legislativa per rafforzare Eurodac⁹, la banca dati nel settore dell'asilo e della migrazione irregolare, al fine di agevolare i rimpatri e contribuire a combattere la migrazione irregolare. Inoltre nel gennaio 2016 aveva presentato una proposta legislativa per facilitare lo scambio all'interno dell'UE dei casellari giudiziari di cittadini di paesi terzi potenziando il sistema europeo di informazione sui casellari giudiziari (ECRIS)¹⁰. Come annunciato¹¹, e alla luce delle discussioni con i colegislatori sulla proposta del gennaio 2016, la Commissione prevede di presentare nel giugno 2017 un'ulteriore proposta per istituire un sistema centralizzato¹² per identificare i cittadini di paesi terzi condannati e gli Stati membri che posseggono informazioni che li riguardano.

Nel giugno 2017 la Commissione presenterà una proposta legislativa per rivedere il mandato giuridico di eu-LISA¹³ ed estenderlo allo sviluppo dell'interoperabilità dei sistemi d'informazione centralizzati dell'UE per la gestione della sicurezza, delle frontiere e della migrazione.

In secondo luogo, la comunicazione indica possibili opzioni per **elaborare nuove azioni complementari per colmare le lacune nell'architettura della gestione dei dati dell'UE**. In

⁸ COM(2016) 881 final del 21.12.2016, COM(2016) 882 final del 21.12.2016 e COM(2016) 883 final del 21.12.2016.

⁹ COM(2016) 272 final del 4.5.2016.

¹⁰ COM(2016) 7 final del 19.1.2016.

¹¹ Cfr. la quinta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 203 final del 2.3.2017.

¹² Quando uno Stato membro cerca informazioni sulla condanna di un cittadino di un paese terzo il sistema centralizzato lo orienta verso gli Stati membri in possesso di informazioni estratte dai casellari giudiziari.

¹³ Agenzia europea per la gestione operativa dei sistemi di tecnologia dell'informazione su larga scala del settore della libertà, della sicurezza e della giustizia.

particolare, la Commissione ha rilevato notevoli carenze di informazioni sui cittadini di paesi terzi che si recano nello spazio Schengen e, all'interno di questo gruppo, sui cittadini di paesi terzi esenti dall'obbligo del visto che entrano nell'UE per via terrestre. Attualmente gli attraversamenti delle frontiere esterne da parte dei cittadini di paesi terzi non sono registrati, e non sono disponibili informazioni sui cittadini di paesi terzi esenti dall'obbligo del visto prima del loro arrivo a una frontiera esterna terrestre. Per colmare queste importanti lacune la Commissione ha presentato proposte legislative per istituire due nuovi sistemi d'informazione. Nell'aprile 2016 ha proposto un sistema di ingressi/uscite dell'UE per modernizzare la gestione delle frontiere esterne migliorando la qualità e l'efficacia dei controlli¹⁴. Nel novembre 2016 ha proposto un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) per raccogliere informazioni sulle persone esenti dall'obbligo di visto che si recano nell'Unione europea e poter effettuare preventivamente i controlli in materia di migrazione irregolare e sicurezza¹⁵.

In terzo luogo, la comunicazione evidenzia la **necessità di migliorare l'interoperabilità dei sistemi d'informazione**. La comunicazione rileva che grazie al nuovo quadro generale per la protezione dei dati personali nell'UE e ai significativi progressi nel campo delle tecnologie e della sicurezza informatica, c'è modo per conseguire l'interoperabilità dei sistemi d'informazione, con il necessario rigore delle norme in materia di accesso e utilizzo, senza compromettere l'attuale principio di limitazione delle finalità. La comunicazione indica **quattro opzioni** per conseguire l'interoperabilità:

- **un'interfaccia di ricerca unica** per l'interrogazione contemporanea di diversi sistemi d'informazione, che consente di ottenere risultati combinati su una sola schermata;
- **l'interconnettività dei sistemi d'informazione**, grazie alla quale i dati registrati in un sistema vengono consultati automaticamente da un altro sistema;
- la creazione di **un servizio comune di confronto biometrico** a sostegno dei vari sistemi d'informazione;
- un **archivio comune di dati relativi all'identità**, basato su dati alfanumerici, per i diversi sistemi d'informazione (comprendente dati anagrafici comuni quali nome e data di nascita).

La Commissione ha avviato una riflessione sul modo in cui i sistemi d'informazione dell'Unione europea possono rafforzare la gestione delle frontiere e la sicurezza interna e ha istituito un gruppo di esperti ad alto livello sui sistemi d'informazione e l'interoperabilità per portare avanti questi lavori (cfr. sezione II.3).

2. *Progressi compiuti sui fascicoli prioritari riguardanti i sistemi d'informazione*

Per svolgere il loro lavoro, le guardie di frontiera, i funzionari delle autorità di contrasto, i funzionari dei servizi per l'immigrazione e le autorità giudiziarie hanno bisogno di accedere a dati esatti e completi. **È pertanto fondamentale che il Parlamento europeo e il Consiglio portino avanti le proposte prioritarie relative ai sistemi d'informazione** nel quadro del primo aspetto della comunicazione della Commissione dell'aprile 2016. Come indicato sopra, questo è essenziale per rendere i sistemi d'informazione esistenti più efficaci per la gestione delle frontiere e della sicurezza, e per colmare le importanti lacune informative mediante l'istituzione di nuovi sistemi necessari per rendere sicure le frontiere esterne.

