COMMISSIONE
EUROPEA

Strasburgo, 17.4.2018
COM(2018) 211 final

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

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

I. INTRODUZIONE

Il presente documento è la quattordicesima relazione 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 e della criminalità organizzata e dei relativi mezzi di sostegno, e rafforzare le nostre difese e la nostra resilienza contro tali minacce.

I brutali attentati perpetrati a Trèbes e Carcassonne, in Francia, il 23 marzo 2018 ricordano quanto sia tuttora grave la minaccia terroristica nell'UE. Nell'ambito del costante impegno profuso nell'Unione della sicurezza per reagire a tale minaccia, la Commissione presenta, insieme alla presente relazione, un nuovo pacchetto sulla sicurezza che prevede misure volte a ridurre il margine di manovra dei terroristi e altri criminali, rendendo loro più difficile progettare ed eseguire le loro azioni efferate. Il pacchetto comprende misure legislative dirette a migliorare l'accesso transfrontaliero alle **prove elettroniche** e alle **informazioni finanziarie** ai fini delle indagini e delle azioni penali, segnatamente per i reati gravi, rafforzando inoltre la cooperazione tra le unità di informazione finanziaria e le autorità di contrasto. Comprende inoltre misure operative per impedire l'accesso di terroristi e altri criminali alle **armi da fuoco** importate e ai **precursori di esplosivi** che possono essere impropriamente utilizzati per la fabbricazione di esplosivi artigianali, come sperimentato in vari attentati recenti. Infine, una proposta legislativa volta a migliorare la **sicurezza delle carte d'identità e dei titoli di soggiorno nazionali** renderà molto più difficile per i terroristi e altri criminali abusare di tali documenti o falsificarli per entrare o spostarsi nell'UE.

L'attentato di Salisbury del 4 marzo 2018 rappresenta un esempio sconvolgente della vera e propria minaccia che le sostanze chimiche possono rappresentare per la sicurezza collettiva. Il 22-23 marzo 2018 il Consiglio europeo ha condannato l'attacco nei termini più decisi possibili, sottolineando che per reagire l'UE deve fra l'altro rafforzare la sua resilienza ai rischi chimici, biologici, radiologici e nucleari. La presente relazione presenta le misure adottate a questo scopo, attuando il piano d'azione dell'ottobre 2017 per rafforzare la preparazione contro questi rischi per la sicurezza. Contiene inoltre un aggiornamento sull'attuazione di altre iniziative prioritarie nell'Unione della sicurezza: la lotta contro la radicalizzazione online, il miglioramento della condivisione delle informazioni, il sostegno alla protezione degli spazi pubblici e la lotta contro le minacce informatiche.

II. RIDURRE IL MARGINE DI MANOVRA DEI TERRORISTI E DEI CRIMINALI

1. Nuove regole per ottenere prove elettroniche nei procedimenti penali

Le prove elettroniche sono divenute importanti nella vasta maggioranza delle indagini penali e sempre più spesso le autorità giudiziarie devono inoltrare una richiesta in un'altra giurisdizione per ottenere le prove necessarie da prestatori di servizi. Rendere più facile e più veloce l'acquisizione di queste prove oltrefrontiera è quindi di cruciale importanza per l'indagine e l'azione penale, anche in caso di terrorismo o criminalità informatica. A questo scopo la Commissione presenta, insieme alla presente relazione, due proposte legislative volte a migliorare l'acquisizione transfrontaliera di prove elettroniche per i procedimenti penali: una proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali[1] e una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei

[1] COM(2018) 225 final del 17.4.2018.

procedimenti penali[2]. Il regolamento e la direttiva proposti forniranno alle autorità di contrasto e alle autorità giudiziarie competenti nuovi strumenti per acquisire prove elettroniche ai fini dell'indagine e dell'azione penale, anche per i reati di terrorismo e criminalità informatica. Con queste proposte la Commissione risponde agli inviti rivoltile dal Parlamento europeo e dal Consiglio affinché presentasse un quadro legislativo a livello di UE contenente misure volte ad agevolare l'acquisizione di prove elettroniche al di là delle frontiere, unite a solide garanzie a tutela dei diritti e delle libertà dei cittadini[3].

Il regolamento proposto crea un ordine europeo di produzione e un ordine europeo di conservazione. Tali ordini permetteranno alle autorità competenti di uno Stato membro di ingiungere direttamente ai prestatori di servizi (prestatori di servizi di comunicazione elettronica e specifici prestatori di servizi della società dell'informazione) stabiliti o rappresentati in un altro Stato membro di conservare o produrre dati elettronici esistenti ai fini dell'indagine e del perseguimento di reati che rientrano nel campo di applicazione del regolamento, in maniera proporzionata e necessaria in ciascun caso specifico. Per garantire che gli ordini siano eseguiti, la direttiva proposta impone ai prestatori di servizi di designare almeno un rappresentante legale nell'Unione. Dato che internet non conosce frontiere, le proposte riguardano i prestatori di servizi che offrono servizi in uno o più Stati membri, a prescindere dal luogo in cui sono situate la loro sede principale e le loro infrastrutture e in cui vengono conservate le informazioni.

