COMMISSIONE
EUROPEA

Bruxelles, 18.10.2017
COM(2017) 608 final

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

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

I. INTRODUZIONE

Il presente documento è l'undicesima relazione mensile sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza e verte sugli sviluppi attinenti a due ambiti 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.

Nel discorso sullo Stato dell'Unione[1], il Presidente Juncker ha sottolineato che l'Unione europea deve essere più forte nella lotta contro il terrorismo, basandosi sui veri progressi compiuti negli ultimi tre anni. Come annunciato nella lettera di intenti[2] al Parlamento europeo e alla Presidenza del Consiglio e nella tabella di marcia per un'Unione più unita, più forte e più democratica ad essa allegata, nella presente relazione la Commissione presenta un **pacchetto di misure antiterrorismo** da adottare nel corso dei prossimi sedici mesi. Queste misure operative aiuteranno gli Stati membri ad affrontare i punti deboli significativi messi in evidenza dai recenti attentati terroristici, e segneranno una vera e propria differenza nel rafforzamento della sicurezza. Ciò contribuirà a creare un'Unione della sicurezza in cui i terroristi non potranno più sfruttare eventuali lacune per commettere le loro atrocità. Oltre a queste misure pratiche a breve termine, la Commissione sta lavorando a una futura Unità di intelligence europea, come annunciato dal Presidente Juncker quale parte della sua visione dell'Unione europea da qui al 2025.

Il pacchetto antiterrorismo include:

- misure per aiutare gli Stati membri a **proteggere gli spazi pubblici** (sezione II), che comprendono un piano d'azione per sostenere la protezione degli spazi pubblici e un piano d'azione per rafforzare la preparazione contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare;
- misure per impedire l'accesso ai mezzi usati dai terroristi per preparare e perpetrare attentati, come **sostanze pericolose** o **finanziamenti** (sezione III), che includono una raccomandazione relativa a misure immediate volte a prevenire l'uso improprio dei precursori di esplosivi, così come misure per aiutare le autorità giudiziarie e di contrasto nelle indagini penali in cui si riscontra **l'uso di informazioni criptate**;
- le prossime misure per **contrastare la radicalizzazione** (sezione IV);
- le prossime misure per rafforzare la **dimensione esterna** della lotta contro il terrorismo (sezione V), che includono le proposte di decisioni del Consiglio relative alla conclusione, a nome dell'UE, della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e del Protocollo addizionale di tale Convenzione, così come una raccomandazione al Consiglio per autorizzare l'avvio di negoziati col Canada per la revisione dell'accordo sui dati del codice di prenotazione.

II. MISURE PER MIGLIORARE LA PROTEZIONE E LA RESILIENZA CONTRO IL TERRORISMO

1. Rafforzata protezione degli spazi pubblici

[1] http://europa.eu/rapid/press-release_SPEECH-17-3165_it.htm.
[2] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_en.pdf.

Nella propaganda e nella scelta dei bersagli, l'attenzione dei terroristi si sposta sempre più spesso verso gli spazi pubblici come le zone pedonali, i siti turistici, i centri commeciali, le sale da concerto e le piazze cittadine, come dimostrato dagli attentati commessi ad esempio a Barcellona, Berlino, Bruxelles, Londra, Manchester, Nizza, Parigi e Stoccolma. Ciò che tutti i questi obiettivi (i cosiddetti "soft target") hanno in comune è il fatto di essere aperti, pubblici e caratterizzati da un'alta concentrazione di persone, cosa che li rende intrinsecamente vulnerabili.

Si può intervenire maggiormente per ridurre le vulnerabilità di questi luoghi, individuare le minacce più precocemente e aumentare la resilienza. Per questo motivo la Commissione, in un **piano d'azione per sostenere la protezione degli spazi pubblici**[3] presentato insieme alla presente relazione, definisce misure per sostenere gli Stati membri a livello nazionale, regionale e locale nei loro sforzi di rafforzamento della protezione fisica contro le minacce terroristiche. Anche se non ci potrà mai essere "rischio zero", il piano d'azione mira ad aiutare gli Stati membri ad individuare le minacce, ridurre la vulnerabilità degli spazi pubblici, attenuare le conseguenze di un attentato terroristico e migliorare la cooperazione.

Il sostegno che l'UE può fornire per la protezione degli spazi pubblici è duplice. In primo luogo, essa può promuovere lo **scambio transfrontaliero di migliori pratiche, anche mediante finanziamenti**. Questo include, ad esempio, misure per promuovere e sostenere lo sviluppo di barriere innovative e discrete per garantire la sicurezza delle città senza compromettere la loro apertura ("proteggere fin dalla progettazione"). Sostenendo finanziariamente le misure del piano d'azione, la Commissione ha pubblicato oggi un invito a presentare proposte attraverso il Fondo Sicurezza interna - Polizia per un importo totale di 18,5 milioni di euro. A tale dotazione andranno ad aggiungersi nel 2018 finanziamenti a breve termine nel quadro delle **azioni innovative urbane** del Fondo europeo di sviluppo regionale, dove la sicurezza sarà un tema fondamentale, e per le quali il finanziamento totale arriverà fino ai 100 milioni di euro. Il 15 settembre 2017 è stata avviata una consultazione pubblica per raccogliere idee dalle città sulle soluzioni innovative per la sicurezza. Questo aiuterà la Commissione a delineare i futuri inviti a presentare proposte in questo settore.

In secondo luogo, l'UE può promuovere la **cooperazione con un'ampia gamma di portatori d'interessi**, condizione che si ritiene indispensabile per migliorare la protezione degli spazi pubblici. La condivisione delle esperienze e la messa in comune delle risorse dovrebbero essere strutturate meglio. La Commissione creerà un forum per avviare un dialogo con operatori privati come centri commerciali, organizzatori di concerti, palazzetti dello sport, alberghi e società di autonoleggio. Ciò faciliterà una presa di coscienza comune delle sfide attuali in materia di sicurezza e promuoverà i partenariati pubblico-privato per migliorare la protezione. Le autorità locali e regionali hanno a loro volta un ruolo fondamentale da svolgere nella protezione degli spazi pubblici, e devono partecipare alle relative attività a livello UE. La Commissione rafforzerà il coinvolgimento dei portatori d'interessi e l'avvio di un dialogo con le autorità locali e regionali, come i sindaci di grandi città, per scambiare informazioni e migliori pratiche in materia di protezione degli spazi pubblici. Come follow up della dichiarazione di Nizza[4] del 29 settembre 2017, all'inizio dell'anno prossimo la Commissione

[3] COM(2017) 612 final del 18.10.2017.

[4] La dichiarazione di Nizza è stata adottata nel corso di una conferenza dei sindaci della regione euromediterranea a Nizza il 29 settembre 2017, organizzata su iniziativa del sindaco di Nizza, e con la partecipazione della Commissione, per scambiare tra le città e i livelli locali e regionali le migliori pratiche

organizzerà, in collaborazione con il Comitato delle regioni, una riunione ad alto livello con i sindaci che hanno sottoscritto la dichiarazione di Nizza e altri rappresentanti di enti locali e regionali per continuare lo scambio di buone pratiche sulla protezione degli spazi pubblici.