¹⁴ COM(2016) 194 final del 6.4.2016.

¹⁵ COM(2016) 731 final del 16.11.2016.

La proposta allo stadio più avanzato è quella relativa al **sistema di ingressi/uscite dell'UE**, attualmente in fase di trilogio. Il calendario fissato dal Consiglio europeo per la sua adozione nel giugno 2017 finora è rispettato. Le discussioni tecniche sul **sistema europeo di informazione e autorizzazione ai viaggi** (ETIAS) proseguono, ma le due istituzioni devono ancora stabilire le rispettive posizioni di negoziato. L'adozione del mandato del Consiglio è prevista per giugno 2017, mentre la commissione del Parlamento europeo per le libertà civili, la giustizia e gli affari interni (LIBE) prevede di adottare il suo mandato negoziale nel settembre 2017. La dichiarazione comune sulle priorità legislative dell'UE per il 2017¹⁶ ha accordato priorità a questo fascicolo per garantirne l'adozione entro la fine del 2017. La Commissione continuerà a sostenere i legislatori per raggiungere questo obiettivo. Le due istituzioni stanno inoltre lavorando alle proposte della Commissione volte a rafforzare il **sistema d'informazione Schengen** (SIS). Il primo ciclo di discussioni sulle tre proposte a livello di gruppo di lavoro del Consiglio si concluderà durante la presidenza maltese del Consiglio. Il relatore del Parlamento europeo prevede di presentare un progetto di relazione alla commissione per le libertà civili, la giustizia e gli affari interni (LIBE) entro fine giugno 2017. Per quanto riguarda la proposta legislativa per rafforzare **Eurodac**, il Consiglio ha convenuto un approccio generale parziale nel dicembre 2016, mentre la commissione del Parlamento europeo per le libertà civili, la giustizia e gli affari interni (LIBE) prevede di votare la sua relazione nel maggio 2017. La fase di trilogio dovrebbe iniziare subito dopo.

3. Lavori del gruppo di esperti ad alto livello sui sistemi d'informazione e l'interoperabilità

Nel giugno 2016 la Commissione ha istituito il gruppo di esperti ad alto livello sui sistemi d'informazione e l'interoperabilità, incaricandolo di **affrontare gli aspetti giuridici, tecnici e operativi delle quattro opzioni** per l'interoperabilità, tra cui la loro necessità, fattibilità tecnica e proporzionalità e le loro implicazioni in termini di protezione dei dati¹⁷. Il gruppo di esperti è stato inoltre incaricato di individuare e affrontare le carenze e le potenziali lacune informative dovute alla complessità e alla frammentazione dei sistemi d'informazione¹⁸. Il gruppo ha riunito esperti degli Stati membri e di paesi associati a Schengen e delle agenzie dell'UE eu-LISA, Europol, Ufficio europeo di sostegno per l'asilo, Agenzia europea della guardia di frontiera e costiera e Agenzia per i diritti fondamentali. Il coordinatore antiterrorismo dell'UE e il garante europeo della protezione dei dati hanno partecipato in qualità di membri a pieno titolo. I rappresentanti del segretariato della commissione del Parlamento europeo per le libertà civili, la giustizia e gli affari interni (LIBE) e del Segretariato generale del Consiglio hanno partecipato in qualità di osservatori.

La Commissione si compiace della relazione finale¹⁹ del gruppo di esperti ad alto livello dell'11 maggio 2017. Il gruppo di esperti ha concluso che **è necessario e tecnicamente fattibile lavorare per realizzare le tre seguenti soluzioni in materia di interoperabilità e**

¹⁶ Dichiarazione comune sulle priorità legislative dell'UE per il 2017, del 13.12.2016, https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.

¹⁷ Decisione 2016/C 257/03 della Commissione del 17.6.2016.

¹⁸ Cfr. il documento di orientamento del gruppo di esperti (giugno 2016): <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2>.

¹⁹ La relazione finale del gruppo di esperti è consultabile al seguente indirizzo: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>. I suoi allegati comprendono una sintesi di una relazione dell'Agenzia per i diritti fondamentali e le dichiarazioni del garante europeo della protezione dei dati e del coordinatore antiterrorismo dell'UE.

che tali soluzioni possono, in linea di principio, **offrire vantaggi operativi** ed essere istituite **nel rispetto dei requisiti in materia di protezione dei dati**:

- un portale di ricerca europeo²⁰,
- un servizio comune di corrispondenza biometrica,
- un archivio comune di dati relativi all'identità.

Il gruppo di esperti ritiene che l'opzione dell'interconnettività dei sistemi dovrebbe essere presa in considerazione solo caso per caso. Uno di questi casi è l'interconnessione del proposto sistema di ingressi/uscite dell'UE e del sistema d'informazione visti²¹. La proposta della Commissione relativa al sistema di ingressi/uscite dell'UE prevede che detto sistema consulti sistematicamente e automaticamente i dati contenuti nel sistema d'informazione visti e ne conservi una piccola parte (visto adesivo, numero di ingressi, durata del soggiorno) in modo da poter trattare i dati sui titolari di visto in conformità ai requisiti in materia di minimizzazione dei dati e coerenza dei dati. Il gruppo di esperti ha ritenuto che, se vengono conseguiti progressi sufficienti riguardo alle altre tre soluzioni per l'interoperabilità, l'esigenza di interconnettività tra sistemi per il solo motivo di migliorare lo scambio di dati è meno necessaria.