Il regolamento proposto prevede solide garanzie per assicurare il pieno rispetto dei diritti fondamentali, quali l'intervento preliminare delle autorità giudiziarie e requisiti supplementari per l'acquisizione di alcune categorie di dati. Inoltre, poiché gli ordini possono essere emessi soltanto nel quadro di procedimenti penali e se previsto in situazioni nazionali analoghe, si applicano tutte le garanzie procedurali in materia penale. In più, il regolamento prevede norme specifiche relative a mezzi di ricorso effettivi per le persone interessate. Prevede inoltre il diritto del prestatore di servizi di chiedere un riesame nello Stato membro di emissione o, se l'ordine è trasmesso per l'esecuzione, nello Stato membro ospitante, sulla base di motivi specifici, ad esempio casi in cui risulta evidente che l'ordine non è stato emesso o convalidato da un'autorità competente, è incompleto, viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o è manifestamente arbitrario. Infine, il regolamento contiene un meccanismo per evitare e attenuare potenziali conflitti con eventuali obblighi imposti ai prestatori di servizi da legislazioni di paesi terzi.

Le proposte legislative sono basate su un'accurata valutazione d'impatto e su un processo biennale di consultazione cui hanno partecipato professionisti, cittadini, prestatori di servizi, organizzazioni governative e non governative e accademici[4]. La Commissione ha inoltre partecipato alle discussioni sull'argomento nell'ambito del Consiglio d'Europa e ha seguito attentamente gli sviluppi nei paesi terzi, tra cui la recente adozione da parte del Congresso degli Stati Uniti del "Clarifying Lawful Overseas Use of Data" (CLOUD Act), la legge recante chiarimento sull'utilizzo legittimo di dati all'estero. Le proposte adottate insieme alla presente relazione forniscono la base per un approccio coordinato e coerente sia all'interno

---

2 COM(2018) 226 final del 17.4.2018.

3 Conclusioni del Consiglio sul miglioramento della giustizia penale nel ciberspazio (ST 9579/16) e risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068 (INI)).

4 La relazione sulla consultazione è disponibile sul seguente sito: https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en; ulteriori informazioni sono disponibili su https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

dell'UE sia da parte dell'UE a livello internazionale, con la debita attenzione alle norme dell'UE, segnatamente quelle sul divieto di discriminazione tra gli Stati membri dell'UE e i loro cittadini. La Commissione continua inoltre a partecipare attivamente alle discussioni nel quadro della Convenzione del Consiglio d'Europa sulla criminalità informatica.

La Commissione esorta i colegislatori a esaminare senza indugio la normativa proposta, che è prevista nella dichiarazione comune sulle priorità legislative dell'UE per il periodo 2018-2019, per raggiungere rapidamente un accordo.

Parallelamente a queste proposte legislative, la Commissione continua a elaborare **misure pratiche per migliorare la cooperazione giudiziaria** sulla base dell'assistenza giudiziaria e della direttiva sull'ordine europeo di indagine penale[5], nonché della cooperazione tra autorità e prestatori di servizi nel quadro giuridico vigente. Tali misure comprendono la formazione delle autorità, la promozione dell'uso dei punti di contatto unici a livello nazionale e la creazione di una piattaforma online per lo scambio sicuro di richieste e risposte relative all'ordine europeo di indagine, basato su una versione elettronica dei moduli di ordini europei di indagine. La Commissione collabora intensamente con le agenzie dell'UE competenti[6] e con i portatori di interessi per assicurarne la rapida attuazione.

2. Facilitare l'uso delle informazioni finanziarie a fini di prevenzione, accertamento, indagine o perseguimento di reati gravi

Criminali e terroristi operano in più Stati membri e sono in grado di trasferire fondi tra diversi conti bancari in poche ore per preparare le loro azioni o per spostare e riciclare i proventi di attività criminose. Le indagini sui reati gravi e di terrorismo possono giungere a un punto morto per mancanza di un accesso tempestivo, accurato e completo ai dati finanziari pertinenti[7]. Data l'importanza delle informazioni finanziarie per le indagini, è cruciale intensificare la cooperazione tra le autorità competenti per la lotta contro i reati gravi e il terrorismo e facilitare loro l'accesso alle informazioni finanziarie e l'uso delle medesime, nel pieno rispetto dei diritti fondamentali e delle garanzie procedurali applicabili. A questo scopo la Commissione ha adottato, insieme alla presente relazione, una **proposta di direttiva per facilitare l'uso delle informazioni finanziarie e di altre informazioni** a fine di prevenzione, accertamento, indagine o perseguimento di reati gravi[8].

La proposta, basata su un'approfondita valutazione d'impatto, conferisce ad autorità di contrasto e uffici per il recupero dei beni designati un **accesso diretto alle informazioni sui conti bancari** detenuti in registri nazionali centralizzati dei conti bancari e in sistemi nazionali di reperimento dei dati, come previsto dalla direttiva antiriciclaggio[9]. L'accesso sarà

---

5 Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale (GU L 130 dell'1.5.2014, pag. 1).

6 Europol, Eurojust e Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL).

7 La relazione di Europol "From suspicion to action: converting financial intelligence into greater operational impact" ("Dal sospetto all'azione - conversione di informazioni finanziarie in un maggiore impatto operativo"), pubblicata nel 2017, sottolinea questi problemi e l'esigenza di un migliore accesso delle autorità di contrasto alle informazioni finanziarie.

8 COM(2018) 213 final del 17.4.2018.

9 Nel dicembre 2017 i colegislatori dell'Unione hanno concordato queste misure come una delle modifiche alla direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (GU L 141 del 5.6.2015, pag. 73).

accordato **caso per caso ai fini della lotta contro le forme gravi di criminalità.** Tali disposizioni, fra l'altro, diminuiranno notevolmente l'onere amministrativo a carico delle istituzioni finanziarie, che non dovranno più rispondere a richieste generalizzate di informazioni da parte di autorità di contrasto.

