Consiglio
dell'Unione europea

Bruxelles, 31 ottobre 2019
(OR. en)

13682/19

JAI 1139
COSI 220
FRONT 299
ASIM 131
DAPIX 321
ENFOPOL 471
SIRIS 161
VISA 231
FAUXDOC 72
COPEN 417
CYBER 295
DATAPROTECT 265
CT 113
JAIEX 161
EF 319

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	31 ottobre 2019
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2019) 552 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO Ventesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza

Si trasmette in allegato, per le delegazioni, il documento COM(2019) 552 final.

All.: COM(2019) 552 final

COMMISSIONE
EUROPEA

Bruxelles, 30.10.2019
COM(2019) 552 final

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

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

I. INTRODUZIONE

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

Per la Commissione Juncker la sicurezza è stata una priorità assoluta fin dal primo giorno. Sulla scorta dell'Agenda europea sulla sicurezza di aprile 2015[1] e della comunicazione di aprile 2016 che prepara il terreno per l'Unione della sicurezza[2], l'UE ha risposto con un approccio coordinato a una serie di attacchi terroristici e ad altre sfide crescenti in materia di sicurezza, compiendo significativi progressi nel miglioramento della nostra sicurezza collettiva[3]. È diventato sempre più chiaro che le attuali sfide in materia di sicurezza sono minacce comuni, che si tratti di terrorismo, criminalità organizzata, attacchi informatici, disinformazione o altre minacce in evoluzione basate sull'uso degli strumenti informatici. Solo operando insieme possiamo conseguire il livello di sicurezza collettiva che i cittadini giustamente richiedono e si aspettano. Tale idea condivisa ha costituito il fondamento dei progressi compiuti verso un'autentica ed efficace Unione della sicurezza. Sulla spinta delle esigenze delle autorità nazionali che operano per garantire la sicurezza dei cittadini, il sostegno a livello dell'UE si è concentrato su misure legislative e operative nell'ambito delle quali un'azione congiunta può avere un impatto sulla sicurezza degli Stati membri. Questo lavoro è stato portato avanti a stretto contatto con il Parlamento europeo e il Consiglio e in modo pienamente trasparente nei confronti del grande pubblico. Il pieno rispetto dei diritti fondamentali è stato al centro di questo lavoro, poiché è possibile garantire la sicurezza dell'Unione solo se i cittadini sono sicuri che i propri diritti sono pienamente rispettati.

L'UE ha operato per la **lotta contro il terrorismo** riducendo il margine di manovra dei terroristi, introducendo nuove norme che rendono più difficile il loro accesso a esplosivi, armi da fuoco e finanziamenti e ne limitano gli spostamenti. L'UE ha migliorato **lo scambio di informazioni** per fornire a coloro che lavorano in prima linea, funzionari di polizia e guardie di frontiera, un accesso efficiente a dati accurati e completi, sfruttando al meglio le informazioni disponibili ed eliminando le lacune e le zone d'ombra. Una solida protezione delle frontiere esterne è una condizione essenziale per la sicurezza nello spazio di libera circolazione senza controlli alle frontiere interne. A marzo 2019 il Parlamento europeo e il Consiglio hanno raggiunto un accordo per una **guardia di frontiera e costiera europea** rafforzata e pienamente attrezzata e l'entrata in vigore del nuovo regolamento è prevista per l'inizio di dicembre 2019. L'UE ha predisposto una piattaforma e finanziamenti destinati agli operatori delle comunità locali per lo scambio delle migliori prassi in materia di **contrasto della radicalizzazione e prevenzione dell'estremismo violento** e ha inoltre proposto nuove norme per una rimozione efficace dei contenuti terroristici online. Il sostegno dell'UE ha contribuito a **incrementare la resilienza delle città** agli attacchi, con piani d'azione volti a sostenere la protezione degli spazi pubblici e a migliorare il livello di preparazione contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare. L'UE ha affrontato **le minacce per la cibersicurezza e le minacce basate sull'uso degli strumenti informatici**

---

1 COM(2015) 185 final del 28.4.2015.
2 COM(2016) 230 final del 20.4.2016.
3 Per le precedenti relazioni sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza si rimanda all'indirizzo seguente: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

elaborando una nuova strategia per la cibersicurezza e adottando atti legislativi in materia, nonché contrastando la **disinformazione** allo scopo di proteggere meglio le nostre elezioni. Si continua a lavorare per potenziare la sicurezza delle nostre **infrastrutture digitali critiche**, anche intensificando la cooperazione in materia di **cibersicurezza delle reti 5G** in tutta Europa.

Resta tuttavia ancora molto da fare. L'attacco a una sinagoga e l'uccisione di due cittadini a Halle, in Germania, il 9 ottobre 2019, trasmessi in diretta streaming, sono stati un monito terribile della minaccia rappresentata dall'estremismo violento di destra e dall'antisemitismo. L'attacco ha inoltre messo in luce ancora una volta l'uso di Internet per la propaganda del terrorismo e la conseguente **necessità di norme a livello dell'UE per la cancellazione dei contenuti terroristici online**. Il 7 e l'8 ottobre 2019 il Consiglio "Giustizia e affari interni" ha discusso il tema dell'estremismo violento di destra e del terrorismo, sottolineando la necessità di lavorare ulteriormente anche per contrastare la diffusione online e offline dei contenuti illeciti dell'estremismo violento di destra. Allo stesso tempo l'uccisione di tre funzionari di polizia e un altro membro del personale all'interno di un ufficio di polizia di Parigi il 3 ottobre 2019 mostra che la minaccia rappresentata dal terrorismo di ispirazione jihadista è ancora reale e che gli attuali sforzi per sostenere gli Stati membri nel contrasto di tale minaccia devono essere portati avanti. La fuga di prigionieri affiliati all'ISIS/Da'esh nell'ambito dei recenti eventi verificatisi nella Siria settentrionale potrebbe avere gravi ripercussioni sulla sicurezza in Europa. È importante che gli Stati membri sfruttino appieno i sistemi di informazione esistenti per rilevare e individuare i combattenti terroristi stranieri nel momento in cui attraversano le frontiere esterne. Sono inoltre in corso lavori sull'uso delle informazioni ottenute sul campo di battaglia per le azioni penali contro i combattenti terroristi stranieri.

La presente relazione delinea i progressi recentemente compiuti nell'ambito dei lavori per un'autentica ed efficace Unione della sicurezza, sottolineando i settori in cui sono necessarie ulteriori azioni. Essa fornisce aggiornamenti sull'attuazione delle misure concordate in materia di **cibersicurezza delle reti 5G**, in particolare sulla **relazione dell'UE sulla valutazione dei rischi** pubblicata il 9 ottobre 2019, e di **lotta contro la disinformazione**.

La presente relazione si concentra in particolare sulla **dimensione esterna** della cooperazione nell'ambito dell'Unione della sicurezza, che ha visto la firma di due **accordi bilaterali in materia di lotta contro il terrorismo** con l'Albania e la Repubblica di Macedonia del Nord e progressi nella cooperazione con i paesi terzi per quanto riguarda lo scambio dei **dati del codice di prenotazione**. Insieme alla presente relazione la Commissione ha inoltre adottato una richiesta di autorizzazione all'avvio di negoziati per un accordo tra l'UE e la **Nuova Zelanda** sullo scambio di dati personali per la lotta contro le forme gravi di criminalità e il terrorismo.

II. ATTUAZIONE DELLE PRIORITÀ LEGISLATIVE

1. Prevenire la radicalizzazione online e nelle comunità

La **prevenzione della radicalizzazione** è una pietra angolare della risposta dell'Unione alle minacce del terrorismo. In tal senso Internet costituisce il principale campo di battaglia delle azioni dei terroristi nel XXI secolo. Gli spazi in cui i soggetti radicalizzati possono comunicare e condividere contenuti permettono lo sviluppo e l'espansione di reti dell'estremismo violento di matrice jihadista e di destra in tutto il mondo. Per questo motivo la Commissione porta avanti il proprio duplice approccio al problema della radicalizzazione

online, secondo cui le norme proposte sulla rimozione dei contenuti terroristici illeciti online dovrebbero rafforzare il partenariato volontario con le piattaforme online.