La relazione finale del gruppo di esperti ha inoltre sottolineato **l'importanza della piena attuazione e applicazione dei sistemi d'informazione esistenti**. Ha inoltre esaminato il **quadro di Prüm** decentrato per lo scambio di dati riguardanti il DNA, le impronte digitali e l'immatricolazione dei veicoli²², raccomandando uno studio di fattibilità del passaggio a una componente di inoltro centralizzato e dell'eventuale aggiunta di nuove funzionalità. Per quanto riguarda il sistema decentrato istituito dalla **direttiva UE sul codice di prenotazione (PNR)**²³, il gruppo di esperti ha raccomandato uno studio di fattibilità di una componente centralizzata per le informazioni anticipate sui passeggeri e i dati del codice di prenotazione quale strumento di supporto tecnico per agevolare la connettività con i vettori aerei. Il gruppo di esperti ha considerato che in questo modo si rafforzerebbe l'efficacia delle Unità d'informazione sui passeggeri una volta che gli Stati membri avranno attuato la direttiva UE sul codice di prenotazione (PNR).

La Commissione continuerà a concentrarsi sulla **piena attuazione dei sistemi d'informazione esistenti**. È essenziale che gli Stati membri facciano pieno uso dei sistemi esistenti, sfruttandone integralmente il potenziale. La Commissione continuerà a fornire un sostegno globale, in linea con il suo piano di attuazione²⁴, per contribuire affinché tutti gli Stati membri attuino la direttiva UE sul codice di prenotazione (PNR) entro maggio 2018. La Commissione collaborerà strettamente con tutti gli Stati membri per la realizzazione completa del quadro di Prüm, in particolare con i cinque Stati membri che devono ancora attuare le decisioni di Prüm. Nello spirito delle raccomandazioni del gruppo di esperti, la Commissione esaminerà il modo per rafforzare il funzionamento e l'efficacia di questi sistemi nella loro applicazione da parte degli Stati membri.

²⁰ L'espressione "interfaccia di ricerca unica" è stata modificata in "portale di ricerca europeo" per evitare qualsiasi confusione con le interfacce di ricerca unica nazionali che esistono negli Stati membri per i sistemi d'informazione nazionali.

²¹ Regolamento (CE) n. 767/2008 del 9.7.2008.

²² Decisione 2008/615/GAI della Commissione del 23.6.2008.

²³ Direttiva (UE) 2016/681 del 27.4.2016.

²⁴ SWD(2016) 426 final del 28.11.2016.

Il gruppo di esperti ha individuato una **carenza di informazioni sugli attraversamenti delle frontiere esterne da parte dei cittadini dell'UE**. La sua relazione finale fa riferimento alla recente introduzione di verifiche sistematiche nelle banche dati pertinenti su tutti i beneficiari del diritto alla libera circolazione ai sensi del diritto dell'Unione al momento dell'uscita o dell'ingresso nello spazio Schengen²⁵. Essa sottolinea che la data e il luogo di tali verifiche non sono registrati e rileva che queste informazioni potrebbero rivelarsi utili a fini di contrasto. Il gruppo di esperti raccomanda pertanto un'ulteriore analisi della proporzionalità e della fattibilità di una registrazione sistematica degli attraversamenti delle frontiere esterne di tutti i cittadini dell'UE²⁶.

La Commissione osserva che la relazione del gruppo di esperti non dimostra la necessità e la proporzionalità di registrare gli attraversamenti delle frontiere esterne di tutti i cittadini dell'UE. Qualora dovessero emergere nuovi elementi che lo dimostrano, la Commissione valuterà l'opportunità di ulteriori azioni. Nel frattempo, esaminerà la raccomandazione del gruppo di esperti relativa all'eventuale registrazione dei riscontri positivi ("hit") ottenuti nel sistema d'informazione Schengen su persone segnalate, come possibile modo per registrare gli spostamenti dei cittadini dell'UE che sono sospettati di terrorismo o di altre forme gravi di criminalità.

Il gruppo di esperti ha inoltre identificato una **carenza di informazioni sui visti per soggiorni di lunga durata, sui permessi di soggiorno e sulle carte di soggiorno**. Ha osservato che gli Stati membri hanno pochi mezzi per controllare la validità di questi documenti rilasciati da altri Stati membri, e suggerisce che si potrebbe esplorare la soluzione di un archivio centralizzato dell'UE contenente informazioni sui visti per soggiorni di lunga durata, i permessi di soggiorno e le carte di soggiorno. La Commissione valuterà l'esigenza di un tale archivio, compresa la sua necessità, fattibilità tecnica e proporzionalità.

Infine, la relazione del gruppo di esperti dichiara che le **autorità doganali** sono soggetti imprescindibili nella cooperazione tra agenzie alle frontiere esterne. Pertanto, la Commissione sta valutando gli aspetti tecnici, operativi e giuridici dell'interoperabilità con i sistemi doganali.

III. VERSO L'INTEROPERABILITÀ DEI SISTEMI D'INFORMAZIONE

1. L'obiettivo della Commissione di garantire l'interoperabilità dei sistemi d'informazione entro il 2020

L'obiettivo di base è assicurare che le guardie di frontiera, i funzionari delle autorità di contrasto, i funzionari dei servizi per l'immigrazione e le autorità giudiziarie dispongano delle informazioni necessarie per proteggere meglio le frontiere esterne e rafforzare la sicurezza interna, a beneficio di tutti i cittadini. Per questo motivo, occorre innanzitutto garantire che i vari sistemi d'informazione in questo settore funzionino efficacemente e che le proposte legislative già sul tavolo vengano adottate rapidamente.