La proposta rafforza ulteriormente la cooperazione tra le **unità di informazione finanziaria** e le autorità di contrasto nazionali, nonché tra le varie unità di informazione finanziaria dei diversi Stati membri. Inoltre, gli Stati membri dovranno provvedere affinché le loro unità nazionali Europol rispondano alle richieste di Europol volte a ottenere informazioni contenute nei registri centralizzati dei conti bancari, informazioni finanziarie e analisi finanziarie. Le richieste presentate da Europol dovranno essere debitamente giustificate e presentate caso per caso, entro i limiti delle competenze di Europol e ai fini dell'adempimento dei suoi compiti. Un migliore accesso ai dati finanziari da parte delle autorità di contrasto e una migliore cooperazione con le unità di informazione finanziaria accelereranno le indagini e consentiranno alle autorità di combattere più efficacemente la criminalità transfrontaliera. Europol sarà inoltre in grado di offrire un più valido sostegno agli Stati membri nella lotta contro i reati che rientrano nelle sue competenze. Per rispettare i diritti fondamentali alla protezione dei dati personali e alla tutela della vita privata, la proposta di direttiva prevede rigorose garanzie relative al trattamento dei dati personali.

La Commissione esorta i colegislatori a esaminare senza indugio la proposta, che è compresa nella dichiarazione comune sulle priorità legislative dell'UE per il periodo 2018-2019, per raggiungere rapidamente un accordo. La Commissione ribadisce inoltre l'importanza di attuare e applicare pienamente la quarta direttiva antiriciclaggio e gli strumenti che offre per combattere il riciclaggio e il finanziamento del terrorismo, ivi compreso l'obbligo di fornire alle unità di informazione finanziaria risorse adeguate per adempiere i loro compiti. Inoltre, in seguito alla modifica della quarta direttiva antiriciclaggio - approvata a livello politico dai colegislatori nel dicembre 2017 - la Commissione è tenuta a presentare entro giugno 2020 una relazione al Parlamento europeo e al Consiglio in cui valuta la possibilità di una futura interconnessione dei registri centralizzati dei conti bancari. A questo scopo la Commissione sta svolgendo uno studio i cui risultati saranno presentati entro la metà del 2019.

3. Norme rafforzate contro i precursori di esplosivi usati per fabbricare esplosivi artigianali

Terroristi e criminali hanno usato esplosivi artigianali in molti attentati perpetrati nell'UE, tra cui quelli di Madrid (2004), Londra (2005), Parigi (2015), Bruxelles (2016), Manchester (2017) e Parsons Green (2017), e l'uso di tali esplosivi era previsto in un numero ancora superiore di attentati falliti o sventati. Tali attacchi evidenziano la necessità di impedire il più possibile che i terroristi accedano a precursori di esplosivi che possano essere impropriamente utilizzati per fabbricare esplosivi artigianali, e che li sfruttino. A questo scopo la Commissione presenta, insieme alla presente relazione, una **proposta**[10] **di revisione e rafforzamento delle restrizioni attualmente previste dal regolamento 98/2013 relativo all'immissione sul mercato e all'uso di precursori di esplosivi**[11]. Tale proposta fa seguito alla raccomandazione della Commissione[12] dell'ottobre 2017 che presenta azioni immediate per prevenire l'uso improprio di precursori di esplosivi sulla base delle norme esistenti, e si

[10] COM(2018) 209 final del 17.4.2018.

[11] Regolamento (UE) n. 98/2013 del Parlamento europeo e del Consiglio, del 15 gennaio 2013, relativo all'immissione sul mercato e all'uso di precursori di esplosivi (GU L 39 del 9.2.2013, pag. 1).

[12] Raccomandazione della Commissione del 18.10.2017 relativa a misure immediate volte a prevenire l'uso improprio dei precursori di esplosivi (C (2017) 6950 final).

basa su una serie di consultazioni di vari gruppi di portatori di interessi e su un'approfondita valutazione d'impatto. A norma del regolamento del 2013, la messa a disposizione, l'introduzione, la detenzione e l'uso di alcuni precursori di esplosivi sono soggetti a restrizioni e le transazioni sospette devono essere segnalate. Tali restrizioni e controlli hanno contribuito a ridurre la quantità di precursori di esplosivi disponibili ai privati e hanno permesso di aumentare il numero di segnalazioni di transazioni sospette, ma si sono dimostrati insufficienti a impedire che terroristi e criminali usino impropriamente tali sostanze per fabbricare esplosivi.

La proposta della Commissione contribuirà a colmare queste lacune in materia di sicurezza e a rafforzare e chiarire il quadro giuridico. Scopo del regolamento proposto (destinato a sostituire il regolamento del 2013) è limitare ulteriormente l'accesso dei privati a precursori di esplosivi pericolosi mediante una serie di misure: sono aggiunte due sostanze[13] all'elenco dei precursori di esplosivi, è ridotto il numero di sostanze per le quali sarà possibile chiedere una licenza e sono rafforzate le verifiche obbligatorie dei casellari giudiziali dei richiedenti. Il sistema di registrazione previsto dal regolamento del 2013 sarà eliminato, poiché meno adatto a garantire la sicurezza. Inoltre la proposta chiarisce che le norme applicabili agli operatori economici si applicheranno pienamente anche alle vendite online. Il regolamento proposto permetterà una migliore esecuzione da parte delle autorità competenti e una migliore trasmissione delle informazioni lungo la catena di approvvigionamento. In tal modo, renderà notevolmente più difficile per i terroristi fabbricare esplosivi artigianali. La Commissione esorta i colegislatori a esaminare senza indugio la proposta legislativa per raggiungere rapidamente un accordo.