Essenziale in tal senso è la **proposta legislativa per la prevenzione della diffusione di contenuti terroristici online**, che prevede norme e tutele chiare che imporrebbero alle piattaforme Internet l'obbligo di rimuovere i contenuti terroristici entro un'ora dal ricevimento di una richiesta motivata delle autorità competenti, nonché di adottare misure proattive proporzionate al livello di esposizione a contenuti terroristici[4]. I negoziati interistituzionali tra il Parlamento europeo e il Consiglio sono in corso e il primo trilogo si è tenuto il 17 ottobre 2019. Data la minaccia rappresentata dai contenuti terroristici online, la Commissione invita i colegislatori a raggiungere un accordo sulla proposta legislativa entro la fine del 2019.

La proposta legislativa è complementare al partenariato volontario con le imprese del settore di Internet e altri portatori di interessi nell'ambito del **Forum dell'UE su Internet**. Dalla sua creazione nel 2015 il Forum ha agito da catalizzatore di un'azione proattiva delle imprese di Internet finalizzata all'individuazione e alla rimozione dei contenuti terroristici online, spianando la strada per l'iniziativa, guidata dal settore, della "banca dati di hash"[5] condivisa e la creazione del Forum Internet mondiale per la lotta contro il terrorismo. L'unità UE addetta alle segnalazioni su Internet, che fa parte dell'agenzia di contrasto dell'UE Europol, è stata determinante per rafforzare la cooperazione con le imprese di Internet e contribuire agli obiettivi generali del Forum dell'UE su Internet. All'ultima riunione ministeriale del Forum dell'UE su Internet, tenutasi il 7 ottobre 2019, gli Stati membri dell'UE e i rappresentanti ad alto livello delle imprese di Internet si sono impegnati a collaborare nel quadro del cosiddetto **protocollo di crisi dell'UE**, che definisce le soglie per il potenziamento della cooperazione e stabilisce nuovi modi per migliorare la risposta alle crisi. L'azione fa parte degli sforzi compiuti a livello internazionale per attuare l'"appello di Christchurch"[6], che mira a garantire una reazione coordinata e rapida volta a contenere la diffusione online dei contenuti virali legati al terrorismo o all'estremismo violento.

Oltre a tali misure contro la radicalizzazione online, la Commissione continua a sostenere gli sforzi a livello nazionale e locale per la **prevenzione e la lotta contro la radicalizzazione sul campo**. Sulla scorta dell'ampio bagaglio di esperienze e competenze raccolte in seno alla rete di sensibilizzazione al problema della radicalizzazione, l'UE offre sostegno mirato agli attori locali, incluse le città[7], e fornisce opportunità di scambio tra operatori del settore, ricercatori e decisori politici. Per esempio la rete ha pubblicato orientamenti specifici e ha organizzato workshop per sostenere le autorità competenti nella gestione dei minori provenienti da aree di conflitto[8]. Per garantire la prosecuzione delle attività realizzate nel quadro della rete di sensibilizzazione al problema della radicalizzazione, la Commissione ha avviato le procedure

---

4 COM(2018) 640 final del 12.9.2018.

5 Si tratta di uno strumento istituito da un consorzio di imprese per agevolare la cooperazione in modo da prevenire la diffusione di contenuti terroristici da una piattaforma all'altra.

6 In risposta agli attacchi avvenuti a Christchurch, Nuova Zelanda, il 15 marzo 2019, il presidente francese Emmanuel Macron e il primo ministro neozelandese Jacinda Ardern hanno invitato i capi di Stato e di governo e le piattaforme online a Parigi il 15 maggio 2019 per lanciare l'"appello di Christchurch". Il presidente Juncker ha appoggiato l'appello e ha annunciato lo sviluppo di un protocollo di crisi dell'UE.

7 Per quanto riguarda la cooperazione con le città in materia di sicurezza cfr. anche la sezione V.2 sul tema della preparazione e della protezione, e in particolare della protezione degli spazi pubblici.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf.

per istituire un nuovo contratto quadro del valore stimato di 61 milioni di EUR e di durata quadriennale a partire dal 2020[9].

Al fine di contrastare la minaccia rappresentata dai contenuti terroristici online, la Commissione invita il Parlamento europeo e il Consiglio:

- a concludere i negoziati sulla proposta legislativa relativa alla prevenzione della diffusione di **contenuti terroristici online** entro la fine dell'anno.

2. Sistemi di informazione più solidi e intelligenti per la gestione della sicurezza, delle frontiere e della migrazione.

L'UE ha migliorato lo scambio di informazioni, agevolando il contrasto delle frodi connesse all'identità[10], rafforzando le verifiche di frontiera[11], modernizzando le banche dati delle autorità di contrasto a livello europeo[12], colmando le lacune informative[13] e potenziando l'agenzia di contrasto dell'UE Europol[14]. Determinante in tal senso è l'**interoperabilità dei sistemi di informazione dell'UE**[15], che permette di sfruttare al meglio le informazioni disponibili ed eliminare le zone d'ombra. Rispondendo alle esigenze di coloro che lavorano in prima linea, l'interoperabilità garantirà ai funzionari delle autorità di contrasto, alle guardie di frontiera e agli operatori dei servizi per l'immigrazione un accesso più rapido e sistematico

---

9 Il contratto quadro è suddiviso in due lotti: 29 milioni di EUR a sostegno delle attività della rete di sensibilizzazione al problema della radicalizzazione per i prossimi quattro anni e 32 milioni di EUR per potenziare la capacità degli Stati membri, delle autorità nazionali, regionali e locali e dei paesi terzi prioritari di contrastare efficacemente la radicalizzazione, in particolare attraverso la predisposizione di opportunità di rete, servizi mirati e orientati alle esigenze e attività di ricerca e analisi.

10 Regolamento (UE) 2019/1157 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione.

11 Introduzione di verifiche sistematiche alle frontiere esterne su tutti i cittadini mediante l'utilizzo del sistema d'informazione Schengen. Tutti gli Stati Schengen, nonché Romania, Bulgaria, Croazia e Cipro, applicano le norme introdotte ad aprile 2017 sulle verifiche sistematiche rispetto alle banche dati pertinenti alle frontiere esterne. In conformità di tali norme, alla luce dell'impatto sproporzionato sul flusso di traffico, sono ammesse deroghe temporanee alle frontiere terrestri o marittime, ma solo per quanto riguarda i cittadini dell'UE. Attualmente sono state notificate deroghe di questo tipo da sei Stati membri/paesi associati Schengen (Croazia, Finlandia, Ungheria, Lettonia, Norvegia e Slovenia). Per quanto riguarda le frontiere aeree, la possibilità di deroga alle norme sulle verifiche sistematiche è giunta a scadenza ad aprile 2019.

12 Il sistema d'informazione Schengen rafforzato (regolamento (UE) 2018/1860 del 28.11.2018, regolamento (UE) 2018/1861 del 28.11.2018 e regolamento (UE) 2018/1862 del 28.11.2018) e il sistema europeo di informazione sui casellari giudiziali esteso ai cittadini di paesi terzi (regolamento (UE) 2019/816 del 17.4.2019). Il rafforzamento del sistema d'informazione Schengen prevede l'obbligo generale di inserire nel sistema le segnalazioni legate al terrorismo.

13 Il sistema di ingressi/uscite dell'UE (regolamento (UE) 2017/2226 del 30.11.2017) e il sistema europeo di informazione e autorizzazione ai viaggi (regolamento (UE) 2018/1240 del 12.9.2018 e regolamento (UE) 2018/1241 del 12.9.2018).