Come esposto nella comunicazione dell'aprile 2016 e confermato dai risultati e dalle raccomandazioni del gruppo di esperti, la Commissione delinea un **nuovo approccio alla gestione dei dati per le frontiere e la sicurezza** in base al quale tutti i sistemi

²⁵ Regolamento (UE) 2017/458 del 15.3.2017.

²⁶ Il gruppo di esperti ha inoltre discusso le opzioni di estendere il proposto sistema di ingressi/uscite dell'UE ai cittadini dell'UE o di estendere l'uso delle registrazioni del Sistema d'informazione Schengen. Entrambe le opzioni sono state scartate.

d'informazione centralizzati dell'UE per la gestione della sicurezza, delle frontiere e della migrazione²⁷ sono interoperabili, nel pieno rispetto dei diritti fondamentali, affinché:

- i sistemi possano essere consultati simultaneamente tramite un **portale di ricerca europeo**, nel pieno rispetto della limitazione delle finalità e dei diritti di accesso, al fine di fare un uso migliore dei sistemi d'informazione esistenti, eventualmente con norme più snelle per l'accesso a fini di contrasto²⁸;
- i sistemi usino un **servizio comune di confronto biometrico** che consenta di interrogare i vari sistemi d'informazione contenenti dati biometrici, eventualmente con segnalatori "hit/no hit" che indichino il collegamento con dati biometrici correlati presenti in un altro sistema²⁹;
- i sistemi condividano un **archivio comune di dati relativi all'identità** contenente dati identificativi alfanumerici³⁰, che consenta di individuare se una persona è registrata con identità multiple in banche dati diverse.

Questo nuovo approccio deve garantire che i sistemi mantengano le loro **disposizioni specifiche in materia di protezione dei dati**, corredate da norme specifiche per l'accesso delle autorità competenti, norme distinte sulla limitazione delle finalità per ciascuna categoria di dati e apposite norme sulla conservazione dei dati. Questo approccio all'interoperabilità non porterebbe all'interconnessione di tutti i singoli sistemi.

Esso compenserebbe gli attuali punti deboli dell'architettura della gestione dei dati dell'UE ed eliminerebbe le zone d'ombra individuate. **eu-LISA** svolgerà un ruolo fondamentale nei lavori per garantire l'interoperabilità dei sistemi d'informazione, anche mediante analisi tecniche in corso e future (cfr. sezione III.2). La proposta legislativa che la Commissione presenterà nel giugno 2017 rafforzerà il mandato di eu-LISA, consentendo così di garantire l'applicazione di questo nuovo approccio. La Commissione continuerà inoltre a coinvolgere il garante europeo della protezione dei dati e l'Agenzia per i diritti fondamentali nei lavori sull'interoperabilità.

Un livello elevato di **qualità dei dati è essenziale per l'efficacia dei sistemi d'informazione**. L'interoperabilità può funzionare solo se i sistemi d'informazione sono alimentati con dati esatti e completi. La Commissione ha già riconosciuto la necessità di rafforzare l'azione dell'UE nel settore della qualità dei dati³¹. Assieme a eu-LISA attuerà con

²⁷ Il sistema d'informazione Schengen, il sistema d'informazione visti, Eurodac, il proposto sistema di ingressi/uscite dell'UE, il proposto sistema europeo di informazione e autorizzazione per i viaggi (ETIAS) e il proposto sistema europeo di informazione sui casellari giudiziari (ECRIS) per i cittadini di paesi terzi.

²⁸ Dopo aver dato mandato alla presidenza del Consiglio per l'avvio dei negoziati interistituzionali sul sistema di ingressi/uscite dell'UE il 2 marzo 2017, il Comitato dei rappresentanti permanenti del Consiglio (Coreper) ha invitato la Commissione a proporre un quadro globale per l'accesso a fini di contrasto alle varie banche dati del settore della giustizia e degli affari interni in modo da garantire una maggiore semplificazione, coerenza, efficacia e attenzione alle esigenze operative. Il gruppo di esperti raccomanda che il quadro per l'accesso a fini di contrasto si basi su un approccio a due fasi che preveda la visualizzazione effettiva dei dati solo dopo che l'esistenza dei dati stessi sia stata accertata, migliorando così l'efficacia e riducendo nel contempo il numero e la portata degli accessi a fini di contrasto.

²⁹ È necessaria un'ulteriore analisi tecnica per quanto riguarda l'eventuale inserimento di funzionalità di segnalazione in un servizio comune di corrispondenza biometrica e le implicazioni in termini di protezione dei dati (cfr. sezione III.2).

³⁰ Tra cui dati anagrafici comuni quali nome, data di nascita e genere.

³¹ Quarta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 41 final del 25.1.2017.

urgenza le raccomandazioni del gruppo di esperti per migliorare la qualità dei dati nei sistemi d'informazione dell'UE.

La Commissione porterà avanti le raccomandazioni del gruppo di esperti riguardanti il controllo di qualità automatizzato, un archivio di dati in grado di analizzare a fini statistici e di relazione dati resi anonimi estrapolati dai sistemi d'informazione pertinenti, e moduli di formazione sulla qualità dei dati per il personale incaricato di alimentare i sistemi a livello nazionale. La proposta legislativa terrà inoltre conto del ruolo importante di eu-LISA nel garantire una qualità elevata dei dati nei sistemi d'informazione centralizzati dell'UE.