4. Carte d'identità e titoli di soggiorno più sicuri per impedire la frode documentale e l'uso di false identità

Come dimostrano le statistiche dell'Agenzia europea della guardia di frontiera e costiera sui documenti falsi, le carte d'identità nazionali con elementi di sicurezza più deboli sono i documenti di viaggio usati più spesso in modo fraudolento all'interno dell'UE. Nell'ambito della risposta europea alle frodi riscontrate nei documenti di viaggio delineata nel piano d'azione del dicembre 2016[14], la Commissione presenta, insieme alla presente relazione, una **proposta di regolamento volto a rafforzare la sicurezza delle carte d'identità rilasciate ai cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari**[15]. In virtù della normativa dell'UE sulla libera circolazione, i cittadini dell'UE possono usare le carte d'identità nazionali come documenti di viaggio, sia quando viaggiano nell'UE, sia quando attraversano le frontiere esterne dell'UE per ritornarvi. In alcuni casi i cittadini dell'UE possono usare carte d'identità nazionali per entrare nei paesi terzi. Le carte di soggiorno rilasciate ai familiari non aventi la cittadinanza di uno Stato membro, utilizzate insieme a un passaporto, danno diritto a tali familiari di entrare nell'UE senza visto quando accompagnano un cittadino dell'UE. Il diritto dell'UE prevede già norme sugli elementi di sicurezza e sugli elementi biometrici (immagine del volto e impronte digitali) dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri[16].

Il rafforzamento degli elementi di sicurezza delle carte d'identità e dei titoli di soggiorno renderà più difficile per i criminali abusare di tali documenti o falsificarli al fine di spostarsi

---

13 Acido solforico e nitrato di ammonio.
14 COM(2016) 790 final del 8.12.2016.
15 COM(2018) 212 final del 17.4.2018.
16 Regolamento (CE) n. 2252/2004 (GU L 385 del 29.12.2004, pag. 1).

all'interno dell'UE o attraversarne le frontiere esterne. Documenti d'identità più sicuri contribuiranno a potenziare la gestione delle frontiere esterne dell'UE (anche per quanto riguarda i problemi inerenti al rimpatrio di combattenti terroristi stranieri e dei loro familiari) e al contempo documenti più sicuri e affidabili agevoleranno i cittadini dell'UE nell'esercizio dei loro diritti di libera circolazione.

La proposta della Commissione, basata su un'approfondita valutazione d'impatto e su una consultazione pubblica, stabilisce quindi norme minime sugli elementi di sicurezza dei documenti per le carte d'identità nazionali, segnatamente l'obbligo di inserire una fotografia biometrica e le impronte digitali in un chip nella carta d'identità. Prevede inoltre l'obbligo di fornire informazioni minime sui titoli di soggiorno rilasciati ai cittadini mobili dell'UE e la piena armonizzazione delle carte di soggiorno di familiari che non sono cittadini dell'UE.

La Commissione esorta i colegislatori a esaminare senza indugio la proposta legislativa per raggiungere rapidamente un accordo.

5. Migliorare il controllo dell'importazione e dell'esportazione delle armi da fuoco per impedirne il traffico illecito

La Commissione ha avviato una serie di azioni volte a limitare la capacità dei criminali e dei terroristi di procurarsi armi da fuoco. Per completare l'iniziativa contro il traffico di armi da fuoco[17] e la revisione della direttiva relativa al controllo dell'acquisizione e della detenzione di armi, del maggio 2017, la Commissione presenta, insieme alla presente relazione, una **raccomandazione**[18] sull'adozione di disposizioni immediate miranti a migliorare la sicurezza delle misure di esportazione, importazione e transito di armi da fuoco, loro parti e componenti essenziali e munizioni. La raccomandazione esorta gli Stati membri dell'UE a prendere iniziative per **migliorare la tracciabilità e la sicurezza delle procedure di controllo all'esportazione e all'importazione delle armi da fuoco e la cooperazione tra le autorità nella lotta contro il traffico di armi da fuoco**. Tale raccomandazione fa seguito alla relazione sull'attuazione del regolamento (UE) n. 258/2012[19] sulle esportazioni e importazioni delle armi da fuoco presentata dalla Commissione nel dicembre 2017, in cui si concludeva che occorre rafforzare il sistema delle autorizzazioni all'esportazione e all'importazione di armi da fuoco per controllare le condizioni del commercio legale e in tal modo combattere meglio il traffico illecito di armi da fuoco. La Commissione controllerà i risultati di tale raccomandazione, che serviranno al monitoraggio generale dell'applicazione del suddetto regolamento.

III. ATTUAZIONE DI ALTRE INIZIATIVE PRIORITARIE IN MATERIA DI SICUREZZA

1. Combattere i contenuti terroristici online

[17] Si veda il piano d'azione dell'UE contro il traffico e l'uso illecito di armi da fuoco ed esplosivi (COM(2015) 624 final del 2.12.2015). Smantellare i gruppi criminali coinvolti nel traffico, nella distribuzione e nell'uso illecito di armi da fuoco è anche una delle priorità del ciclo programmatico dell'UE per contrastare la criminalità organizzata e le formi gravi di criminalità per il periodo 2018-2021.

[18] C(2018) 2197.

[19] Regolamento (UE) n. 258/2012 che dispone autorizzazioni all'esportazione, misure di importazione e di transito per le armi da fuoco, loro parti e componenti e munizioni.