La Commissione continuerà inoltre a lavorare alla protezione e resilienza delle **infrastrutture critiche**. La valutazione complessiva della politica di sicurezza dell'UE[5] ha anche sottolineato la necessità di adattare il programma europeo per la protezione delle infrastrutture critiche (EPCIP)[6] alle minacce emergenti. La Commissione ha cominciato una valutazione della direttiva[7] relativa all'individuazione e alla designazione delle infrastrutture critiche europee, che terrà conto delle esperienze acquisite e degli sviluppi intervenuti negli ultimi anni, come l'adozione della direttiva sulla sicurezza delle reti e dell'informazione[8]. Nel frattempo, il programma europeo per la protezione delle infrastrutture critiche è stato rafforzato in modo da poter affrontare le sfide emergenti quali le minacce interne e le minacce ibride, ampliando inoltre la dimensione esterna del programma grazie a una cooperazione con i paesi del vicinato orientale e dei Balcani occidentali.

Il settore dei trasporti è stato per molti anni sia un bersaglio di attentati terroristici che un mezzo per perpetrarli (ad es. dirottamenti di aerei o camion-ariete). In risposta, è necessario valutare in quale misura le norme relative alla **sicurezza dei trasporti** garantiscano tale protezione assicurando al tempo stesso la fluidità delle reti di trasporto. Se il settore dell'aviazione è decisamente protetto meglio, i terroristi sfruttano ora maggiormente le opportunità disponibili per compiere gli attentati concentrandosi più spesso sugli spazi pubblici. A tale riguardo, il **trasporto ferroviario** è un bersaglio ad alto rischio poiché la sua infrastruttura è, per sua natura, aperta. Non esiste attualmente alcun quadro legislativo dell'UE per proteggere il trasporto ferroviario di passeggeri contro il terrorismo e le forme gravi di criminalità. Il 15 giugno 2017 la Commissione ha varato, insieme agli Stati membri, una valutazione congiunta dei rischi nel settore ferroviario e sta lavorando a nuove misure per migliorare la sicurezza del trasporto ferroviario di passeggeri. La Commissione sta inoltre lavorando a uno strumentario orientativo di migliori pratiche relative alla sicurezza per il settore del **trasporto stradale** commerciale, incentrato sul miglioramento della sicurezza dei camion per attenuare il rischio di intrusione non autorizzata, dirottamento o furto del veicolo per uso come ariete in un attentato terroristico. Lo strumentario sarà disponibile entro la fine del 2017 e fornirà orientamenti per i settori dei trasporti stradali nazionali. La Commissione continuerà anche a lavorare al miglioramento della **sicurezza dei trasporti marittimi**, in particolare per rafforzare la protezione delle infrastrutture di trasporto marittimo, inclusi porti e impianti portuali, navi container e navi passeggeri come le navi da crociera e i traghetti.

---

in materia di prevenzione della radicalizzazione e protezione degli spazi pubblici: http://www.nice.fr/uploads/media/default/0001/15/TERRORISME%20EUROPE%20Déclaration%20-%20der%20version.pdf.

5 Si veda la Nona relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2017) 407 final del 26.7.2017) e l'allegato documento di lavoro dei servizi della Commissione. (SWD(2017) 278 final).

6 Tale programma definisce il quadro delle azioni dell'UE volte a migliorare la protezione delle infrastrutture critiche in Europa –in tutti gli Stati membri e in tutti i settori di attività economica pertinenti. Un elemento fondamentale di tale lavoro è la direttiva del 2008 sulle infrastrutture critiche europee (direttiva 2008/114/CE dell'8.12.2008).

7 Direttiva 2008/114/CE dell'8.12.2008.

8 Direttiva 2016/1148 del 6.7.2016.

2. *Preparazione rafforzata contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare*

Benché nell'Unione europea la probabilità di attentati perpetrati con sostanze chimiche, biologiche, radiologiche e nucleari (CBRN) resti bassa, la minaccia CBRN è, in generale, in evoluzione. Vi sono elementi che indicano che singoli criminali o gruppi terroristici potrebbero avere intenzione di procurarsi materiali CBRN e potrebbero disporre delle conoscenze e delle capacità per usarli a fini terroristici. Il potenziale degli attacchi CBRN è messo in evidenza nella propaganda terroristica. La valutazione complessiva della politica di sicurezza dell'UE[9] ha inoltre indicato la necessità di rafforzare la preparazione contro queste minacce.

Per essere più preparati a far fronte alle minacce CBRN nei prossini anni, la Commissione presenta, contenstualmente alla presente relazione, un **piano d'azione per rafforzare la preparazione contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare[10].** Esso include un'ampia gamma di misure per migliorare la preparazione, la resilienza e il coordinamento a livello dell'UE, ad esempio la creazione di una rete dell'UE per la sicurezza CBRN intesa a riunire tutti gli operatori CBRN, che sarà sostenuta, fra l'altro, da un polo di conoscenze in materia di CBRN istituito presso il Centro europeo antiterrorismo (ECTC) di Europol. Poiché è inoltre importante usare meglio le risorse esistenti, il piano d'azione propone di rafforzare la preparazione e la risposta dell'UE nel settore CBRN attraverso la formazione e le esercitazioni di tutti i vari operatori che intervengono per primi (autorità di contrasto, protezione civile, sanità) e, se del caso, dei partner militari e privati. Saranno di supporto anche strumenti esistenti a livello dell'UE, in particolare il meccanismo unionale di protezione civile (UCPM)[11] e l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). Per fornire un maggiore aiuto in caso di grave incidente CBRN, gli Stati membri dovrebbero continuare a rafforzare l'esistente capacità europea di reazione alle emergenze (EERC) dell'UCPM. In questo contesto, gli Stati membri sono incoraggiati a continuare a mettere a disposizione dell'EERC nuove capacità.

La legislazione dell'UE relativa alle **gravi minacce per la salute a carattere transfrontaliero**[12] verte sulla preparazione, la sorveglianza e il coordinamento delle risposte a emergenze sanitarie nell'insieme dell'UE. In tale contesto, il sistema di allarme rapido e di reazione dell'UE sarà collegato meglio agli altri sistemi di allarme dell'UE riguardanti le minacce biologiche, chimiche, ambientali e sconosciute. Il programma Salute sta inoltre finanziando esercitazioni a livello dell'UE in materia di preparazione alle emergenze e di intervento in caso di emergenza, e azioni congiunte per aiutare gli Stati membri a rinforzare laboratori, programmi di vaccinazione e capacità fondamentali in applicazione del regolamento sanitario internazionale.

Tutte le iniziative saranno sostenute da apposite attività di ricerca, da finanziamenti e dalla cooperazione con i partner internazionali rilevanti.

---

9 Si veda la Nona relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2017) 407 final del 26.7.2017) e l'allegato documento di lavoro dei servizi della Commissione. (SWD(2017) 278 final).