L'interoperabilità richiede l'interazione tecnica tra i sistemi d'informazione esistenti. Agevolare questa interazione è l'obiettivo del **formato universale dei messaggi** (UMF) a livello dell'UE. La Commissione, di concerto con eu-LISA, porterà avanti le raccomandazioni del gruppo di esperti relative al miglioramento del formato universale dei messaggi in linea con i lavori in corso, allo scopo di garantire che lo sviluppo del formato sia preso in considerazione nei sistemi d'informazione centralizzati dell'UE.

2. Prospettive future per garantire l'interoperabilità dei sistemi d'informazione entro il 2020

Parallelamente ai lavori sui fascicoli prioritari riguardanti i sistemi d'informazione, la Commissione invita il Parlamento europeo e il Consiglio a tenere una **discussione comune sulle prospettive future** in materia di interoperabilità, come tratta la presente comunicazione. A tal fine la Commissione intende presentare e discutere queste idee con la commissione del Parlamento europeo per le libertà civili, la giustizia e gli affari interni (LIBE) il 29 maggio 2017 e con gli Stati membri l'8 giugno 2017 in occasione del Consiglio Giustizia e affari interni. Sulla base di tali discussioni, nell'autunno del 2017 le tre istituzioni dovrebbero tenere riunioni a livello tecnico tripartito³² per discutere ulteriormente le prospettive future in materia di interoperabilità, come tratta la presente comunicazione, comprese le esigenze operative per le frontiere e la sicurezza, e il modo per garantire la proporzionalità e il pieno rispetto dei diritti fondamentali. L'obiettivo è raggiungere il più rapidamente possibile, al più tardi entro la fine del 2017, un'**intesa comune sulle prospettive future** e sulle misure che dovranno essere adottate per garantire l'interoperabilità dei sistemi d'informazione entro il 2020.

Parallelamente alla discussione comune delle tre istituzioni, e senza anticiparne il risultato, nel corso del 2017 la Commissione ed eu-LISA svolgeranno **ulteriori analisi tecniche delle soluzioni individuate per l'interoperabilità**, mediante una serie di studi tecnici e prototipi. La Commissione terrà periodicamente aggiornati il Parlamento europeo e il Consiglio in merito ai progressi compiuti in tale analisi tecnica.

Facendo tesoro degli scambi con il Parlamento europeo e il Consiglio e dei risultati dell'attività legislativa in corso sui sistemi d'informazione e delle ulteriori analisi tecniche, **la Commissione si sta prodigando per presentare il prima possibile³³ una proposta legislativa sull'interoperabilità**. In linea con i principi per legiferare meglio, l'elaborazione della proposta legislativa comprenderà una consultazione pubblica e una valutazione di

³² Queste riunioni tecniche potrebbero ispirarsi alla riunione sulle frontiere intelligenti, tenutasi nel febbraio 2015.

³³ A tal fine sarà necessario l'accordo dei colegislatori sui fascicoli legislativi correlati attualmente in discussione — cfr. sezione II.2.

impatto, anche in materia di diritti fondamentali, in particolare il diritto alla protezione dei dati personali. Insieme alla proposta legislativa sull'interoperabilità, la Commissione presenterà una proposta legislativa per rivedere la base giuridica del Sistema d'informazione visti³⁴ onde dare seguito alla relazione di valutazione presentata nell'ottobre 2016³⁵. Il sistema d'informazione visti è uno dei sistemi d'informazione centralizzati che dovrebbero fare parte del nuovo approccio alla gestione dei dati per le frontiere e la sicurezza.

La discussione comune delle tre istituzioni sulle prospettive future per garantire l'interoperabilità dei sistemi d'informazione entro il 2020 non dovrebbe ritardare i lavori sulle proposte legislative concernenti i sistemi d'informazione attualmente in discussione da parte dei colegislatori. La dichiarazione comune ha già dichiarato urgenti e prioritarie la maggior parte di queste proposte, che affrontano importanti lacune informative che richiedono un'azione urgente, anche in linea con le raccomandazioni del gruppo di esperti. Anche la proposta legislativa supplementare relativa a un sistema europeo di informazione sui casellari giudiziari (ECRIS) per i cittadini di paesi terzi, che la Commissione presenterà nel giugno 2017, sarà pienamente compatibile con le raccomandazioni del gruppo di esperti in materia di interoperabilità e con l'approccio delineato nella presente comunicazione. Al fine di attuare questo nuovo approccio in modo gestibile, è essenziale che le basi giuridiche di tutti i sistemi d'informazione interessati siano stabili. Per questo motivo deve essere data priorità al raggiungimento di un accordo sulle proposte legislative attualmente in discussione.

IV. ATTUAZIONE DI ALTRI FASCICOLI PRIORITARI IN MATERIA DI SICUREZZA

1. Iniziative legislative

Il 1° maggio 2017 è entrato in applicazione il nuovo **regolamento Europol**³⁶, che costituisce un punto di svolta per Europol e introduce una serie di elementi nuovi che consentiranno all'agenzia di contrasto dell'UE di diventare un autentico centro nevralgico dell'UE per lo scambio di informazioni sulle forme gravi di criminalità transfrontaliera e il terrorismo. Europol disporrà degli strumenti necessari per diventare più efficace, efficiente e responsabile. In particolare, un quadro modificato per il trattamento dei dati migliorerà la capacità dell'agenzia di sviluppare analisi criminali al servizio degli Stati membri e un regime per la protezione dei dati più solido garantirà un controllo indipendente ed efficace della protezione dei dati.