Come dichiara nel programma di lavoro per il 2018 e in precedenti relazioni sull'Unione della sicurezza, la Commissione promuove e favorisce la cooperazione con piattaforme internet per individuare e rimuovere contenuti illeciti online terroristici o di altra natura. Il 1° marzo 2018 la Commissione ha preso un'altra iniziativa importante per affrontare il problema grave e urgente dei contenuti terroristici online, adottando una **raccomandazione** sulle misure che devono prendere i prestatori di servizi online e gli Stati membri per intensificare gli sforzi relativi ai **contenuti illeciti online, in particolare i contenuti terroristici**[20].

Sulla base della comunicazione del settembre 2017 sulla lotta ai contenuti illeciti online[21], la raccomandazione esorta i prestatori di servizi online a provvedere a una più rapida individuazione e rimozione di tali contenuti, a intensificare la cooperazione tra gli stessi prestatori di servizi online, i segnalatori attendibili e le autorità di contrasto dell'UE, ad accrescere la trasparenza delle relazioni alle autorità pubbliche e a prevedere garanzie dei diritti fondamentali dei cittadini. La raccomandazione fornisce ai prestatori di servizi online orientamenti operativi per rimuovere più rapidamente i contenuti terroristici e cooperare meglio con le autorità di contrasto. Poiché i contenuti terroristici sono generalmente più dannosi entro la prima ora dalla pubblicazione online, e date le specifiche competenze e responsabilità delle autorità competenti e di Europol, la raccomandazione sottolinea che i prestatori di servizi online dovrebbero esaminare e, se del caso, rimuovere i contenuti identificati nelle segnalazioni qualificate o disabilitare l'accesso ai medesimi entro un'ora come regola generale. Raccomanda inoltre alle piattaforme di adottare misure proattive e fare ricorso a strumenti automatizzati al fine di rilevare e identificare i contenuti terroristici e di usare gli strumenti tecnologici disponibili per impedire che tali contenuti siano ripubblicati su altre piattaforme.

È attualmente in corso un esercizio di segnalazione per monitorare gli effetti della raccomandazione. Le informazioni che i prestatori di servizi online dovrebbero trasmettere entro l'inizio di maggio 2018 aiuteranno la Commissione a decidere se l'attuale approccio sia sufficiente o se occorrano misure aggiuntive per garantire l'individuazione e la rimozione rapide e proattive dei contenuti illeciti online, comprese eventuali misure legislative a completamento del quadro normativo vigente.

2. Verso l'interoperabilità dei sistemi d'informazione e un migliore scambio di informazioni

Nell'intento di ottenere sistemi d'informazione più solidi e intelligenti per la gestione della sicurezza, delle frontiere e della migrazione, l'UE sta affrontando urgentemente e in via prioritaria le carenze nella gestione e nella condivisione delle informazioni dell'UE. Tutte le relative proposte legislative sono incluse nella dichiarazione comune sulle priorità legislative dell'UE per il periodo 2018-2019. Le discussioni tra i colegislatori sulle proposte legislative relative all'**interoperabilità** dei sistemi d'informazione dell'UE stanno progredendo. In seguito al Consiglio Giustizia e affari interni dell'8 marzo 2018, in cui gli Stati membri hanno espresso un vasto consenso per le componenti dell'interoperabilità proposte dalla Commissione, il Consiglio mira a concordare un approccio generale entro giugno 2018. Anche le discussioni tecniche in seno al Parlamento europeo stanno avanzando rapidamente, nell'intento di avviare i triloghi con i colegislatori entro luglio 2018 e di raggiungere un

[20] Raccomandazione della Commissione dell'1.3.2018 sulle misure per contrastare efficacemente i contenuti illegali online (C(2018) 1177 final).

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

accordo entro la fine dell'anno. A tale scopo, e come annunciato nel dicembre 2017[22], è necessario presentare modifiche adeguate delle proposte sull'interoperabilità in relazione agli strumenti giuridici[23] che sono attualmente oggetto di negoziati da parte dei colegislatori. Dato l'obiettivo comune di raggiungere un accordo sulle proposte relative all'interoperabilità entro la fine del 2018, come previsto nella dichiarazione comune sulle priorità legislative dell'UE per il periodo 2018-2019, occorre pertanto **raggiungere rapidamente un accordo sulle iniziative che sono ancora oggetto di negoziati**. In ogni caso, la Commissione presenterà entro la metà di giugno 2018 tutte le necessarie modifiche delle sue proposte sull'interoperabilità per consentire l'avvio dei triloghi entro luglio 2018.

I negoziati interistituzionali per stabilire un **sistema europeo di informazione e autorizzazione ai viaggi** (ETIAS) hanno raggiunto la fase finale e l'adozione dovrebbe avvenire nel corso delle prossime settimane.