10 COM(2017 610 final del 18.10.2017.

11 Decisione n. 1313/2013/UE del 17.12.2013.

12 Decisione n. 1082/2013/UE del 22.10.2013.

III. AFFRONTARE I MEZZI DI SOSTEGNO DEL TERRORISMO

1. Finanziamento del terrorismo: accesso transfrontaliero alle informazioni finanziarie

Le informazioni sulle attività finanziarie di sospetti terroristi possono fornire piste fondamentali nelle indagini antiterrorismo. Per la loro affidabilità e la loro precisione, i dati finanziari (inclusi quelli relativi alle operazioni finanziarie) possono aiutare a identificare terroristi, a fare emergere legami con i complici, a stabilire le attività, la logistica e gli spostamenti di persone sospette, e a tracciare i contorni delle reti terroristiche. Una rapida panoramica delle attività finanziarie dei terroristi e dei loro complici può fornire alle autorità di contrasto informazioni fondamentali per impedire attentati o per reagire se vengono compiuti. Il crescente fenomeno di attentati artigianali e su piccola scala pone nuove sfide; i segnali che indicano progetti di attentati possono essere meno evidenti quando questi sono pianificati a breve termine. Le operazioni finanziarie collegate a piani su piccola scala possono non risultare sospette, col risultato che l'informazione è portata all'attenzione delle autorità competenti solo dopo un attentato.

Come annunciato nel piano d'azione del 2016 sulla lotta contro il finanziamento del terrorismo[13], la **Commissione sta valutando la necessità di misure supplementari** per facilitare l'accesso alle informazioni finanziarie detenute in altre giurisdizioni dell'UE ai fini di indagini antiterrorismo. Nella Terza relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza del dicembre 2016[14], la Commissione ha presentato la sua prima analisi e ha dichiarato che avrebbe continuato la sua valutazione, prendendo in particolare considerazione le eventuali ripercussioni sui diritti fondamentali e soprattutto sul diritto alla protezione dei dati personali. Da allora la Commissione sta consultando i portatori d'interessi e ha analizzato i meccanismi attraverso i quali le autorità competenti possono attualmente accedere alle informazioni rilevanti, in particolare ai dati finanziari conservati in altri Stati membri, gli ostacoli che impediscono loro di farlo rapidamente ed efficacemente, e le possibili misure per affrontare questi ostacoli.

Oltre alla valutazione in corso, la Commissione continua a promuovere lo **scambio di migliori prassi** relative alle tecniche di indagine e all'analisi dei metodi usati dai terroristi per raccogliere e movimentare fondi, apportando fra l'altro il suo sostegno finanziario sulla base di un invito a presentare proposte, lanciato oggi, per un importo di 2,5 milioni di euro.

In questo contesto la Commissione sta anche esaminando come **migliorare la cooperazione fra le unità di informazione finanziaria**[15]**,** istituite per prevenire, individuare e combattere efficacemente il riciclaggio e il finanziamento del terrorismo. Una relazione sinottica del dicembre 2016 svolta dalle unità di informazione finanziaria, e il collegato documento di lavoro dei servizi della Commissione sul miglioramento della collaborazione tra le unità di

---

13 COM(2016) 50 final del 2.2.2016.

14 COM(2016) 831 final del 21.12.2016.

15 Le unità di informazione finanziaria sono state istituite con la decisione 2000/642/GAI del Consiglio del 17.10.2000, e sono disciplinate dalla direttiva (UE) 2015/849 (20.5.2015) relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Sono unità indipendenti e autonome a livello operativo, con la responsabilità di ricevere e di analizzare le segnalazioni, provenienti da entità rilevanti, di operazioni sospette ed altre informazioni che riguardano attività di riciclaggio, reati presupposto associati o attività di finanziamento del terrorismo, e di comunicare alle autorità competenti i risultati delle loro analisi e qualsiasi altra informazione pertinente.

informazione finanziaria[16], evidenziano una serie di limiti nelle competenze nazionali di tali unità e definiscono una via da seguire per risolvere tali questioni attraverso: i) l'attuazione della 4ª direttiva antiriciclaggio[17] e delle sue modifiche[18], attualmente in corso di negoziazione; ii) altre iniziative svolte dalla piattaforma delle unità di informazione finanziaria dell'UE per rafforzare la cooperazione operativa, soprattutto attraverso orientamenti, lavori di standardizzazione e soluzioni di impresa da attuare nel quadro di FIU.Net, e iii) misure regolamentari per affrontare le altre questioni derivanti dal diverso status e dalle competenze divergenti delle unità di informazione finanziaria, in particolare per facilitare il coordinamento e lo scambio di informazioni sia all'interno di tali unità che fra esse e le autorità di contrasto.

Sono inoltre in corso lavori per facilitare l'**accesso ai dati finanziari all'interno di uno Stato membro**. Le proposte modifiche alla **4ª direttiva antiriciclaggio**[19], attualmente in corso di negoziazione con i colegislatori, porterebbero alla crezione di registri centrali dei conti bancari o a sistemi di reperimento dei dati in tutti gli Stati membri, accessibili alle unità di informazione finanziaria e alle altre autorità competenti responsabili della lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. Questi registri, una volta istituiti in tutti gli Stati membri, faciliteranno l'individuazione dei dati relativi ai conti bancari. In base a ciò, la Commissione sta preparando un'iniziativa per **ampliare l'accesso delle autorità di contrasto a tali registri centrali dei conti bancari**[20], che consentirebbe a tali autorità di individuare più rapidamente l'esistenza di un conto.

Durante le consultazioni con i portatori d'interessi è stata anche sollevata la questione degli **ostacoli all'ottenimento dei dati relativi alle operazioni finanziarie detenuti da altri Stati membri**. Se necessario, le informazioni sui conti bancari possono essere scambiate fra gli Stati membri attraverso canali di cooperazione di polizia entro le otto ore[21]. L'accesso ai dati relativi alle operazioni finanziarie detenuti da altri Stati membri può inoltre essere facilitato attraverso le unità di informazione finanziaria. Qualora tali informazioni debbano essere usate come prova in un procedimento penale, può essere necessario richiederle tramite assistenza giudiziaria. L'ordine europeo di indagine penale[22] offre nuove possibilità di ottenimento dei dati relativi alle operazioni finanziarie, in un modo significativamente più rapido rispetto al canale dell'assistenza giudiziaria. Finora, dopo pochi mesi dalla scadenza del relativo termine, solo 16 Stati membri hanno recepito l'ordine europeo di indagine, e gli altri sono invitati a farlo senza ulteriori ritardi. Infine, le proposte legislative a venire sulle prove elettroniche, previste per l'inizio del 2018, faciliteranno a loro volta l'accesso transfrontaliero a tali dati.

Le consultazioni con i portatori d'interessi hanno anche evidenziato **ostacoli all'individuazione di dati sulle operazioni finanziarie detenuti in altri Stati membri**.

---

16 SWD(2017)275 final del 26.6.2017.
17 Direttiva (UE) 2015/849 del 20.5.2015.
18 COM(2016) 450 final del 5.7.2016.
19 COM(2016) 450 final del 5.7.2016.
20 http://ec.europa.eu/info/law/better-regulation/initiatives/Ares-2017-3971182.
21 La decisione quadro 2006/960/GAI del Consiglio (l'"iniziativa svedese") prevede i seguenti termini entro i quali le autorità incaricate dell'applicazione della legge devono rispondere alle richieste provenienti dall'estero: otto ore se le informazioni o l'intelligence richieste sono conservate in una banca dati alla quale un'autorità incaricata dell'applicazione della legge può accedere direttamente; termini più lunghi se le informazioni o l'intelligence richieste non sono conservate in una banca dati direttamente accessibile.
22 Direttiva 2014/41/UE del 3.4.2014.