Come richiesto dal trattato, le attività di Europol saranno oggetto di un ulteriore controllo del Parlamento europeo, in associazione con i parlamenti nazionali, il che rafforzerà ulteriormente la trasparenza e la legittimità dell'agenzia agli occhi dei cittadini.

Per ridurre al minimo gli effetti negativi della partenza danese da Europol a seguito dei risultati del referendum svoltosi in Danimarca il 3 dicembre 2016, il 30 aprile 2017 è stato firmato un **accordo di cooperazione operativa tra Europol e la Danimarca**. Come concordato nella dichiarazione congiunta del 15 dicembre 2016 del presidente Juncker, del presidente del Consiglio Tusk e del primo ministro danese Rasmussen³⁷, l'accordo stabilisce

³⁴ Regolamento (CE) n. 767/2008 del 9.7.2008.

³⁵ COM(2016) 655 final del 14.10.2016.

³⁶ Regolamento (UE) 2016/794 dell'11.5.2016.

³⁷ Dichiarazione del presidente della Commissione europea, Jean-Claude Juncker, del presidente del Consiglio europeo, Donald Tusk, e del primo ministro della Danimarca, Lars Løkke Rasmussen del 15.12.2016, http://europa.eu/rapid/press-release_IP-16-4398_en.htm.

disposizioni operative speciali che permettono un livello sufficiente di cooperazione operativa tra la Danimarca e Europol, compreso lo scambio di dati operativi e lo scambio di ufficiali di collegamento, fatte salve adeguate garanzie. Sebbene questo accordo non sostituisca la piena adesione della Danimarca a Europol, ossia l'accesso agli archivi di dati di Europol o la partecipazione a pieno titolo ai forum sulla governance di Europol, la Danimarca ha accettato la competenza giurisdizionale della Corte di giustizia dell'Unione europea e le competenze del garante europeo della protezione dei dati, e ha attuato nel diritto danese le norme pertinenti sulla protezione dei dati³⁸. Come indicato nella dichiarazione comune, tali disposizioni sono subordinate al mantenimento dell'adesione della Danimarca all'UE e allo spazio Schengen.

Il 28 aprile 2017 la Commissione ha adottato una decisione di esecuzione sui protocolli comuni e i formati dei dati che i vettori aerei devono utilizzare per trasferire i **dati PNR** alle Unità di informazione sui passeggeri (UIP) a norma della direttiva sul codice di prenotazione (PNR) dell'UE³⁹. La decisione di esecuzione armonizza gli aspetti tecnici della trasmissione dei dati del codice di prenotazione da parte dei vettori aerei. A partire dal 28 aprile 2018 i formati dei dati e i protocolli di trasmissione saranno obbligatori per tutti i trasferimenti di dati PNR da parte dei vettori aerei alle Unità d'informazione sui passeggeri.

Il 25 aprile 2017 il Consiglio ha formalmente adottato la nuova **direttiva sulle armi da fuoco**⁴⁰. Gli Stati membri hanno ora 15 mesi di tempo per mettere in atto i necessari controlli riguardo all'acquisizione e alla detenzione di armi da fuoco al fine di garantire che i gruppi criminali o i terroristi non approfittino della frammentazione delle norme all'interno dell'Unione. Il 28 aprile 2017 il gruppo di esperti sulle norme di disattivazione ha raggiunto un accordo sulle nuove norme di disattivazione in vista dell'adozione di una revisione del regolamento (UE) 2015/2403 della Commissione prima del luglio 2017. L'attuale versione riveduta mira a chiarire alcune norme tecniche per assicurare l'applicazione corretta di tutte le procedure tecniche per la disattivazione di un'arma.

2. *Attuazione di misure non legislative*

L'attacco informatico ransomware globale del 12 maggio 2017 ha sottolineato l'urgente necessità per l'Unione europea, le sue agenzie e gli Stati membri di intensificare le azioni per combattere la crescente minaccia della **criminalità informatica**, concentrandosi anche sull'individuazione e sulla deterrenza. Il Centro europeo per la lotta alla criminalità informatica di Europol (EC3) ha svolto un ruolo di primo piano nella risposta dei servizi di contrasto all'ultimo attacco, basandosi sui lavori svolti in precedenza in questo settore, in particolare nel quadro della campagna "no more ransom". La squadra di pronto intervento informatico delle istituzioni e agenzie dell'UE ha inoltre stabilito uno stretto contatto con il Centro europeo per la lotta alla criminalità informatica, i gruppi di intervento per la sicurezza informatica in caso di incidente dei paesi colpiti, le unità specializzate nella lotta alla criminalità informatica e i principali partner del settore per attenuare la minaccia e assistere le vittime. Nella revisione intermedia della strategia per il mercato unico digitale del 10 maggio 2017 la Commissione ha annunciato la sua intenzione di rivedere la strategia dell'UE per la cibersicurezza del 2013 entro settembre 2017. Questi lavori sono in fase di accelerazione onde estendere la portata delle misure attuali, concentrate sulla prevenzione, all'individuazione e alla deterrenza. L'obiettivo dovrebbe essere ridurre tanto il rischio di

³⁸ Direttiva (UE) 2016/680 del 27.4.2016.

³⁹ Direttiva (UE) 2016/681 del 27.4.2016.