14 Negli ultimi anni il ruolo di Europol è stato notevolmente potenziato in termini sia di portata che di profondità. L'agenzia è stata rafforzata grazie all'adozione del regolamento Europol del 2016 (regolamento (UE) 2016/794 dell'11.5.2016). Gli Stati membri hanno incrementato notevolmente la quantità di informazioni condivise con e tramite Europol. L'istituzione del Centro europeo antiterrorismo di Europol (ECTC) ha potenziato le capacità analitiche di Europol nei casi di terrorismo. Negli ultimi anni il bilancio di Europol è notevolmente aumentato, passando da 82 milioni di EUR nel 2014 a 138 milioni di EUR nel 2019. Sono in corso i negoziati sul bilancio per il 2020.

15 Regolamento (UE) 2019/817 del 20.5.2019 e regolamento (UE) 2019/818 del 20.5.2019.

alle informazioni, contribuendo così a migliorare la sicurezza interna e la gestione delle frontiere.

L'interoperabilità e tutte le innovazioni ad essa correlate tuttavia faranno la differenza per la gestione della sicurezza, delle frontiere e della migrazione sul campo solo se ogni Stato membro attuerà integralmente la legislazione in materia. Per questo motivo l'**attuazione** dell'interoperabilità è una priorità assoluta dell'Unione della sicurezza, a livello sia politico che tecnico. La Commissione e l'Agenzia dell'UE per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) sostengono gli Stati membri per quanto riguarda le competenze e lo scambio di migliori prassi, utilizzando una rete di coordinatori nazionali e sviluppando una scheda di valutazione per consentire un monitoraggio efficace e accordi di coordinamento. La stretta cooperazione tra le agenzie dell'UE, tutti gli Stati membri e i paesi associati Schengen sarà fondamentale per conseguire l'obiettivo ambizioso di una piena interoperabilità dei sistemi di informazione dell'UE per la gestione della sicurezza, delle frontiere e dell'immigrazione entro il 2020.

Allo stesso tempo il Parlamento europeo e il Consiglio devono ancora **portare a termine i lavori legislativi** in questo settore. Per garantire un avvio completo e tempestivo dell'interoperabilità è essenziale raggiungere rapidamente un accordo su tutte le proposte legislative pendenti. In primo luogo, nel quadro dell'attuazione tecnica del **sistema europeo di informazione e autorizzazione ai viaggi**, è necessario apportare modifiche tecniche ai regolamenti in materia[16] al fine di consentire una predisposizione completa del sistema. La Commissione invita il Parlamento europeo ad accelerare i lavori su tali modifiche tecniche affinché i negoziati interistituzionali possano essere avviati il prima possibile. In secondo luogo sono ancora in corso i negoziati interistituzionali sulla proposta di maggio 2018 per il rafforzamento e il miglioramento dell'attuale **sistema di informazione visti**[17]. Sulla scorta del primo trilogo tenutosi il 22 ottobre 2019, la Commissione invita entrambi i colegislatori a concludere rapidamente i negoziati. In terzo luogo manca ancora un accordo sulla proposta della Commissione di maggio 2016, che prevede l'estensione dell'ambito di applicazione dell'**Eurodac**[18] in modo che permetta di conservare le impronte digitali e i dati pertinenti non solo dei richiedenti asilo e delle persone fermate in relazione all'attraversamento irregolare di una frontiera esterna, ma anche dei cittadini di paesi terzi il cui soggiorno è irregolare. Le modifiche proposte estenderebbero inoltre il periodo di conservazione delle impronte digitali e dei dati pertinenti di coloro che entrano nell'UE in modo irregolare. La Commissione invita i colegislatori a procedere all'adozione della proposta.

Al fine di rafforzare i sistemi di informazione dell'UE per la gestione della sicurezza, delle frontiere e della migrazione, la Commissione invita il Parlamento europeo e il Consiglio:

- a portare avanti i lavori in modo che sia possibile giungere rapidamente a un accordo sulle modifiche tecniche necessarie per l'istituzione del **sistema europeo di informazione e autorizzazione ai viaggi**,
- a condurre e concludere rapidamente i negoziati sulla proposta per il rafforzamento dell'attuale **sistema di informazione visti**,
- ad adottare la proposta legislativa sull'**Eurodac** *(priorità della dichiarazione comune)*.

16 Regolamento (UE) 2018/1240 del 12.9.2018 e regolamento (UE) 2018/1241 del 12.9.2018.
17 COM(2018) 302 final del 16.5.2018.
18 COM(2016) 272 final del 4.5.2016.

3. *Ridurre il margine di manovra dei terroristi*

L'UE ha intrapreso un'azione decisa volta a ridurre il margine di manovra dei terroristi, introducendo nuove norme che rendono più difficile il loro accesso a esplosivi[19], armi da fuoco[20] e finanziamenti e ne limitano gli spostamenti[21].

Per potenziare la risposta giudiziaria al terrorismo, il 1º settembre 2019 l'Agenzia dell'UE per la cooperazione giudiziaria penale (Eurojust) ha istituito un **registro giudiziario europeo antiterrorismo**. Il registro raccoglierà informazioni giudiziarie allo scopo di consentire collegamenti tra i procedimenti avviati contro i soggetti sospettati di reati terroristici, rafforzando così il coordinamento tra i pubblici ministeri nell'ambito delle indagini antiterroristiche con potenziali implicazioni transfrontaliere.

Sono tuttavia necessari ulteriori sforzi per sostenere e agevolare le indagini nei casi transfrontalieri, in particolare per quanto riguarda l'**accesso alle prove elettroniche** da parte delle autorità di contrasto. Per quanto riguarda le proposte legislative di aprile 2018 intese a migliorare l'accesso alle prove elettroniche nell'ambito delle indagini penali[22], il Parlamento europeo deve ancora adottare la propria posizione negoziale prima che i colegislatori possano avviare i negoziati. La Commissione esorta il Parlamento europeo a procedere sulla proposta legislativa, in modo da consentire ai colegislatori di lavorare nell'ottica di una rapida adozione. Sulla base della propria proposta riguardante norme interne all'UE, la Commissione sta partecipando inoltre a **negoziati internazionali** per il miglioramento dell'accesso transfrontaliero alle prove elettroniche. Il 25 settembre 2019 si è tenuto il primo ciclo di negoziati tra le autorità della Commissione e degli Stati Uniti per un **accordo UE-USA sull'accesso transfrontaliero alle prove elettroniche**. Il prossimo ciclo è previsto per il 6 novembre 2019. Nell'ambito dei negoziati in corso sul **secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica**, la Commissione ha partecipato per conto dell'Unione a tre sessioni negoziali tenutesi a luglio, settembre e ottobre 2019. Per quanto nel corso dei negoziati siano stati registrati buoni progressi, devono ancora essere affrontati diversi temi importanti di grande interesse per l'Unione europea, come quello delle garanzie in materia di protezione dei dati. I negoziati sul secondo protocollo addizionale proseguiranno a novembre 2019 e per tutto il 2020. Al fine di migliorare la cooperazione internazionale sulla condivisione delle prove elettroniche e garantire al contempo la compatibilità con il diritto dell'UE e con gli obblighi degli Stati membri previsti dallo stesso, tenendo conto anche dei suoi futuri sviluppi, è importante che i negoziati su entrambe le materie procedano rapidamente.

Tenendo conto delle attuali preoccupazioni in materia di riciclaggio di denaro, il 19 settembre 2019 il Parlamento europeo ha adottato una **risoluzione sullo stato di attuazione della legislazione antiriciclaggio dell'Unione**[23], che fa seguito al pacchetto di

---

19 Regolamento (UE) 2019/1148 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativo all'immissione sul mercato e all'uso di precursori di esplosivi. Il regolamento è entrato in vigore il 31 luglio 2019 e si applica a decorrere da 18 mesi dopo l'entrata in vigore.