Come misura per affrontare questo problema e come parte della sua valutazione in corso, la Commissione analizzerà la necessità, la fattibilità tecnica e la proporzionalità di un lavoro di interconnessione dei registri centralizzati dei conti bancari, tenendo conto di tutti gli strumenti esistenti e previsti per facilitare l'accesso ai dati relativi alle operazioni finanziarie detenuti in altri Stati membri.

A tal fine la Commissione **continuerà le consultazioni con tutte i portatori d'interessi** sulla necessità, la fattibilità tecnica e la proporzionalità di eventuali nuove misure a livello dell'UE per facilitare e accelerare l'accesso transfrontaliero ai dati relativi alle operazioni finanziarie, incluse le procedure per garantire la riservatezza. Sulla base dell'insieme delle valutazioni in corso relative all'uso delle informazioni finanziarie ai fini delle indagini antiterrorismo, la Commissione organizzerà una riunione ad alto livello dei portatori d'interessi nel novembre 2017. I punti centrali di discussione saranno i seguenti:

- i principali ostacoli a un accesso effettivo e tempestivo, ai fini di indagini antiterrorismo, ai dati relativi alle operazioni finanziarie detenuti in altri Stati membri;
- la necessità, la fattibilità tecnica e la proporzionalità di eventuali misure supplementari per facilitare l'accesso transfrontaliero ai dati relativi alle operazioni finanziarie ai fini di indagini antiterrorismo in un modo rapido, efficiente e sicuro.

La Commissione riferirà in merito all'esito delle discussioni.

2. Esplosivi: limitare ulteriormente l'accesso ai precursori di esplosivi

Il **regolamento sui precursori di esplosivi**[23] limita l'accesso dei privati a sette sostanze chimiche (i cosiddetti «precursori di esplosivi soggetti a restrizioni» di cui all'allegato I del regolamento) e il loro utilizzo. Nel febbraio 2017 la Commissione ha adottato una relazione sull'applicazione del regolamento da parte degli Stati membri[24], giungendo alla conclusione che essa abbia contribuito a limitare l'accesso ai precursori di esplosivi pericolosi che possono essere impropriamente utilizzati per fabbricare esplosivi artigianali. Gli Stati membri hanno anche segnalato casi in cui l'applicazione del regolamento ha portato alla rapida individuazione di piani terroristici[25]. Per assicurare che il regolamento sia pienamente applicato, nel maggio e nel settembre 2016 la Commissione ha avviato procedure di infrazione nei confronti di numerosi Stati membri a motivo della trasposizione incompleta del regolamento. Ad ottobre 2017 sono pendenti solo due casi di infrazione, segnatamente nei confronti della Spagna e della Romania.

Nonostante gli sforzi comuni, i recenti attentati e incidenti terroristici indicano che la **minaccia rappresentata dagli ordigni artigianali** in Europa è ancora elevata. Le sostanze in esame continuano ad essere accessibili e ad essere utilizzate nella fabbricazione di esplosivi

[23] Regolamento (UE) n. 98/2013 del 15.1.2013.
[24] COM(2017) 103 final del 28.2.2017.
[25] Il 23 giugno 2017 il ministero belga dell'Interno ha annunciato di aver ricevuto, in un anno, 30 segnalazioni di vendite sospette. Da febbraio a giugno 2017, la Francia ha ricevuto 11 segnalazioni riguardanti, nella maggior parte dei casi, anche il perossido di idrogeno.

artigianali. L'esplosivo utilizzato nella maggior parte degli attentati è il perossido di acetone (TATP), un esplosivo artigianale che sembrerebbe essere la scelta preferita dai terroristi[26].

In considerazione della minaccia rappresentata dai precursori di esplosivi, è necessario adottare misure immediate per garantire che l'attuale regolamento sia attuato da tutti gli Stati membri in modo ottimale. Per questo motivo la Commissione ha pubblicato, unitamente alla presente relazione, una **raccomandazione**[27] che definisce orientamenti sulle misure immediate volte a impedire l'uso improprio di precursori di esplosivi. La Commissione incoraggia gli Stati membri a dare piena attuazione a detta raccomandazione al fine di limitare, per quanto possibile, l'accesso ai precursori di esplosivi e il loro utilizzo da parte di terroristi e di migliorare i controlli sull'utilizzo legittimo e la reazione nei confronti delle transazioni sospette. La Commissione è pronta ad assistere gli Stati membri in tal senso.

Inoltre la Commissione sta accelerando i lavori di **riesame del regolamento sui precursori di esplosivi**, effettuandone un esame cui seguirà una valutazione d'impatto nel corso del primo semestre del 2018. L'esame valuterà la pertinenza, l'efficacia, l'efficienza, la coerenza e il valore aggiunto del regolamento e individuerà i problemi e gli ostacoli che potrebbero richiedere ulteriori interventi. La valutazione d'impatto considererà le varie opzioni strategiche per risolvere i problemi e gli ostacoli individuati.

3. Crittografia: sostenere le autorità di contrasto nell'ambito delle indagini penali

L'utilizzo della crittografia è fondamentale per garantire la sicurezza informatica e la protezione dei dati personali. La legislazione dell'UE ne mette specificamente in evidenza il ruolo quando si tratta di garantire l'adeguata sicurezza del trattamento dei dati personali[28]. Al contempo, nel contesto delle indagini penali, le autorità giudiziarie e di polizia si trovano spesso confrontate alle sfide poste dall'uso della crittografia da parte dei criminali, che pregiudica la loro capacità di ottenere le informazioni necessarie da acquisire come prove nelle indagini penali e di perseguire e condannare gli autori di reati. È presumibile che il ricorso alla crittografia a fini criminosi sarà sempre maggiore nei prossimi anni, e con esso le sue ripercussioni sulle indagini penali.

A seguito di una richiesta del Consiglio «Giustizia e affari interni» nel dicembre 2016, la Commissione ha **esaminato il ruolo della crittografia nelle indagini penali con i pertinenti portatori d'interessi** sotto il profilo tecnico e giuridico. A discuterne sono stati, tra gli altri, esperti di Europol, di Eurojust, della rete giudiziaria europea per la criminalità informatica (EJCN), dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), dell'Agenzia dell'Unione europea per i diritti fondamentali (FRA) e dei servizi di contrasto degli Stati membri, assieme a esponenti dell'industria e delle organizzazioni della società civile. Il Consiglio è stato periodicamente informato dei progressi, a livello di gruppo di lavoro, e un seminario con gli Stati membri ha avuto luogo il 18 settembre 2017. Durante tutto il processo consultivo, si sono tenute diverse tavole rotonde con gli operatori del settore e le organizzazioni della società civile.

---

[26] Relazione sulla situazione e sulle tendenze del terrorismo nell'UE (TE-SAT) 2017: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

[27] C(2017) 6950 final del 18.10.2017.