⁴⁰ <http://www.consilium.europa.eu/it/press/press-releases/2017/04/25-control-acquisition-possession-weapons/>

attacchi informatici quanto il loro impatto, rafforzando la resilienza e sviluppando ulteriormente i lavori degli Stati membri per rafforzare le loro capacità nazionali e attuare integralmente la direttiva sulla sicurezza delle reti e dell'informazione⁴¹. La criminalità informatica (e i reati favoriti dall'uso del cibernazio) trae il suo potenziale non solo dalle carenze dei sistemi e dei software, ma anche dai comportamenti che portano a una cattiva igiene informatica. La Commissione non solo rafforzerà il mandato dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), ma presenterà anche proposte per l'elaborazione di norme di sicurezza, certificazioni ed etichettature, per rafforzare la sicurezza informatica dei sistemi e dei dispositivi. Si concentrerà inoltre sulla creazione di competenze informatiche e di capacità tecnica all'interno dell'Unione.

Nelle circostanze attuali caratterizzate dalle minacce all'ordine pubblico o alla sicurezza interna, l'**intensificazione dei controlli di polizia** sull'intero territorio degli Stati membri, comprese le zone di frontiera, possono essere considerati necessari e giustificati al fine di rafforzare la sicurezza all'interno dello spazio Schengen. Per questo motivo, il 2 maggio 2017 la Commissione ha presentato una raccomandazione relativa a controlli di polizia proporzionati e alla cooperazione di polizia nello spazio Schengen⁴², che stabilisce le misure che gli Stati Schengen dovrebbero adottare per garantire un uso più efficace delle attuali competenze di polizia per far fronte alle minacce per l'ordine pubblico o la sicurezza interna. Se necessario e giustificato, gli Stati membri dovrebbero intensificare i controlli di polizia nelle zone di frontiera e lungo le principali vie di trasporto. La decisione relativa a tali controlli e alla loro ubicazione e intensità continua a spettare unicamente agli Stati membri e dovrebbe sempre essere proporzionata alle minacce individuate. Inoltre, la Commissione invita tutti gli Stati membri a rafforzare la cooperazione transfrontaliera di polizia per contrastare le minacce all'ordine pubblico o alla sicurezza interna.

Nel settore della **sicurezza aerea** nelle ultime settimane si sono registrati sviluppi, con l'imposizione, da parte degli Stati Uniti e del Regno Unito, di nuove misure di sicurezza per i voli in provenienza da un certo numero di paesi del Medio Oriente e dell'Africa settentrionale e dalla Turchia, che richiedono che i dispositivi elettronici di grandi dimensioni siano riposti nel bagaglio registrato. Per quanto riguarda l'UE, i lavori sono progrediti in materia di valutazione dei rischi relativi alle minacce e alle vulnerabilità connesse ai voli provenienti da paesi terzi. A seguito di informazioni secondo cui gli Stati Uniti potrebbero introdurre misure analoghe per i voli in provenienza dagli aeroporti dell'UE, la Commissione ha agevolato i contatti a livello politico per garantire azioni coordinate tra gli Stati Uniti e l'UE. Il 17 maggio 2017 si terrà a Bruxelles una riunione tra gli Stati Uniti e l'UE per valutare congiuntamente i potenziali rischi e definire un approccio comune per affrontare le minacce emergenti.

Sono in corso lavori nell'ambito del comitato permanente per la cooperazione operativa in materia di sicurezza interna (COSI) sul prossimo **ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità** nel periodo 2018-2021, che tengono conto delle otto minacce criminali prioritarie individuate dalla

⁴¹ Direttiva (UE) 2016/1148 del 6.7.2016.

⁴² Il 2 maggio 2017 la Commissione ha approvato in linea di principio raccomandazione relativa a controlli di polizia proporzionati e alla cooperazione di polizia nello spazio Schengen (C(2017) 2923). L'adozione formale è avvenuta il 12 maggio 2017.

Commissione nell'ultima relazione sui progressi dell'Unione della sicurezza⁴³. Il Consiglio dovrebbe adottare le conclusioni sul nuovo ciclo programmatico dell'UE il 18 maggio 2017.

A seguito della sua relazione al Consiglio Giustizia e affari interni del dicembre 2016 sui lavori in corso per migliorare l'accesso transfrontaliero degli investigatori alle **prove elettroniche**⁴⁴, la Commissione sta ultimando la sua valutazione e proporrà le prospettive future da discutere in seno al Consiglio Giustizia e affari interni dell'8 giugno 2017.

La Commissione ha sostenuto i lavori intrapresi finora da un gruppo di Stati membri per assicurare il mantenimento di e-CODEX, un sistema di cooperazione giudiziaria transfrontaliera e di accesso digitale alle procedure giudiziarie. La Commissione ha preso atto della posizione di questi Stati membri, secondo cui questa soluzione non è sostenibile. In sede di gruppo di lavoro del Consiglio, gli Stati membri hanno esaminato varie opzioni e hanno concluso che l'agenzia eu-LISA sarebbe la più indicata per assicurare il mantenimento e l'operabilità del sistema e-CODEX. Al fine di trovare la soluzione migliore la Commissione sta valutando l'impatto di varie opzioni per il mantenimento di e-CODEX. I risultati della valutazione saranno disponibili entro autunno 2017.