È in corso un'intensa attività per progredire nei negoziati nell'ambito del trilogo tra i colegislatori sulle tre proposte legislative volte a rafforzare il **sistema d'informazione Schengen** (SIS), al fine di raggiungere un accordo politico. La Commissione esorta i colegislatori a raggiungere un accordo sulle proposte entro la fine di maggio 2018. Parallelamente a questo lavoro legislativo, il 5 marzo 2018 è stata lanciata una funzionalità per un **sistema automatico per il riconoscimento delle impronte digitali** (AFIS) allo scopo di rafforzare il sistema d'informazione Schengen nella sua forma attuale. Questo miglioramento tecnico presenta un immediato e significativo valore aggiunto per l'attività delle guardie di frontiera e delle autorità di contrasto, in quanto permette loro di interrogare il sistema utilizzando le impronte digitali per identificare le persone che entrano o si spostano nello spazio Schengen. Costituisce quindi una pietra miliare per la sicurezza nello spazio Schengen, dal momento che renderà più facile identificare i criminali che usano identità multiple o false. Da oggi tutte le impronte digitali registrate per la prima volta sono confrontate con tutte le registrazioni esistenti nel SIS per individuare i casi di identità multiple. Inoltre, gli undici Stati Schengen che partecipano alla prima fase di questo progetto[24] effettuano ora interrogazioni utilizzando impronte digitali. Il nuovo quadro giuridico del SIS proposto dalla Commissione si basa sulla funzionalità AFIS in quanto prevede verifiche obbligatorie delle impronte digitali nei casi in cui l'identità della persona non possa essere accertata altrimenti. La Commissione invita tutti gli altri Stati membri a prendere le iniziative necessarie per usare la nuova funzionalità per le verifiche primarie ai valichi di frontiera e per i controlli di polizia all'interno dei loro territori. Nello stesso intento di rafforzare l'uso del sistema d'informazione Schengen, la Commissione presenta, insieme alla presente relazione, una nuova versione del catalogo di raccomandazioni e migliori pratiche basata sulle valutazioni Schengen effettuate nel 2016 e 2017.

Proseguono inoltre nell'ambito del trilogo i negoziati sulle proposte volte a facilitare lo scambio di informazioni sui casellari giudiziali di cittadini di paesi terzi nell'UE tramite il **sistema europeo di informazione sui casellari giudiziali** e a rafforzare l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (**eu-LISA**).

---

22 Cfr. la dodicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 779 final del 12.12.2017.

23 I regolamenti proposti sul sistema europeo di informazione e autorizzazione ai viaggi, sul sistema europeo di informazione sui casellari giudiziali per cittadini di paesi terzi, su Eurodac, sul sistema d'informazione Schengen e su eu-LISA.

24 Austria, Germania, Lettonia, Liechtenstein, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Slovenia e Svizzera.

Nell'ambito delle iniziative dirette a rafforzare gli attuali sistemi d'informazione e la loro interoperabilità, la Commissione presenterà nella primavera 2018, sulla base di studi tecnici e di una valutazione d'impatto, una proposta di revisione del **sistema d'informazione visti** (VIS) il cui scopo è contribuire ad accrescere la sicurezza alle frontiere esterne e all'interno dello spazio Schengen. La prossima revisione del quadro giuridico del VIS comprenderà specifiche misure di interoperabilità per rendere più efficace il trattamento delle domande di visto; si prevede inoltre di affrontare altre questioni individuate nell'ambito della valutazione del VIS condotta nel 2016[25].

La piena attuazione della direttiva sul **codice di prenotazione** (PNR)[26] è un fattore essenziale degli sforzi compiuti parallelamente per usare al massimo i sistemi d'informazione esistenti, dato che questo strumento svolge un ruolo fondamentale nella risposta comune dell'UE alla minaccia del terrorismo e delle forme gravi di criminalità transnazionale. Perché la direttiva sia pienamente efficace a livello dell'UE, è fondamentale che sia completamente attuata da tutti gli Stati membri entro il termine previsto del 25 maggio 2018. In occasione del Consiglio Giustizia e affari interni dell'8 marzo 2018, gli Stati membri che non hanno ancora attuato la direttiva hanno dichiarato che si stavano impegnando al massimo per rispettare tale scadenza. Al 17 aprile 2018, cinque Stati membri[27] sono ancora in una fase relativamente precoce del processo di attuazione. La Commissione esorta ancora una volta tali Stati membri a procedere rapidamente nel processo di attuazione e a prendere tutte le iniziative possibili per far sì che le rispettive unità d'informazione sui passeggeri e le soluzioni tecniche per il PNR siano operative entro le prossime cinque settimane, per rispettare il termine del 25 maggio 2018.

La Commissione continua a incoraggiare e sostenere tutti e cinque gli Stati membri nel loro impegno per l'attuazione della direttiva, organizzando fra l'altro appositi incontri a livello politico e tecnico. L'ottava riunione sull'attuazione della direttiva PNR, avvenuta il 12 aprile 2018, ha offerto agli Stati membri e alla Commissione un'ulteriore opportunità per affrontare i rimanenti problemi di attuazione, nonché per cominciare a esaminare questioni relative all'applicazione della direttiva.

3. Protezione dai rischi chimici, biologici, radiologici e nucleari e protezione degli spazi pubblici

L'attentato chimico di Salisbury è stato uno sconvolgente promemoria della potenziale minaccia per la sicurezza rappresentata dalle **sostanze chimiche, biologiche, radiologiche e nucleari (CBRN)**. Come richiesto dal Consiglio europeo del 22-23 marzo 2018, l'UE deve rafforzare la sua resilienza nei confronti dei rischi CBRN, in linea con il piano d'azione presentato nell'ottobre 2017[28]. Il piano d'azione presenta una serie di misure destinate a ridurre l'accessibilità dei materiali CBRN, a eliminare le lacune nelle capacità di individuare tali materiali e a rafforzare la preparazione e la risposta agli incidenti di tipo CBRN. Le misure intendono inoltre promuovere la cooperazione contro queste minacce all'interno dell'UE e con i principali partner internazionali, compresa la NATO, mediante scambi d'informazioni, azioni congiunte di rafforzamento delle capacità, formazioni ed esercitazioni; si prevede fra l'altro la cooperazione con il centro di eccellenza CBRN accreditato presso la NATO nella Repubblica ceca. Sarà istituita una rete dell'UE per la sicurezza CBRN che riunirà tutti gli operatori CBRN a livello sia strategico che operativo, alla quale parteciperanno gli Stati