[28] Articolo 32 del regolamento (UE) 2016/679 del 27.4.2017.

A seguito di tali discussioni con gli Stati membri e i portatori d'interessi e sulla base dei loro contributi, la Commissione conclude che dovrebbero essere attuate le seguenti **misure a sostegno delle autorità di contrasto e delle autorità giudiziarie** quando esse sono confrontate all'utilizzo della crittografia da parte dei criminali nelle indagini penali: a) misure giuridiche atte a facilitare l'accesso ai dati cifrati, e b) misure tecniche volte ad aumentare la capacità di decifrazione. La Commissione continuerà a monitorare gli sviluppi al riguardo.

a) Quadro giuridico per l'accesso transfrontaliero alle prove elettroniche

Le autorità di contrasto si trovano spesso ad affrontare la sfida di accedere agli elementi di prova che si trovano in un altro paese. Gli sviluppi legislativi in corso a livello europeo possono aiutare le autorità di contrasto e giudiziarie ad ottenere l'accesso alle necessarie informazioni, talvolta in forma cifrata, che si trovano in un altro Stato membro. Un quadro giuridico adeguato è necessario per garantire l'efficacia delle indagini e del perseguimento dei reati. A tal fine, la Commissione presenterà, all'inizio del 2018, proposte intese a facilitare **l'accesso transfrontaliero** al materiale probatorio elettronico. Parallelamente, la Commissione sta attuando una serie di misure pratiche[29] volte a migliorare l'accesso transfrontaliero alle prove elettroniche da acquisire ai fini delle indagini penali, compresi i finanziamenti destinati alla formazione sulla collaborazione transfrontaliera, lo sviluppo di una piattaforma elettronica per lo scambio di informazioni all'interno dell'UE e la standardizzazione delle forme di cooperazione giudiziaria usate tra gli Stati Membri.

b) Misure tecniche

In funzione dell'uso che i criminali fanno della crittografia, le autorità di contrasto e giudiziarie possono riuscire a recuperare una parte delle informazioni. Alcuni Stati membri hanno istituito servizi nazionali dotati di esperti per affrontare la problematica della crittografia nel contesto delle indagini penali, ma la maggior parte degli Stati membri non ha accesso al necessario livello di competenze e di risorse tecniche. Ciò compromette gravemente la capacità delle autorità di contrasto e giudiziarie di accedere a informazioni cifrate nelle indagini penali. Per questo motivo la Commissione propone una **serie di misure volte a sostenere le autorità degli Stati membri,** senza vietare, limitare o indebolire la crittografia.

In primo luogo, la Commissione sosterrà **Europol** nel rafforzamento della sua capacità di decifrazione. A tal fine, la Commissione ha proposto, in fase di preparazione del bilancio UE per il 2018, un totale di 86 posti supplementari connessi alla sicurezza da destinare a Europol (19 in più rispetto al bilancio 2017), segnatamente per rafforzare il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol. Sarà esaminato il fabbisogno di risorse supplementari, e nella prossima relazione dell'Unione sulla sicurezza la Commissione riferirà in merito ai fondi messi a disposizione a tal fine. Occorre tenere conto dei futuri sviluppi tecnologici che deriveranno dalle attività di ricerca e sviluppo condotte nel quadro del programma Orizzonte 2020 e di altri programmi finanziati dall'UE. Non saranno prese in esame misure che potrebbero indebolire la crittografia o tali da incidere su un numero elevato o indiscriminato di persone.

[29] Cfr. Quinta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2017) 354 final del 29.6.2017).

In secondo luogo, è necessario istituire una **rete di centri specializzati** per sostenere le autorità di contrasto e giudiziarie a livello nazionale. Pur senza sostituirsi alle iniziative nazionali, le capacità e le competenze a livello nazionale andrebbero condivise più efficacemente. Gli Stati membri sono incoraggiati a utilizzare i finanziamenti disponibili nell'ambito di programmi nazionali del Fondo Sicurezza interna - Polizia (ISF-P) per istituire, prorogare o sviluppare competenze nazionali. A livello europeo, la Commissione appoggerà Europol nell'espletamento delle funzioni di unità centrale di una rete volta ad agevolare la collaborazione tra i citati centri specializzati nazionali.

In terzo luogo, le autorità degli Stati membri dovrebbero disporre di una **serie di tecniche alternative di indagine** per agevolare la definizione e l'attuazione di misure volte a ottenere le necessarie informazioni cifrate dai criminali. La rete di centri specializzati dovrebbe contribuire a sviluppare gli strumenti e il Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol si trova nella posizione migliore per istituire e conservare un registro di tali tecniche e strumenti. Non saranno prese in esame misure che potrebbero indebolire la crittografia o tali da incidere su un numero elevato o indiscriminato di persone.

In quarto luogo, è opportuno prestare attenzione all'**importante ruolo svolto dai prestatori di servizi e da altri partner dell'industria** nel fornire soluzioni con crittografia forte. Considerando l'impegno della Commissione a favore della crittografia forte, una collaborazione più efficiente e strutturata tra autorità, prestatori di servizi e altri partner dell'industria promuoverebbe una migliore comprensione delle sfide attuali ed emergenti sotto numerosi aspetti. La Commissione sosterrà dialoghi strutturati con i prestatori di servizi e altre imprese nell'ambito del Forum dell'UE su Internet e della rete di centri specializzati, eventualmente con il coinvolgimento della società civile.

In quinto luogo, **i programmi di formazione** destinati alle autorità di contrasto e giudiziarie dovrebbero preparare meglio i funzionari responsabili a ottenere le necessarie informazioni che sono state cifrate dai criminali. Per finanziare l'organizzazione dei programmi di formazione, la Commissione intende mettere a disposizione 500 000 EUR nell'ambito del programma di lavoro annuale 2018 del Fondo Sicurezza interna - Polizia. Sarà fatto ricorso, ove opportuno, alle competenze del Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG). La Commissione sosterrà anche la formazione impartita dall'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL) e gli Stati membri sono incoraggiati a utilizzare ai fini di formazione i fondi disponibili nell'ambito dei rispettivi programmi nazionali del Fondo Sicurezza interna - Polizia.

In sesto luogo, è necessaria una **valutazione costante degli aspetti tecnici e giuridici** del ruolo della crittografia nelle indagini penali, in considerazione della continua evoluzione delle tecniche in questo campo, il loro maggiore uso da parte di criminali e le conseguenze per le indagini penali. La Commissione continuerà tali lavori di grande rilevanza. Sosterrà inoltre lo sviluppo di una funzione di osservatorio in collaborazione con il Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol, il Centro europeo per la lotta alla criminalità informatica giudiziaria europea (EJCN) ed Eurojust.