20 Direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati.

21 Introduzione di verifiche sistematiche alle frontiere esterne su tutti i cittadini mediante l'utilizzo del sistema d'informazione Schengen.

22 COM(2018) 225 final del 17.4.2018 e COM(2018) 226 final del 17.4.2018.

23 https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_IT.html.

quattro relazioni sul contrasto del riciclaggio adottate dalla Commissione il 24 luglio 2019[24]. Il Parlamento europeo ha invitato gli Stati membri a garantire un'attuazione corretta e rapida delle direttive antiriciclaggio. Il Parlamento europeo ha inoltre invitato la Commissione a valutare se un regolamento antiriciclaggio sia più adatto di una direttiva, nonché a esaminare la necessità di un meccanismo di coordinamento e sostegno per le unità di informazione finanziaria.

Al fine di migliorare l'accesso alle prove elettroniche da parte delle autorità di contrasto, la Commissione invita il Parlamento europeo e il Consiglio:

- a raggiungere rapidamente un accordo sulle proposte legislative in materia di **prove elettroniche** *(priorità della dichiarazione comune)*.

4. Rafforzare la cibersicurezza

Il rafforzamento della cibersicurezza resta un aspetto essenziale dei lavori per un'autentica ed efficace Unione della sicurezza. Con l'attuazione della strategia dell'UE per la cibersicurezza del 2017[25] l'Unione ha potenziato la propria resilienza, rendendosi meno vulnerabile agli attacchi e in grado di riprendersi più rapidamente, nonché la propria azione deterrente, incrementando le probabilità che gli autori degli attacchi siano arrestati e puniti, anche mediante un quadro per una risposta diplomatica congiunta dell'UE alle attività informatiche dolose. L'Unione sostiene gli Stati membri anche per quanto riguarda la ciberdifesa, attuando il quadro strategico dell'UE in materia di ciberdifesa.[26]

Con l'entrata in vigore del regolamento sulla cibersicurezza[27] a giugno 2019, il **quadro di certificazione della cibersicurezza dell'UE** sta prendendo forma. La certificazione riveste un ruolo fondamentale nel rafforzare la sicurezza di prodotti e servizi che sono essenziali per il mercato unico digitale e nell'accrescere la fiducia negli stessi. Il quadro di certificazione introdurrà sistemi di certificazione a livello dell'UE, intesi come serie complete di regole, requisiti tecnici, norme e procedure. Il quadro coinvolge due gruppi di esperti, il gruppo europeo per la certificazione della cibersicurezza, in rappresentanza delle autorità degli Stati membri, e il gruppo dei portatori di interessi per la certificazione della cibersicurezza, in rappresentanza del settore. Quest'ultimo riunisce rappresentanti sul versante sia della domanda che dell'offerta di prodotti e servizi delle tecnologie dell'informazione e della comunicazione, fra cui le piccole e medie imprese, i fornitori di servizi digitali, gli organismi europei e internazionali di normazione, gli organismi nazionali di accreditamento, le autorità di controllo preposte alla protezione dei dati e gli organismi di valutazione della conformità.

Nel frattempo il Parlamento europeo e il Consiglio devono ancora raggiungere un accordo sull'iniziativa legislativa[28] riguardante il **Centro europeo di competenza industriale,**

---

[24] Relazione sulla valutazione dei rischi di riciclaggio e finanziamento del terrorismo che incidono sul mercato interno e sono connessi ad attività transfrontaliere (COM(2019) 370 final del 24.7.2019), relazione sulla valutazione del quadro per la cooperazione tra le unità di informazione finanziaria (COM(2019) 371 final del 24.7.2019), relazione sull'interconnessione dei meccanismi nazionali centralizzati automatici (registri centrali o sistemi elettronici centrali di reperimento dei dati) degli Stati membri relativi ai conti bancari (COM(2019) 372 final del 24.7.2019) e relazione sulla valutazione di recenti presunti casi di riciclaggio di denaro concernenti enti creditizi dell'UE (COM(2019) 373 final del 24.7.2019).

[25] JOIN(2017) 450 final del 13.9.2017.

[26] Quadro strategico dell'UE in materia di ciberdifesa (aggiornamento 2018) adottato dal Consiglio il 19 novembre 2018 (14413/18).

[27] Regolamento (UE) 2019/881 del 17.4.2019.

[28] COM(2018) 630 final del 12.9.2018.

tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento. La proposta mira a rafforzare la capacità di cibersicurezza dell'Unione incentivando l'ambiente tecnologico e industriale europeo che opera nel settore della cibersicurezza, nonché coordinando e aggregando le relative risorse. La Commissione invita entrambi i colegislatori a riprendere e a concludere rapidamente i negoziati interistituzionali su questa iniziativa prioritaria per rafforzare la cibersicurezza.

Il lavoro sul rafforzamento della cibersicurezza contempla un sostegno a livello nazionale e regionale[29].

Oltre alle minacce informatiche per i sistemi e i dati, l'UE continua ad affrontare le sfide complesse e variegate poste dalle **minacce ibride** All'interno del Consiglio è stato istituito un gruppo orizzontale sul contrasto delle minacce ibride allo scopo di migliorare la resilienza dell'UE e degli Stati membri a tali minacce e sostenere azioni atte a rafforzare la resilienza delle società alle crisi. La Commissione e il servizio europeo per l'azione esterna sostengono tali sforzi secondo quanto previsto dal quadro congiunto per contrastare le minacce ibride del 2016[30] e dalla comunicazione congiunta del 2018[31] riguardante il rafforzamento della resilienza e il potenziamento delle capacità di affrontare minacce ibride. Il Centro comune di ricerca sta inoltre elaborando un "modello concettuale" per la caratterizzazione delle minacce ibride, al fine di aiutare gli Stati membri e le relative autorità competenti a identificare i tipi di attacchi ibridi che potrebbero trovarsi ad affrontare. Il modello esamina il modo in cui un soggetto (statale o non statale) adopera una serie di strumenti (dalla disinformazione allo spionaggio, fino alle operazioni fisiche) in vari settori (economico, militare, sociale, politico) per colpire un bersaglio allo scopo di raggiungere una serie di obiettivi.

Al fine di rafforzare la cibersicurezza la Commissione invita il Parlamento europeo e il Consiglio a:

- raggiungere rapidamente un accordo sulla proposta legislativa riguardante il **Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento**.

[29] La Commissione sostiene ad esempio un partenariato interregionale per l'innovazione in materia di cibersicurezza che coinvolge Bretagna, Castiglia e León, Renania settentrionale-Vestfalia, Finlandia centrale ed Estonia, finalizzato allo sviluppo di una catena di valore europea della cibersicurezza incentrata sulla commercializzazione e sull'espansione.

[30] JOIN(2016) 18 final del 6.4.2016.

[31] JOIN(2018) 16 final del 13.6.2018.

III. RAFFORZARE LA SICUREZZA DELLE INFRASTRUTTURE DIGITALI

Le reti di quinta generazione (5G) costituiranno la futura colonna portante di economie e società sempre più digitalizzate. Sono interessati miliardi di oggetti e sistemi connessi, anche in ambiti critici quali l'energia, i trasporti, le banche e la salute, oltre a sistemi di controllo industriali che trasportano informazioni sensibili e fanno da supporto ai sistemi di sicurezza. È quindi essenziale garantire la sicurezza e la resilienza delle reti 5G.

Nel quadro di un approccio coordinato, il 9 ottobre 2019 gli Stati membri hanno pubblicato una relazione sulla **valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti 5G** con il sostegno della Commissione e dell'Agenzia dell'Unione europea per la cibersicurezza[32]. Si tratta di una tappa fondamentale nell'attuazione della raccomandazione della Commissione europea di marzo 2019 finalizzata a garantire un elevato livello di cibersicurezza delle reti 5G in tutta l'UE[33]. La relazione si basa sui risultati delle valutazioni nazionali dei rischi per la cibersicurezza effettuate da tutti gli Stati membri e individua le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo), nonché diversi rischi strategici. La valutazione costituisce il punto di partenza per individuare le misure di attenuazione che possono essere applicate a livello nazionale ed europeo.