[25] Comunicazione della Commissione al Parlamento europeo e al Consiglio: Adattare la politica comune in materia di visti alle nuove sfide (COM (2018) 251 final del 14.3.2018).
[26] Direttiva (UE) 2016/681 del 27 aprile 2016.
[27] Croazia, Cipro, Repubblica ceca, Grecia e Italia.
[28] COM(2017) 610 final del 18.10.2017.

membri, le istituzioni dell'UE e le agenzie competenti e, se del caso, i principali partner internazionali e il settore privato. Cinque Stati membri devono ancora nominare i loro coordinatori della sicurezza CBRN e dovrebbero farlo al più presto. Come richiesto dal Consiglio europeo, la Commissione e l'Alto rappresentante riferiranno sui progressi compiuti nell'attuazione del piano d'azione CBRN e nel potenziamento delle capacità di affrontare minacce ibride, in previsione del Consiglio europeo del giugno 2018.

Nel quadro dell'attuazione del piano d'azione per migliorare la **protezione degli spazi pubblici**[29], specialmente dagli attentati terroristici, l'8 marzo 2018 la Commissione e il Comitato europeo delle regioni hanno organizzato insieme il convegno dei sindaci dell'UE sul tema "Creare delle difese urbane contro il terrorismo: gli insegnamenti tratti dai recenti attacchi"; dei quasi 200 partecipanti, alcuni rappresentavano città recentemente colpite da attentati terroristici. Il convegno ha esaminato le lezioni tratte dai recenti attentati, concentrandosi sulla condivisione delle esperienze e delle buone pratiche. Ha permesso di individuare soluzioni volte a potenziare la protezione fisica degli spazi pubblici, pur mantenendo le città e gli spazi pubblici aperti e invitanti, attuando fra l'altro il concetto di "sicurezza fin dalla progettazione". Per sostenere l'attuazione di tali soluzioni l'UE mette a disposizione finanziamenti a titolo del Fondo sicurezza interna. La Commissione sta attualmente valutando 35 proposte di progetto ricevute in seguito a un bando. Nel corso di quest'anno, la sicurezza figurerà inoltre come una delle priorità di un bando a titolo delle azioni innovative urbane, con un bilancio complessivo di 100 milioni di EUR del Fondo europeo di sviluppo regionale. La ricerca sulla sicurezza contribuisce anch'essa all'impegno generale per accrescere la protezione degli spazi pubblici. Nel 2019 sarà presentato un tema di ricerca specifico sulla "Sicurezza per città intelligenti e sicure, anche negli spazi pubblici", con una dotazione di 16 milioni di EUR.

4. Cibersicurezza

Combattere la criminalità informatica e rafforzare la cibersicurezza rimane una priorità di azione per l'UE. Per creare sinergie, potenziare le competenze e la ricerca e proporre soluzioni commercializzabili in grado di migliorare la cibersicurezza del mercato unico digitale, la Commissione ha lanciato il 1° febbraio 2018 un invito a presentare proposte per un **progetto pilota per sostenere la creazione di una rete di centri di competenza sulla cibersicurezza in tutta l'UE**, del valore di 50 milioni di EUR. La rete permetterà di mettere in comune le ricerche sulla cibersicurezza svolte in tutta l'Unione europea (ad esempio nei laboratori universitari e in centri di ricerca pubblici o privati senza scopo di lucro). Il progetto pilota è stato annunciato nella comunicazione congiunta sulla cibersicurezza[30] adottata nel settembre 2017 e sarà finanziato grazie al programma quadro Orizzonte 2020 secondo il programma di lavoro modificato per il periodo 2018-2020. La scadenza dell'invito a presentare proposte è il 29 maggio 2018[31].

Il recente uso di mezzi informatici per manipolare i comportamenti, aggravare le divisioni della società e sovvertire i sistemi e le istituzioni democratici ha messo ulteriormente in rilievo l'esigenza di mantenere strumenti che consentano di attribuire la responsabilità delle azioni online. La comunicazione congiunta del 2017 ha sottolineato anche questo aspetto, dichiarando che occorre migliorare **la disponibilità e l'accuratezza delle informazioni nella**

---

29 Piano d'azione per migliorare la protezione degli spazi pubblici (COM(2017) 612 final del 18.10.2017).

30 JOIN(2017) 450 final del 13.9.2017.

31 Ulteriori informazioni sono disponibili sul seguente sito: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-03-2018.html.

banca dati "WHOIS" di registrazione dei nomi di dominio, una risorsa importante per le indagini sulla criminalità informatica e la cibersicurezza. È in corso una collaborazione con l'ICANN per rendere tale banca dati conforme alle norme in materia di protezione dei dati, in particolare al regolamento generale sulla protezione dei dati; la Commissione ha inviato all'ICANN una lettera[32] in cui si enunciano gli obiettivi paralleli di ottenere un rapido accesso ai suoi elenchi a fini di interesse pubblico e di rispettare pienamente le norme dell'UE sulla protezione dei dati. Il comitato governativo consultivo dell'ICANN, che riunisce rappresentanti dei governi nazionali e della Commissione, ha espresso le sue preoccupazioni e ha invitato l'ICANN a garantire un accesso continuativo a WHOIS, compresi i dati non pubblici, per gli utenti con fini legittimi.