IV. Combattere la radicalizzazione

1. Gruppo di esperti ad alto livello sulla radicalizzazione

I recenti attentati, in particolare quelli perpetrati da soggetti isolati, e la velocità nel modo in cui gli attentatori si sono radicalizzati, hanno crudelmente ricordato l'importanza di prevenire e contrastare la radicalizzazione. La Commissione ha istituito un G**ruppo di esperti di alto livello sulla radicalizzazione** per intensificare gli sforzi volti a prevenire e a contrastare la radicalizzazione e per migliorare il coordinamento e la cooperazione tra tutti i portatori di interessi, sulla base dei risultati raggiunti sinora[30]. Il gruppo è incaricato di definire raccomandazioni per i lavori futuri in questo settore; una prima relazione intermedia è prevista entro quest'anno. La Commissione riferirà al Consiglio "Giustizia e affari interni" nel dicembre 2017 in merito ai progressi compiuti. Il gruppo esaminerà anche le condizioni necessarie per rafforzare le capacità e le competenze in materia di contrasto alla radicalizzazione, compreso l'eventuale fabbisogno di ulteriori strutture di cooperazione a livello dell'UE. A tale riguardo, alcuni Stati membri hanno chiesto che sia istituito un centro dell'UE per la prevenzione della radicalizzazione e il Gruppo esaminerà la necessità e il valore aggiunto di una siffatta struttura.

La **radicalizzazione nelle carceri** è uno dei temi prioritari che il Gruppo intende discutere. L'attenzione è attualmente rivolta all'attuazione da parte degli Stati membri delle conclusioni del Consiglio GAI sul rafforzamento della risposta penale alla radicalizzazione del 20 novembre 2015[31]. La Commissione organizzerà una conferenza dei portatori di interessi sulla risposta penale alla radicalizzazione il 27 febbraio 2018 per condividere i risultati dei progetti in corso.

La Commissione prenderà in considerazione le conclusioni e raccomandazioni del Gruppo nel piano di lavoro delle iniziative esistenti (in particolare nell'ambito del centro di eccellenza della rete di sensibilizzazione al problema della radicalizzazione), nonché ai fini dell'applicazione e delle priorità dei suoi strumenti di finanziamento (compreso il Fondo Sicurezza interna, così come altri fondi collegati, quali Erasmus +, il programma «Giustizia» o il Fondo sociale europeo).

2. Combattere la radicalizzazione online

I terroristi continuano a utilizzare Internet per radicalizzare, reclutare, preparare e istigare attentati, oltre che per esaltarne le atrocità. Il Consiglio europeo[32], il G7[33] e il G20[34], hanno recentemente chiesto l'adozione di ulteriori azioni per far fronte a tale sfida di livello mondiale e hanno sottolineato la responsabilità dell'industria al riguardo.

Nel luglio 2017 il Forum dell'UE su Internet ha definito un **piano d'azione per contrastare i contenuti di stampo terroristico online**, invitando le imprese di internet a intraprendere un'azione risoluta, destinare risorse e sviluppare gli strumenti tecnologici necessari a garantire

---

30 Cfr. Quinta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2017) 354 final del 29.7.2017).

31 Conclusioni del Consiglio dell'Unione europea e degli Stati membri riuniti in sede di Consiglio sul rafforzamento della risposta di giustizia penale alla radicalizzazione che porta al terrorismo e all'estremismo violento (14419/15).

32 http://www.consilium.europa.eu/it/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.

33 http://www.consilium.europa.eu/it/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

34 http://data.consilium.europa.eu/doc/document/ST-10384-2017-INIT/it/pdf.

la rapida individuazione e rimozione di materiale pericoloso. Il piano d'azione sollecita progressi immediati per un'ampia gamma di settori[35] e istituisce un meccanismo di periodica comunicazione per misurare e valutare i risultati.

Il 29 settembre 2017 la Commissione ha organizzato una riunione a livello di alti funzionari del Forum dell'UE su Internet per fare il punto sull'**attuazione del piano d'azione per contrastare i contenuti terroristici online**. Per quanto riguarda l'individuazione automatica, diverse imprese si stanno muovendo in questa direzione e sono in grado di applicare competenze tecniche per identificare i contenuti terroristici nel punto in cui sono caricati. Alcune imprese hanno riferito che il 75% dei contenuti è ora individuato automaticamente, ma la decisione finale sulla rimozione del contenuto è presa da esaminatori umani, mentre altre indicano che il 95% del contenuto è attualmente individuato attraverso strumenti proprietari. Nonostante si tratti di progressi concreti, la Commissione ha invitato tutte le imprese a intensificare la diffusione di questi strumenti per garantire la rapida individuazione, ridurre i tempi di presenza dei contenuti terroristici online e rimuovere in modo ancora più veloce ed efficace i contenuti di propaganda terroristica. La Commissione ha anche invitato le imprese a espandere il loro strumento "banca dati di hash" per impedire che i contenuti terroristici rimossi possano essere ricaricati su altre piattaforme, e da lì diffusi su piattaforme multiple. Tale strumento dovrebbe essere esteso in termini di contenuto — in aggiunta ai video e alle immagini che sono attualmente presenti — e in termini di società partecipanti.

La Commissione continua anche a sostenere le organizzazioni della società civile che incoraggia a diffondere **messaggi positivi di contro-narrazione** online. Il 6 ottobre 2017 la Commissione ha pubblicato un invito a presentare proposte in vista della concessione di finanziamenti per 6 milioni di EUR a consorzi di soggetti della società civile che sviluppano e attuano tali campagne.

Successivamente, il 6 dicembre 2017 la Commissione europea organizzerà il **Forum dell'UE su Internet a livello ministeriale** con la partecipazione di rappresentanti di alto livello del settore di Internet al fine di valutare i progressi compiuti e preparare il terreno per le azioni future.

Le azioni intraprese contro i contenuti terroristici online nel quadro del Forum dell'UE su Internet dovrebbero essere considerate nel più ampio contesto della lotta contro i contenuti illeciti su internet. Tali azioni sono state rafforzate da una comunicazione adottata dalla Commissione il 28 settembre 2017, che stabilisce **orientamenti e principi per le piattaforme online** affinché intensifichino la lotta contro i contenuti illeciti online[36], in cooperazione con le autorità nazionali, gli Stati membri e gli altri pertinenti portatori di interessi. La comunicazione mira ad agevolare e intensificare l'attuazione di buone pratiche per impedire, rilevare, sopprimere e disabilitare l'accesso al contenuto illecito in modo da assicurarne l'effettiva rimozione, aumentare la trasparenza e tutelare i diritti fondamentali. Essa mira altresì a fornire chiarimenti alle piattaforme sulla loro responsabilità quando adottano misure proattive per individuare, sopprimere o disabilitare l'accesso ai contenuti illegali. La Commissione confida che le piattaforme online agiscano rapidamente nei prossimi

[35] COM(2017) 407 final del 26.7.2017.

[36] Comunicazione "Lotta ai contenuti illeciti online, Verso una maggiore responsabilizzazione delle piattaforme online" (COM(2017) 555 final del 28.9.2017).

mesi, anche nel contesto dei dialoghi pertinenti quali il Forum dell'UE su Internet nei confronti della propaganda terroristica e le forme di incitamento all'odio.

In parallelo, la Commissione monitorerà i progressi e valuterà la necessità di misure supplementari, al fine di garantire l'individuazione e la rimozione rapide e proattive di contenuti illeciti online, comprese eventuali misure legislative ad integrazione del quadro normativo esistente. I lavori saranno conclusi entro maggio 2018.