La relazione individua diverse importanti **sfide per la cibersicurezza** che possono palesarsi o assumere maggior rilievo nell'ambito delle reti 5G. Tali sfide per la sicurezza sono soprattutto legate a *innovazioni* chiave nella tecnologia 5G, in particolare l'importanza del software e l'ampia gamma di servizi e applicazioni resi possibili dal 5G; nonché al ruolo dei *fornitori* nella realizzazione e nell'uso delle reti 5G e al grado di dipendenza da singoli fornitori. Ciò significa che prodotti, servizi e operazioni dei fornitori entrano sempre più a far parte della "superficie di attacco" delle reti 5G. Il profilo di rischio dei singoli fornitori, compresa la probabilità che il fornitore subisca interferenze da un paese non membro dell'UE, assumerà inoltre particolare importanza.

In linea con il processo definito nella raccomandazione della Commissione di marzo 2019, gli Stati membri dovrebbero concordare entro il 31 dicembre 2019 **una serie di misure di attenuazione** per far fronte ai rischi per la cibersicurezza individuati a livello nazionale e dell'Unione. La Commissione e il servizio europeo per l'azione esterna continueranno inoltre a confrontarsi sulla cibersicurezza e sulla resilienza delle reti 5G con partner che condividono la loro visione. In tal senso la Commissione è in contatto con la NATO in merito alla valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti 5G.

---

[32] La valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti 5G è stata completata dal gruppo di cooperazione delle autorità competenti istituito nel quadro della direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva (UE) 2016/1148 del 6.7.2016), con l'ausilio della Commissione e dell'Agenzia dell'Unione europea per la cibersicurezza: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019) 2335 final del 26.3.2019.

IV. LOTTA CONTRO LA DISINFORMAZIONE E PROTEZIONE DELLE ELEZIONI DA ALTRE MINACCE BASATE SULL'USO DI STRUMENTI INFORMATICI

L'UE ha istituito un **quadro per un'azione coordinata contro la disinformazione**, nel pieno rispetto dei valori e dei diritti fondamentali europei[34]. Nell'ambito del piano d'azione contro la disinformazione[35] continuano i lavori volti a ridurre lo spazio per la disinformazione, anche nell'ottica di proteggere l'integrità delle elezioni.

In tale contesto è fondamentale il lavoro svolto con il settore tramite il **codice di buone pratiche sulla disinformazione**, uno strumento di autoregolamentazione per le piattaforme online e il settore pubblicitario che è divenuto applicabile a ottobre 2018[36]. La Commissione ha valutato l'efficacia del codice dopo il primo anno di applicazione, sulla base delle relazioni annuali di autovalutazione presentate dalle piattaforme online e dagli altri firmatari del codice e pubblicate il 29 ottobre 2019 insieme a una dichiarazione della Commissione[37]. In linea generale le relazioni dimostrano gli ingenti sforzi messi in campo dai firmatari per attuare i propri impegni.

Le azioni adottate dalle piattaforme firmatarie differiscono in termini di rapidità e portata tra i cinque pilastri d'impegno previsti dal codice. In generale sono stati compiuti maggiori progressi per gli impegni legati alle elezioni europee del 2019, nello specifico per l'interruzione della pubblicità e degli incentivi monetari ai comportamenti in questione (pilastro 1), la garanzia della trasparenza per quanto riguarda i messaggi pubblicitari di natura politica e le campagne di sensibilizzazione (pilastro 2) e la garanzia dell'integrità dei servizi contro i profili e i comportamenti non autentici (pilastro 3). Si registrano invece progressi minori o scarsi per quanto riguarda gli impegni legati alla responsabilizzazione dei consumatori (pilastro 4) e alla responsabilizzazione della comunità dei ricercatori, anche mediante la predisposizione, da parte delle piattaforme, di un accesso agli insiemi di dati a fini di ricerca che sia pertinente e conforme ai principi di riservatezza (pilastro 5). Sono emerse inoltre differenze nella portata delle azioni intraprese da ciascuna piattaforma per assicurare l'attuazione dei propri impegni, nonché differenze tra gli Stati membri per quanto riguarda l'applicazione delle singole politiche. La Commissione continua a lavorare insieme ai firmatari del codice e agli altri portatori di interessi per intensificare l'azione intrapresa contro la disinformazione.

Nel quadro del piano d'azione contro la disinformazione la Commissione e l'Alto rappresentante, in collaborazione con gli Stati membri, hanno istituito un **sistema di allarme rapido** contro le campagne di disinformazione. Il sistema di allarme rapido ha permesso alle

---

34 Cfr. il piano d'azione contro la disinformazione (JOIN(2018) 36 final del 5.12.2018).

35 JOIN(2019) 12 final del 14.6.2019.

36 In conformità del codice le piattaforme online Google, Facebook, Twitter e Microsoft si sono impegnate a prevenire l'uso manipolativo dei propri servizi da parte dei soggetti malintenzionati, a garantire la trasparenza e la divulgazione al pubblico dei messaggi pubblicitari di natura politica, nonché ad adottare altre azioni volte a migliorare la trasparenza, la responsabilità e l'affidabilità dell'ecosistema online. Le associazioni di categoria del settore pubblicitario si sono impegnate inoltre a collaborare con le piattaforme per migliorare il vaglio delle inserzioni pubblicitarie e sviluppare strumenti di sicurezza dei marchi finalizzati a limitare le inserzioni pubblicitarie sui siti web che veicolano disinformazione.

37 https://ec.europa.eu/commission/presscorner/detail/it/statement_19_6166. Oltre a Google, Facebook, Twitter e Microsoft, tra i firmatari del codice rientrano Mozilla, sette associazioni a livello europeo o nazionale che rappresentano il settore pubblicitario, nonché EDiMA, un'associazione europea che rappresenta piattaforme e altre imprese tecnologiche attive nel settore online.

istituzioni e agli Stati membri dell'UE di condividere informazioni e analisi nel periodo precedente alle elezioni del Parlamento europeo del 2019 e di coordinare le risposte. Tale lavoro si è ulteriormente intensificato dopo le elezioni: sono in corso scambi quotidiani a livello operativo e sono state organizzate da diversi Stati membri tre riunioni dei punti di contatto del sistema di allarme rapido.

Un ulteriore passo avanti concreto per l'identificazione della disinformazione è stato fatto grazie al lavoro della **squadra di comunicazione strategica** ("StratComms"), e in particolare della sua task force di comunicazione strategica per l'Est, che gestisce il progetto "EUvsDisinfo" inteso a monitorare, analizzare e reagire alle attività di disinformazione a favore del Cremlino[38]. Dall'inizio del 2019 la prima dotazione finanziaria stanziata, pari a 3 milioni di EUR, ha consentito di intensificare ed espandere tale lavoro fino ad includere il monitoraggio e l'analisi della disinformazione a favore del Cremlino sui media online e radiotelevisivi e sui social network in 19 lingue, dall'inglese al serbo fino all'arabo. Grazie al miglioramento della capacità di monitoraggio il numero delle attività di disinformazione portate alla luce è più che raddoppiato, con circa 2 000 casi di disinformazione smascherati finora nel 2019, contro i 765 dello stesso periodo nel 2018. La task force di comunicazione strategica per l'Est ha rivestito un ruolo fondamentale nel monitoraggio e nello smascheramento della disinformazione a favore del Cremlino mirata alle elezioni del Parlamento europeo del 2019. La ricerca è stata affiancata da una campagna di sensibilizzazione sui tentativi di interferenze nei processi elettorali in tutto il mondo. Grazie alla sua divulgazione, realizzata in stretta collaborazione con il Parlamento europeo e la Commissione, sono state rilasciate più di 20 interviste sui media, mentre la campagna ha coinvolto oltre 300 giornalisti.