Nel gennaio 2018 la Commissione europea ha costituito un gruppo indipendente di esperti ad alto livello che fornisce consulenza sulle opzioni strategiche per contrastare le false notizie e la **disinformazione** diffuse online e per contribuire a sviluppare una strategia generale dell'UE al riguardo. Il 12 marzo 2018 il gruppo ha pubblicato la sua relazione su "Un approccio multidimensionale alla disinformazione", che offre contributi per la comunicazione della Commissione in materia, la cui adozione è prevista per questa primavera.

Il 16 aprile 2018 **il Consiglio Affari esteri ha adottato le conclusioni del Consiglio sulle attività informatiche dolose**, che costituiscono l'attuazione pratica della risposta diplomatica comune dell'UE alle attività informatiche dolose (il "pacchetto di strumenti della diplomazia informatica")[33] rispetto a specifiche attività dolose quali gli attacchi informatici *Wannacry* e *NotPetya*. Le conclusioni del Consiglio Affari esteri evidenziano l'importanza di mantenere il ciberspazio aperto, libero, stabile e sicuro e sottolineano che l'applicazione del diritto internazionale vigente e l'adesione a norme volontarie e non vincolanti per un comportamento responsabile da parte degli Stati sono essenziali per mantenere la pace e la stabilità.

5. Dimensione esterna

Per promuovere la raccolta e la condivisione di informazioni ai fini della lotta contro il traffico di migranti, la tratta di esseri umani, il traffico di armi da fuoco e il traffico delle esportazioni di petrolio dalla Libia, il Consiglio Giustizia e affari interni dell'8-9 marzo 2018 ha appoggiato il principio generale della partecipazione di Europol e dell'Agenzia europea della guardia di frontiera e costiera a un progetto pilota per una "**cellula sulle informazioni sui reati**" da istituire nell'ambito dell'operazione navale Sophia della politica di sicurezza e di difesa comune (EUNAVOR MED). Tale cellula faciliterà uno scambio di informazioni tempestivo e bilaterale a uso analitico e operativo tra l'operazione Sophia e le agenzie competenti del settore Giustizia e affari interni. Si tratta della prima iniziativa di questo tipo concordata tra le agenzie del settore Giustizia e affari interni e le missioni od operazioni della politica di sicurezza e difesa comune. Attualmente si stanno discutendo le modalità pratiche in seno al Consiglio, allo scopo di avviare il progetto pilota prima possibile. Una volta lanciato, il progetto sarà costantemente valutato: dopo sei mesi sarà presentata agli Stati membri una relazione completa per valutare il valore aggiunto e il rendimento della cellula sulle informazioni sui reati e gli aspetti giuridici e operativi, prima che sia presa una decisione sull'opportunità di proseguirla o replicarla in altre missioni od operazioni della politica di sicurezza e di difesa comune.

---

[32] https://www.icann.org/resources/correspondence/1212685-2018-01-29-en

[33] Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica"), 19 giugno 2017.

La sicurezza nei **Balcani occidentali** incide direttamente sulla sicurezza dell'UE e dei suoi Stati membri. Il 6 febbraio 2018 la Commissione ha adottato la comunicazione "Una prospettiva di allargamento credibile e un maggior impegno dell'UE per i Balcani occidentali"[34]. Il piano d'azione a sostegno della trasformazione dei Balcani occidentali allegato alla comunicazione presenta sei azioni tematiche principali, di cui una in materia di sicurezza e migrazione, da completare entro il 2020. Sono iniziati i lavori per attuare una serie di azioni volte a rafforzare la cooperazione con i Balcani occidentali per lottare contro il terrorismo, prevenire l'estremismo violento e contrastare la criminalità organizzata, in particolare tramite l'invio di ufficiali di collegamento di Europol nella regione[35] e apposite riunioni di esperti con la partecipazione dei Balcani occidentali, quali la riunione degli esperti europei di armi da fuoco tenutasi a Sofia il 12-13 aprile 2018 e il dialogo UE sulla droga svoltosi a Bruxelles il 18 aprile 2018. Il prossimo vertice di Sofia, del 17 maggio 2018, offrirà un'altra opportunità di fare il punto sui progressi conseguiti a questo riguardo.

IV. CONCLUSIONI

A sei mesi dall'adozione, nell'ottobre 2017, di una serie di misure pratiche per difendere meglio i cittadini dell'UE dalle minacce terroristiche, la Commissione presenta, insieme alla presente relazione, un ulteriore insieme di misure destinate a ridurre il margine di manovra dei terroristi e dei criminali e a favorire le indagini e il perseguimento dei reati e degli attentati terroristici. La Commissione invita il Parlamento europeo e il Consiglio a esaminare con urgenza queste iniziative per rafforzare la sicurezza dei cittadini.

Realizzare un'Europa che protegge rimane una priorità politica per l'Unione; la Commissione continuerà ad adoperarsi per realizzare un'autentica ed efficace Unione della sicurezza, anche in vista della riunione informale dei capi di Stato o di governo sulla sicurezza interna, annunciata nell'agenda dei leader per il settembre 2018 a Vienna. La Commissione presenterà la prossima relazione sull'Unione della sicurezza nel giugno 2018.

[34] Comunicazione della Commissione: Una prospettiva di allargamento credibile e un maggior impegno dell'UE per i Balcani occidentali (COM(2018) 65 final).

[35] Entro l'estate 2018 tre ufficiali di collegamento di Europol saranno inviati in Albania, in Bosnia-Erzegovina e in Serbia.