Sul piano legislativo, la proposta della Commissione[37] per la **revisione della direttiva sui servizi di media audiovisivi**, presentata nel maggio 2016, rafforza la lotta contro l'incitamento all'odio. Essa mira ad allineare la direttiva alla decisione quadro sulla lotta contro talune forme ed espressioni di razzismo e xenofobia[38] e alla Carta dei diritti fondamentali dell'Unione europea. Essa prevede inoltre l'obbligo per gli Stati membri di garantire che le piattaforme di condivisione video adottino misure adeguate per proteggere tutti i cittadini dall'istigazione alla violenza o all'odio. Tali azioni consistono, ad esempio, in meccanismi di contrassegno e segnalazione.

V. LA DIMENSIONE ESTERNA DELL'ANTITERRORISMO

1. Azione esterna dell'UE in materia di lotta al terrorismo

L'azione esterna dell'UE in materia di lotta al terrorismo contribuisce all'obiettivo prioritario di rafforzare la sicurezza interna dell'Unione. É opportuno pertanto rafforzare ulteriormente la continuità, sul piano piano strategico e politico, tra la sicurezza interna ed esterna dell'UE per rafforzare l'efficacia delle azioni di lotta al terrorismo sotto tutti gli aspetti.

La Commissione sostiene una vasta gamma di azioni esterne al fine di rafforzare la sicurezza, con un finanziamento di oltre 2,3 miliardi di euro per più di 600 progetti in corso a partire dal 1º gennaio 2017. Alcune attività vertono sulla sicurezza (cioè le azioni specifiche concernenti questioni quali la lotta contro il finanziamento del terrorismo, la lotta alla radicalizzazione, le carceri, le frontiere) e altre presentano interesse per la sicurezza (cioè programmi che affrontano le cause profonde dell'insicurezza e delle rimostranze contribuendo a migliorare l'istruzione, l'accesso alle risorse naturali e all'energia, il buon governo e il settore della sicurezza, il sostegno alla società civile).

Il Consiglio «Affari esteri», del 19 giugno 2017, ha rinnovato la direzione strategica in questi settori adottando una serie completa di **conclusioni sull'azione esterna dell'UE relativa alla lotta al terrorismo**[39]. L'alta rappresentante e la Commissione europea collaboreranno nella misura necessaria per dare efficace attuazione a dette conclusioni. Per assicurare la tempestiva e completa attuazione delle conclusioni e riferire al Consiglio entro giugno 2018, è stata messa in atto una procedura di coordinamento tra il Servizio europeo per l'azione esterna e la Commissione europea. Sarà data priorità ai seguenti aspetti:

- **rafforzare la rete di esperti antiterrorismo presso le delegazioni dell'UE:** gli esperti antiterrorismo dovrebbero essere coinvolti nella programmazione del sostegno dell'UE e nel coordinamento locale della cooperazione di ciascuno Stato membro con i nostri partner. Per promuovere questo ruolo rafforzato, sarà accelerata la formazione

[37] COM(2016) 287 final del 25.5.2016.
[38] Decisione quadro 2008/913/GAI del Consiglio del 28.11.2008.
[39] http://data.consilium.europa.eu/doc/document/ST-10384-2017-INIT/it/pdf.

impartita prima e durante la missione di tali esperti. I compiti di tali esperti saranno più mirati grazie a lettere d'incarico specifico e il collegamento con le agenzie dell'UE nei settori della giustizia e gli affari interni sarà reso più stabile. Al fine di coprire tutti i settori prioritari, la rete di esperti antiterrorismo[40] sarà ampliata al Corno d'Africa, all'Asia centrale e all'Asia sudorientale;

- **rafforzare la cooperazione tra le missioni e le operazioni relative alla politica di sicurezza e di difesa comune e le agenzie dell'UE in materia di giustizia e affari interni** per la raccolta, l'analisi e lo scambio di informazioni e continuare a esplorare in che modo migliorare i collegamenti tra forze militari e servizi di contrasto ai fini della lotta al terrorismo. Al fine di migliorare lo scambio di dati e di informazioni tra i settori della politica di sicurezza e di difesa comune e quelli della giustizia e degli affari interni, sarà importante promuovere una revisione degli elementi del quadro normativo attuale e pilotare l'integrazione delle cellule dedicate alle informazioni sui reati in determinate missioni e operazioni della politica di sicurezza e di difesa comune. Sarà importante continuare ad agevolare e migliorare i legami con le attività delle agenzie dell'UE del settore Giustizia e affari interni nei paesi terzi prioritari, compreso, ove possibile, potenziare la condivisione di informazioni tra i soggetti dell'UE e di paesi terzi;
- **rafforzare la cooperazione internazionale nella lotta contro il terrorismo e la prevenzione e la lotta contro l'estremismo violento** con paesi partner dei Balcani occidentali, del Medio Oriente, del Nord Africa, del Golfo, la Turchia, il Sahel e il Corno d'Africa; con i principali partner strategici, tra cui gli Stati Uniti, il Canada e l'Australia; e con i principali partner regionali e multilaterali come le Nazioni Unite, la NATO, il Forum globale contro il terrorismo, il GAFI, l'Unione africana, l'Associazione delle Nazioni del Sud-Est Asiatico, il Consiglio di cooperazione del Golfo e la Lega degli Stati arabi.

2. Convenzione del Consiglio d'Europa per la prevenzione del terrorismo

Per rafforzare la cooperazione internazionale in materia di lotta al terrorismo, la Commissione presenta, unitamente alla presente relazione, le **proposte**[41] **di decisioni del Consiglio relative alla conclusione della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e del suo protocollo addizionale**. La Convenzione[42], adottata dal Consiglio d'Europa il 16 maggio 2005, riguarda l'incriminazione di atti di terrorismo e le attività legate al terrorismo, la cooperazione internazionale per tali reati e la protezione, il risarcimento e il sostegno delle vittime del terrorismo. La Convenzione è entrata in vigore il 1° giugno 2007. Tutti gli Stati membri dell'UE hanno firmato la Convenzione e 23 Stati membri dell'UE l'hanno ratificata. L'obiettivo del protocollo addizionale[43], adottato dal Consiglio d'Europa il 18 maggio 2015, è quello di integrare la Convenzione con una serie di disposizioni volte ad applicare il diritto penale gli aspetti della risoluzione 2178(2014)[44] del Consiglio di sicurezza delle Nazioni Unite sulle minacce alla pace e alla sicurezza internazionali causate da atti terroristici. Il protocollo addizionale risponde a tale risoluzione favorendo una comprensione

---

40 Ad oggi, l'UE ha distaccato esperti antiterrorismo presso le proprie delegazioni in: Algeria, Bosnia-Erzegovina (con mandato regionale per i Balcani occidentali), Ciad (Sahel), Iraq, Giordania, Libano, Libia (di stanza a Tunisi), Marocco, Nigeria, Pakistan, Arabia Saudita, Tunisia e Turchia.

41 COM(2017) 606 final del 18.10.2017 e COM(2017) 607 final del 18.10.2017.

42 https://rm.coe.int/168008371c.

43 https://rm.coe.int/168047c5ea.

44 http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf.

comune dei reati connessi ai combattenti terroristi stranieri e una risposta comune. Il protocollo addizionale è entrato in vigore il 1º luglio 2017.