La Commissione ha anche intrapreso azioni volte a **ridurre la diffusione di disinformazione e miti sulle istituzioni e sulle politiche dell'UE**. Ha istituito una rete di esperti di comunicazione dotata di un portale online che offre materiale informativo interattivo sulle politiche dell'UE, sul problema della disinformazione e sul suo impatto sulla società. Ha inoltre lanciato varie campagne sui social media incentrate sulla lotta alla disinformazione[39], in collaborazione con il Parlamento europeo e il servizio europeo per l'azione esterna.

V. ATTUAZIONE DI ALTRI FASCICOLI PRIORITARI IN MATERIA DI SICUREZZA

1. Attuazione delle misure legislative nel quadro dell'Unione della sicurezza

Le misure concordate nel quadro dell'Unione della sicurezza produrranno appieno i vantaggi previsti per la sicurezza solo se saranno attuate rapidamente e integralmente da tutti gli Stati membri. A tal fine la Commissione sta sostenendo attivamente gli Stati membri nell'attuazione della legislazione dell'UE, anche mediante finanziamenti e attraverso l'agevolazione dello scambio di migliori prassi. La Commissione sfrutta appieno i poteri conferiteli dai trattati per garantire l'applicazione del diritto dell'UE, inclusi i procedimenti di infrazione laddove opportuno.

Il termine per il recepimento della **direttiva UE sul codice di prenotazione**[40] è scaduto

---

38 www.euvsdisinfo.eu.

39 https://europa.eu/euprotects/.

40 Direttiva (UE) 2016/681 del 27.4.2016. La Danimarca non ha partecipato all'adozione della direttiva e pertanto non è vincolata dalla stessa, né è tenuta ad applicarla.

il 25 maggio 2018. A oggi 25 Stati membri hanno notificato il pieno recepimento della direttiva[41]: un notevole passo avanti rispetto a luglio 2018, quando la Commissione aveva avviato procedure di infrazione contro 14 Stati membri[42]. Due Stati membri devono ancora notificare il pieno recepimento, nonostante siano in corso le procedure di infrazione avviate il 19 luglio 2018[43]. Parallelamente la Commissione continua a sostenere tutti gli Stati membri nei loro sforzi per completare lo sviluppo dei rispettivi sistemi di codici di prenotazione, anche agevolando lo scambio di informazioni e migliori prassi.

Il termine per il recepimento della direttiva sulla **lotta contro il terrorismo**[44] è scaduto l'8 settembre 2018. A oggi 22 Stati membri hanno notificato il pieno recepimento della direttiva: un notevole passo avanti rispetto a novembre 2018, quando la Commissione aveva avviato procedure di infrazione contro 16 Stati membri[45]. Tre Stati membri devono ancora notificare il pieno recepimento, nonostante le procedure di infrazione in corso[46]. Il 25 luglio 2019 la Commissione ha inviato pareri motivati a due Stati membri per la mancata notifica del pieno recepimento della direttiva[47]. Entrambi gli Stati membri hanno risposto annunciando che i lavori legislativi saranno completati entro la fine dell'anno.

Il termine per il recepimento della **direttiva relativa al controllo dell'acquisizione e della detenzione di armi**[48] è scaduto il 14 settembre 2018. A oggi 13 Stati membri hanno notificato il pieno recepimento e 15 Stati membri devono ancora notificare il pieno recepimento, nonostante siano in corso le procedure di infrazione avviate il 22 novembre 2018[49]. Il 25 luglio 2019 la Commissione ha inviato pareri motivati a 20 Stati membri per la mancata notifica del pieno recepimento della direttiva. Cinque Stati membri hanno risposto notificando il pieno recepimento della direttiva[50].

Il termine per il recepimento della **direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie**[51] è scaduto il 6 maggio 2018. A oggi 25 Stati membri hanno notificato il pieno recepimento della direttiva: un notevole passo avanti rispetto a luglio 2018, quando la Commissione aveva avviato procedure di infrazione contro 19 Stati membri[52]. Tre Stati membri devono ancora notificare il pieno recepimento, nonostante le procedure di infrazione

---

41 I riferimenti alla notifica di pieno recepimento tengono conto delle dichiarazioni degli Stati membri e non pregiudicano il controllo del recepimento da parte dei servizi della Commissione (situazione al 17.10.2019).

42 Cfr. la sedicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2018) 690 final del 10.10.2018).

43 La Slovenia ha notificato un recepimento parziale. La Spagna non ha notificato il recepimento (situazione al 17.10.2019).

44 Direttiva (UE) 2017/541 del 15.3.2017. La direttiva non si applica in Regno Unito, Irlanda e Danimarca.

45 Cfr. la diciassettesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2018) 845 final dell'11.12.2018).

46 Grecia e Lussemburgo non hanno notificato misure nazionali di attuazione. La Polonia ha notificato misure nazionali corrispondenti a un recepimento parziale (situazione al 17.10.2019).

47 Grecia e Lussemburgo.

48 Direttiva (UE) 2017/853 del 17.5.2017.

49 Belgio, Cechia, Estonia, Polonia, Svezia, Slovacchia e Regno Unito hanno notificato misure di recepimento per parte delle nuove disposizioni. Cipro, Germania, Grecia, Spagna, Lussemburgo, Ungheria, Romania e Slovenia non hanno notificato alcuna misura di recepimento (situazione al 17.10.2019).

50 Finlandia, Irlanda, Lituania, Paesi Bassi, Portogallo (situazione al 17.10.2019).

51 Direttiva (UE) 2016/680 del 27.4.2016.

52 Cfr. la sedicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2018) 690 final del 10.10.2018).

in corso[53]. Il 25 luglio 2019 la Commissione ha deciso di deferire due Stati membri[54] alla Corte di giustizia dell'Unione europea per il mancato recepimento della direttiva e ha inviato una lettera di costituzione in mora a uno Stato membro[55] per non aver recepito pienamente la direttiva[56].

La Commissione sta valutando il recepimento della **quarta direttiva antiriciclaggio**[57], verificando nel contempo che le norme siano attuate dagli Stati membri. Gli Stati membri dovevano recepire la direttiva nel diritto nazionale entro il 26 giugno 2018. La Commissione porta avanti le procedure di infrazione contro 21 Stati membri in quanto ha valutato che le comunicazioni trasmesse dagli stessi non indicano un recepimento completo della direttiva[58].

La Commissione ha valutato la conformità del recepimento delle **direttive in materia di criminalità informatica**. A luglio e a ottobre 2019 la Commissione ha avviato procedure di infrazione contro 23 Stati membri[59] in quanto ha valutato che la legislazione nazionale di attuazione notificata dagli stessi non rappresenta un corretto recepimento della **direttiva relativa alla lotta contro l'abuso sessuale dei minori**[60]. Analogamente a luglio e a ottobre 2019 la Commissione ha avviato procedure di infrazione contro quattro Stati membri[61] in quanto ha valutato che la legislazione nazionale di attuazione notificata dagli stessi non rappresenta un corretto recepimento della **direttiva relativa agli attacchi contro i sistemi di informazione**[62].