La richiamata adozione della direttiva sulle armi da fuoco è un importante passo avanti per far rispettare le norme sull'acquisizione e sulla detenzione legali di armi da fuoco. La Commissione sta inoltre trattando il problema del **traffico illecito di armi da fuoco** all'interno e al di fuori dell'UE. Il 16 marzo 2017 si è tenuta a Kiev una tavola rotonda tecnica UE-Ucraina sul traffico illecito di armi da fuoco. Questa riunione è stata la prima di questo tipo tra l'UE e l'Ucraina per migliorare lo scambio di informazioni relative al traffico illecito di armi da fuoco. Il 28 marzo 2017 si è svolta a Tunisi la seconda tavola rotonda tecnica UE-Tunisia sul traffico illecito di armi da fuoco. Sia per l'Ucraina che per la Tunisia è stato concordato un piano d'azione che prevede missioni di esperti dell'UE per valutare il quadro amministrativo dei due paesi, organizzare una conferenza di alto livello sulla legislazione pertinente e proporre attività di formazione, visite di studio e seminari sulla gestione pratica dei dati, e una cooperazione operativa.

Il 12 maggio 2017 la Commissione e il Servizio europeo per l'azione esterna hanno presentato al Consiglio un **documento informale comune sull'azione esterna dell'UE relativa alla lotta al terrorismo** che indica i paesi, settori e strumenti prioritari per l'azione dell'UE in questo settore. Questo documento comune costituisce un contributo alla discussione sulla revisione delle conclusioni del Consiglio del febbraio 2015 sull'azione esterna dell'UE relativa alla lotta al terrorismo⁴⁵, in vista delle nuove conclusioni del Consiglio Affari esteri del giugno 2017.

⁴³ COM(2017) 213 final del 12.4.2017. Le otto minacce criminali prioritarie individuate dalla Commissione sono la criminalità informatica, la criminalità connessa alla droga, il traffico di migranti, i reati organizzati contro il patrimonio, la tratta di esseri umani, il traffico di armi da fuoco, la frode sull'IVA e la criminalità ambientale.

⁴⁴ Cfr. il documento informale dei servizi della Commissione "Progress report following the Conclusions of the Council of the European Union on improving criminal justice in cyberspace" del 2.12.2016: <http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf>. Nelle sue conclusioni sul miglioramento della giustizia penale nel ciberspazio del 9 giugno 2016, il Consiglio ha invitato la Commissione ad adottare azioni concrete, sviluppare un approccio comune dell'UE e presentare risultati entro giugno 2017.

⁴⁵ Conclusioni del Consiglio sulla lotta al terrorismo del 9.2.2015: <http://www.consilium.europa.eu/en/press/press-releases/2015/02/150209-council-conclusions-counter-terrorism/>.

Il 16 e 17 marzo 2017 si è tenuto a Bucarest un primo seminario con paesi vicini dell'UE in materia di **protezione delle infrastrutture critiche** (PIC), nel quadro di un ampliamento della dimensione esterna del programma europeo per la protezione delle infrastrutture critiche. Oltre agli Stati membri, hanno partecipato rappresentanti di otto paesi dell'Europa orientale e dei Balcani occidentali. L'obiettivo di questo primo seminario è stato quello di stabilire contatti e scambiare informazioni sulle misure e sugli strumenti per la protezione delle infrastrutture critiche. Sono state individuate possibili aree di ulteriore cooperazione, tra cui attività di formazione o esercitazioni congiunte incentrate su aspetti pratici (operativi), studi sulle interdipendenze regionali e valutazioni inter pares delle strategie nazionali di protezione delle infrastrutture critiche.

V. CONCLUSIONI

La Commissione invita il Parlamento europeo e il Consiglio a far progredire i fascicoli legislativi prioritari riguardanti i sistemi d'informazione per la gestione della sicurezza, delle frontiere e della migrazione. L'adozione di tali atti legislativi rafforzerà i sistemi esistenti e colmerà le lacune informative già individuate, rispondendo ai bisogni delle guardie di frontiera, dei funzionari delle autorità di contrasto, compresi quelli delle amministrazioni doganali, dei funzionari dei servizi per l'immigrazione e delle autorità giudiziarie, e creando la base per rendere tali sistemi più interoperabili.

Come seguito alla comunicazione dell'aprile 2016 sui sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza, e alla luce delle raccomandazioni del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità, la Commissione ha delineato un nuovo approccio alla gestione dei dati per le frontiere e la sicurezza, in base al quale tutti i sistemi d'informazione centralizzati dell'UE per la gestione della sicurezza, delle frontiere e della migrazione sono interoperabili, nel pieno rispetto dei diritti fondamentali. A tal fine, basandosi sui lavori tecnici e legislativi in corso in materia di sistemi d'informazione, nel giugno 2017 la Commissione presenterà una proposta legislativa che rafforza il mandato di eu-LISA per consentire all'agenzia di garantire l'attuazione di questo nuovo approccio; farà poi seguito, non appena possibile, una proposta legislativa sull'interoperabilità. La Commissione invita il Parlamento europeo e il Consiglio a tenere una discussione comune sulle prospettive future. In tal modo le tre istituzioni potranno raggiungere un'intesa comune sulle prospettive future in materia di interoperabilità e sulle misure necessarie per il conseguimento dell'interoperabilità entro il 2020, nel pieno rispetto dei diritti fondamentali. L'attuazione del proposto approccio all'interoperabilità aumenterebbe l'efficacia e l'efficienza della gestione dei dati nell'UE, per una migliore protezione delle frontiere esterne e un rafforzamento della sicurezza interna, a beneficio di tutti i cittadini.