L'UE ha firmato la convenzione e il suo protocollo addizionale il 22 ottobre 2015. Considerando che l'UE ha adottato una serie completa di strumenti giuridici per contrastare il terrorismo, in particolare la direttiva sulla lotta contro il terrorismo[45], l'UE è ora pronta a onorare il suo impegno di aderire alla convenzione e al suo protocollo addizionale.

3. Verso un accordo rivisto sul codice di prenotazione (PNR) con il Canada

Nel suo parere del 26 luglio 2017[46], la Corte di giustizia dell'Unione europea ha stabilito che l'accordo tra il Canada e l'Unione europea sul trasferimento e sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR), firmato il 25 giugno 2014, non può essere concluso nella sua forma attuale, in quanto molte delle sue disposizioni sono incompatibili con i diritti fondamentali riconosciuti dall'UE, in particolare il diritto alla protezione dei dati e al rispetto della vita privata. La Commissione è attualmente in contatto con il Canada, che incontrerà anche a margine della prossima riunione dei ministri dell'Interno del G7 a Ischia il 19/20 ottobre 2017, per preparare i prossimi negoziati volti alla revisione del testo dell'accordo. A tal fine, la Commissione ha presentato, unitamente alla presente relazione, una **raccomandazione**[47] **al Consiglio volta ad autorizzare l'apertura di negoziati per un accordo rivisto** conforme a tutti i requisiti stabiliti dalla Corte nel suo parere. Il Consiglio è invitato ad autorizzare rapidamente l'avvio di tali negoziati. Giacché l'uso dei dati PNR è uno strumento importante nella lotta al terrorismo e ai reati gravi di natura transnazionale, la Commissione adotterà tutte le misure necessarie per garantire la prosecuzione del trasferimento di dati PNR al Canada, nel pieno rispetto dei diritti fondamentali in conformità con il parere della Corte.

In tale contesto, la Commissione sottolinea il suo costante sostegno agli Stati membri nell'attuazione della direttiva PNR dell'UE[48]; gli obblighi degli Stati membri derivanti da tale direttiva non sono pregiudicati dal parere della Corte.

4. Rafforzare la cooperazione di Europol con i paesi terzi

La cooperazione con i paesi terzi è fondamentale nella lotta contro il terrorismo e la criminalità organizzata, come sottolineato nelle conclusioni del Consiglio «Affari esteri» del giugno 2017 sull'azione esterna dell'UE relativa alla lotta al terrorismo[49] e le strategie regionali dell'UE[50]. Prima dell'entrata in vigore del nuovo regolamento Europol[51] il 1º maggio 2017, Europol ha concluso, in forza della precedente base giuridica[52], accordi con una serie di paesi terzi al fine di garantire un quadro di cooperazione per lo scambio di

---

45 Direttiva (UE) 2017/541 del 15.3.2017.
46 Parere 1/15 della Corte di giustizia, del 26.7.2017.
47 COM(2017) 605 final del 18.10.2017.
48 Direttiva (UE) 2016/681 del 27.4.2016.
49 http://data.consilium.europa.eu/doc/document/ST-10384-2017-INIT/it/pdf.
50 Ciò comprende la nuova politica europea di vicinato (JOIN(2015) 50 final del 18.11.2015).
51 Regolamento (UE) n. 2016/794 del 11.5.2016.
52 Decisione 2009/371/GAI del Consiglio del 6.4.2009.

informazioni strategiche e tecniche. Alcuni di questi accordi prevedono anche la possibilità di scambiare dati personali[53]. Tali accordi rimarranno in vigore.

Dal 1º maggio 2017, il nuovo **regolamento Europol** stabilisce le norme sulle relazioni esterne di Europol con i paesi terzi, in particolare le condizioni per lo scambio di dati personali con gli organismi dell'Unione, i paesi terzi e le organizzazioni internazionali. A norma del trattato e del regolamento, la Commissione è competente a negoziare, a nome dell'Unione, accordi internazionali con paesi terzi per lo scambio di dati personali con Europol[54]. Nella misura necessaria per lo svolgimento dei suoi compiti, Europol può instaurare e mantenere relazioni di cooperazione con partner esterni attraverso accordi di lavoro e amministrativi che non consentono lo scambio di dati personali.

Alla luce delle esigenze operative dell'Unione in termini di cooperazione in materia di sicurezza con i paesi terzi, e in linea con il regolamento Europol, la **Commissione presenterà raccomandazioni al Consiglio entro la fine dell'anno** affinché autorizzi l'avvio di negoziati per un accordo tra l'Unione europea e l'Algeria, l'Egitto, Israele, la Giordania, il Libano, il Marocco, la Tunisia e la Turchia al fine di fornire una base giuridica per il trasferimento di dati personali tra Europol e i citati paesi terzi[55]. Tali accordi rafforzeranno ulteriormente la capacità di Europol di dialogare con tali paesi terzi al fine di prevenire e combattere i reati che rientrano nell'ambito degli obiettivi di Europol.

VI. CONCLUSIONE

La presente relazione definisce un pacchetto di misure antiterrorismo che continuerà a sostenere gli Stati membri nei loro sforzi volti ad affrontare le attuali minacce alla sicurezza. La Commissione invita gli Stati membri e il Consiglio ad attuare tali misure in via prioritaria. La Commissione terrà informato il Parlamento europeo e il Consiglio dei progressi compiuti.

La prossima relazione sullo stato dei lavori relativo all'Unione della sicurezza sarà presentata nel dicembre 2017, con un'attenzione particolare per l'interoperabilità dei sistemi d'informazione dell'Unione europea per la sicurezza e la gestione delle frontiere e della migrazione. In questo contesto, la Commissione ricorda l'importanza di compiere progressi sulle priorità legislative su tali sistemi di informazione.

---

53 Europol ha concluso accordi per consentire lo scambio di dati personali con i paesi terzi seguenti: Albania, Australia, Bosnia-Erzegovina, Canada, Colombia, ex Repubblica jugoslava di Macedonia, Georgia, Islanda, Liechtenstein, Moldova, Monaco, Montenegro, Norvegia, Serbia, Svizzera, Ucraina e Stati Uniti. Il consiglio di amministrazione di Europol ha autorizzato l'avvio di negoziati su un accordo tra Europol e Israele, ma i negoziati non erano giunti a conclusione al momento in cui il nuovo regolamento Europol è entrato in applicazione.

54 Il regolamento Europol prevede inoltre il trasferimento di dati personali tra Europol e un paese terzo sulla base di una decisione della Commissione che accerta che il paese in questione garantisce un livello adeguato di protezione dei dati («decisione sull'adeguatezza»).

55 Al di là di questi paesi terzi, la Commissione ricorda il quadro strategico per le «decisioni di adeguatezza» nonché altri strumenti per i trasferimenti di dati e strumenti internazionali in materia di protezione dei dati, conformemente a quanto stabilito nella comunicazione della Commissione per lo scambio e la protezione dei dati personali in un mondo globalizzato (COM(2017) 7 final del 10.1.2017) in cui la Commissione incoraggia l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa n. 108 e relativo protocollo addizionale.