La Commissione invita gli Stati membri ad adottare urgentemente, nonché a comunicare alla Commissione, le misure necessarie a recepire pienamente nel diritto nazionale le direttive seguenti:

- la **direttiva UE sul codice di prenotazione**: uno Stato membro deve ancora notificare il recepimento nel diritto nazionale e uno Stato membro deve ancora completare la notifica del recepimento[63];
- la **direttiva sulla lotta contro il terrorismo**: due Stati membri devono ancora notificare il recepimento nel diritto nazionale e uno Stato membro deve ancora completare la notifica del recepimento[64];
- la **direttiva relativa al controllo dell'acquisizione e della detenzione di armi**: otto Stati membri devono ancora notificare il recepimento nel diritto nazionale e sette Stati membri devono ancora completare la notifica del recepimento[65];

---

53 La Slovenia ha notificato un recepimento parziale. La Spagna non ha notificato il recepimento. Nonostante la Germania abbia notificato un recepimento completo, la Commissione non lo ritiene tale (situazione al 17.10.2019).

54 Grecia e Spagna.

55 Germania.

56 La Grecia ha notificato il pieno recepimento e la Commissione lo sta attualmente valutando.

57 Direttiva (UE) 2015/849 del 20.5.2015.

58 Belgio, Bulgaria, Cechia, Danimarca, Germania, Estonia, Irlanda, Francia, Italia, Cipro, Lettonia, Lituania, Ungheria, Paesi Bassi, Austria, Polonia, Romania, Slovacchia, Finlandia, Svezia e Regno Unito (situazione al 17.10.2019). In precedenza erano state archiviate 7 procedure di infrazione relative alla direttiva.

59 Belgio, Bulgaria, Cechia, Germania, Estonia, Grecia, Spagna, Francia, Croazia, Italia, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia e Svezia.

60 Direttiva 2011/93/UE del 13.12.2011.

61 Bulgaria, Italia, Portogallo e Slovenia.

62 Direttiva 2013/40/UE del 12.8.2013.

63 La Slovenia ha notificato un recepimento parziale. La Spagna non ha notificato il recepimento (situazione al 17.10.2019).

64 Grecia e Lussemburgo non hanno notificato il recepimento. La Polonia ha notificato un recepimento parziale (situazione al 17.10.2019).

- la **direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie**: uno Stato membro deve ancora notificare il recepimento nel diritto nazionale e due Stati membri devono ancora completare la notifica del recepimento[66];
- la **quarta direttiva antiriciclaggio**: 21 Stati membri devono ancora completare la notifica del recepimento[67];
- la **direttiva relativa alla lotta contro l'abuso sessuale dei minori**: sono state avviate procedure di infrazione per recepimento non corretto contro 23 Stati membri[68];
- la **direttiva relativa agli attacchi contro i sistemi di informazione**: sono state avviate procedure di infrazione per recepimento non corretto contro quattro Stati membri[69].

2. Preparazione e protezione

Sviluppare la resilienza alle minacce per la sicurezza è una componente essenziale del lavoro verso un'autentica ed efficace Unione della sicurezza. La Commissione sostiene gli Stati membri e le autorità locali nel miglioramento della protezione degli spazi pubblici, attuando il piano d'azione dell'ottobre 2017 e il partenariato per la sicurezza negli spazi pubblici avviato a gennaio 2019 nel quadro dell'agenda urbana per l'UE. Tale lavoro coinvolge le città che si sono rivolte alla Commissione richiedendo sostegno per affrontare problemi nell'ambito della protezione degli spazi pubblici.

Lo scambio di migliori prassi tra le autorità locali e i gestori privati è essenziale per rafforzare la sicurezza degli spazi pubblici. Questo tema è stato al centro della **settimana europea della sicurezza**, tenutasi a Nizza, Francia, dal 14 al 18 ottobre 2019 e organizzata dal progetto finanziato dall'UE "Protect Allied Cities against Terrorism in Securing Urban Areas". L'evento, che ha riunito 500 partecipanti provenienti da città di tutta Europa, autorità nazionali e istituti di ricerca, ha sottolineato l'importanza di una stretta collaborazione tra tutti i portatori di interessi coinvolti, sia pubblici sia privati, nonché il ruolo delle nuove tecnologie per il miglioramento della protezione delle città. La protezione degli spazi pubblici è stata discussa anche durante la **settimana europea delle regioni e delle città** che si è tenuta a Bruxelles dal 7 al 10 ottobre 2019, con un seminario sull'agenda urbana del partenariato dell'UE per la sicurezza negli spazi pubblici. Il seminario si è concentrato sul ruolo delle autorità locali nella politica di sicurezza, sulla legislazione dell'UE e sui finanziamenti ai fini del contrasto delle principali sfide in materia di sicurezza negli spazi pubblici urbani, nonché su tematiche fondamentali come l'innovazione tramite soluzioni e tecnologie intelligenti, compresi i concetti di sicurezza fin dalla progettazione, prevenzione e inclusione sociale. La Commissione sta inoltre contribuendo a promuovere l'innovazione delle città in tali settori attraverso l'ultimo invito a presentare proposte per azioni innovative urbane, i cui risultati

---

65 Belgio, Cechia, Estonia, Polonia, Svezia, Slovacchia e Regno Unito hanno notificato misure di recepimento per parte delle nuove disposizioni. Cipro, Germania, Grecia, Spagna, Lussemburgo, Ungheria, Romania e Slovenia non hanno notificato alcuna misura di recepimento (situazione al 17.10.2019).

66 La Slovenia ha notificato un recepimento parziale. La Spagna non ha notificato il recepimento. Nonostante la Germania abbia notificato un recepimento completo, la Commissione non lo ritiene tale (situazione al 17.10.2019).

67 Belgio, Bulgaria, Cechia, Danimarca, Germania, Estonia, Irlanda, Francia, Italia, Cipro, Lettonia, Lituania, Ungheria, Paesi Bassi, Austria, Polonia, Romania, Slovacchia, Finlandia, Svezia e Regno Unito (situazione al 17.10.2019).

68 Belgio, Bulgaria, Cechia, Germania, Estonia, Grecia, Spagna, Francia, Croazia, Italia, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia e Svezia.

69 Bulgaria, Italia, Portogallo e Slovenia.

sono stati annunciati ad agosto 2019. Tra i progetti selezionati, tre città (Pireo in Grecia, Tampere in Finlandia e Torino in Italia) sperimenteranno nuove soluzioni relative a questioni di sicurezza pubblica[70].

Per **proteggere meglio i luoghi di culto** ed esaminare le esigenze dei diversi gruppi religiosi la Commissione ha organizzato per il 7 ottobre 2019 un incontro con i rappresentanti delle comunità ebraica, musulmana, cristiana e buddista. L'incontro, che si inserisce nel quadro dell'attuazione del piano d'azione dell'UE per migliorare la protezione degli spazi pubblici del 2017, ha mostrato come la consapevolezza e la preparazione in materia di sicurezza varino significativamente da una comunità religiosa all'altra e ha messo in luce l'importanza di un maggiore scambio di buone prassi. Dall'incontro è emerso inoltre che l'introduzione di misure di sicurezza di base e il miglioramento della consapevolezza in materia di sicurezza non sono incompatibili con il mantenimento della natura aperta e accessibile dei luoghi di culto. La Commissione raccoglierà buone prassi e materiale di sensibilizzazione sulla propria piattaforma elettronica destinata agli esperti e sottoporrà la questione all'attenzione delle autorità di sicurezza degli Stati membri nel contesto del forum pubblico-privato sulla protezione degli spazi pubblici.

Un tema specifico che richiede ulteriore attenzione è la crescente minaccia per la sicurezza delle infrastrutture critiche e degli spazi pubblici rappresentata dai **droni**. A integrazione della recente legislazione UE[71] sull'uso sicuro dei droni nello spazio aereo degli aeromobili con equipaggio, e senza pregiudicare le opportunità insite nell'uso benefico dei droni, la Commissione sostiene gli Stati membri nel monitoraggio delle tendenze relative all'uso dannoso dei droni, finanziando la ricerca in materia e agevolando la sperimentazione di contromisure. Lo scambio di esperienze e migliori prassi è essenziale, come dimostrato dalla conferenza internazionale ad alto livello sul contrasto delle minacce rappresentate dai sistemi di aeromobili senza equipaggio che si è tenuta a Bruxelles il 17 ottobre 2019. L'evento, organizzato dalla Commissione, ha riunito 250 partecipanti in rappresentanza degli Stati membri, delle organizzazioni internazionali, dei partner di paesi terzi, del settore, del mondo accademico e della società civile per discutere delle sfide in materia di sicurezza poste dai droni e di come affrontarle. Dall'incontro è emersa la necessità di valutazioni periodiche dei rischi legati ai droni, nonché di una stretta cooperazione tra il settore dell'aviazione e le autorità di contrasto per lo sviluppo ulteriore della legislazione dell'UE in materia di uso sicuro dei droni. È necessario inoltre testare ulteriormente le contromisure per i droni attraverso un approccio coordinato a livello europeo. Tutti hanno convenuto inoltre che affinché i droni siano sicuri, affidabili in termini di funzionamento e difficili da utilizzare impropriamente a fini dolosi, è essenziale una stretta collaborazione tra le autorità e il settore industriale.

3. Dimensione esterna

Poiché la maggior parte dei rischi che l'Unione si trova ad affrontare in materia di sicurezza travalicano i confini dell'UE e rappresentano minacce globali, la cooperazione con i paesi partner, le organizzazioni e i portatori di interessi in questo settore riveste un ruolo cruciale per la creazione di un'autentica ed efficace Unione della sicurezza.

---

70 Le azioni innovative urbane sono uno strumento cofinanziato dal Fondo europeo di sviluppo regionale. Per maggiori informazioni cfr.: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

71 Regolamento di esecuzione (EU) 2019/947 della Commissione, del 24 maggio 2019, relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio.

Lo scambio di informazioni è essenziale per tale cooperazione. Insieme alla presente relazione, la Commissione ha adottato una raccomandazione al Consiglio affinché autorizzi l'avvio dei negoziati per un **accordo tra l'UE e la Nuova Zelanda sullo scambio di dati personali per la lotta contro le forme gravi di criminalità e il terrorismo** tra Europol e le autorità competenti neozelandesi. Tale accordo rafforzerà ulteriormente la capacità di Europol di collaborare con la Nuova Zelanda per prevenire e contrastare i reati rientranti nell'ambito degli obiettivi di Europol. L'accordo operativo tra Europol e la polizia neozelandese siglato ad aprile 2019, per quanto fornisca un quadro per una cooperazione strutturata a livello strategico, non costituisce una base giuridica per lo scambio di dati personali. La possibilità di scambiare dati personali nel pieno rispetto della legislazione dell'UE e dei diritti fondamentali è essenziale per un'efficace collaborazione operativa delle forze di polizia. In precedenza la Commissione aveva individuato otto paesi prioritari della regione del Medio Oriente/Nord Africa con cui avviare negoziati, sulla base della minaccia rappresentata dal terrorismo, delle sfide legate alla migrazione e delle esigenze operative di Europol[72]. Alla luce delle esigenze operative delle autorità di contrasto di tutta l'UE e dei potenziali vantaggi di una più stretta cooperazione in questo settore, dimostrati anche dal seguito dato all'attacco di Christchurch di marzo 2019, la Commissione ritiene necessario aggiungere la Nuova Zelanda ai paesi prioritari con cui dovranno essere avviati negoziati nel breve termine.

Un'altra pietra angolare della cooperazione tra l'Unione e i paesi terzi in materia di sicurezza è il trasferimento dei **dati del codice di prenotazione**. Il 27 settembre 2019 la Commissione ha adottato una raccomandazione al Consiglio affinché autorizzi l'avvio di negoziati per la conclusione di un accordo **UE-Giappone** sul trasferimento dei dati del codice di prenotazione al fine di prevenire e combattere il terrorismo e i reati gravi di natura transnazionale nel pieno rispetto delle garanzie in materia di protezione dei dati e dei diritti fondamentali[73]. La raccomandazione è attualmente al vaglio del gruppo di lavoro del Consiglio e la Commissione invita il Consiglio ad adottare rapidamente un mandato per i negoziati con il Giappone. Disporre di accordi vigenti in tempo per le Olimpiadi 2020 sarebbe un vero valore aggiunto per la sicurezza.

A livello globale la Commissione sostiene il lavoro svolto dall'**Organizzazione per l'aviazione civile internazionale** per stabilire uno standard per il trattamento dei dati del codice di prenotazione. Tale lavoro risponde all'appello della risoluzione 2396 del Consiglio di sicurezza delle Nazioni Unite, che esorta tutti gli Stati membri delle Nazioni Unite a sviluppare la capacità di raccogliere, trattare e analizzare i dati del codice di prenotazione. Il 13 settembre 2019 la Commissione ha presentato una proposta[74] di decisione del Consiglio relativa alla posizione da adottare a nome dell'UE nell'ambito dell'Organizzazione per l'aviazione civile internazionale per quanto riguarda gli standard e le pratiche raccomandate sui dati del codice di prenotazione. La proposta è attualmente al vaglio del gruppo di lavoro del Consiglio e la Commissione invita ad adottare rapidamente la decisione del Consiglio. L'Unione e i suoi Stati membri hanno definito la propria posizione anche nel documento informativo "Norme e principi in materia di raccolta, uso, trattamento e protezione dei dati del codice di prenotazione (Passenger Name Record — PNR)", che è stato presentato alla 40ª sessione dell'assemblea dell'Organizzazione per l'aviazione civile internazionale.

---

72 Cfr. l'undicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2017) 608 final del 18.10.2017). I paesi prioritari sono Algeria, Egitto, Israele, Giordania, Libano, Marocco, Tunisia e Turchia.

73 COM(2019) 420 final del 27.9.2019.

74 COM(2019) 416 final del 13.9.2019.

Per quanto riguarda i lavori relativi al nuovo accordo sul codice di prenotazione con il **Canada**, la Commissione mira a concludere rapidamente l'accordo. Nel frattempo durante l'estate sono state avviate la revisione congiunta e la valutazione congiunta combinate dell'accordo sul codice di prenotazione con l'**Australia**, nonché la valutazione congiunta dell'accordo sul codice di prenotazione con gli **Stati Uniti**: le prime visite a Canberra e a Washington si sono svolte rispettivamente ad agosto e a settembre 2019. Il 14 ottobre 2019, nel corso di una sessione a porte chiuse, la Commissione ha informato la commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo sullo stato di avanzamento dei lavori con il Giappone, l'Australia e il Canada sui dati del codice di prenotazione.

Sono stati compiuti progressi anche nell'ambito della cooperazione in materia di sicurezza con i partner dei **Balcani occidentali**, con l'attuazione del piano d'azione comune per i Balcani occidentali sulla lotta al terrorismo dell'ottobre 2018. Il 9 ottobre la Commissione ha firmato due accordi bilaterali non vincolanti in materia di lotta contro il terrorismo con l'Albania e la Repubblica di Macedonia del Nord[75]. Tali accordi definiscono azioni prioritarie su misura che dovranno essere adottate dalle autorità di ognuno dei due paesi partner, riguardanti i cinque obiettivi del piano d'azione comune[76] e che indicano il sostegno che la Commissione prevede di fornire. Nelle prossime settimane si prevede la firma di accordi analoghi con i restanti paesi partner dei Balcani occidentali. Il 7 ottobre 2019, inoltre, la Commissione ha firmato con il Montenegro un accordo per la cooperazione in materia di gestione delle frontiere tra il Montenegro e l'Agenzia europea della guardia di frontiera e costiera (Frontex), che consente all'Agenzia di assistere il Montenegro nella gestione delle frontiere al fine di contrastare la migrazione irregolare e la criminalità transfrontaliera, potenziando così la sicurezza alle frontiere esterne dell'UE.

Al fine di potenziare la cooperazione con i paesi partner nel contrasto delle minacce comuni per la sicurezza, la Commissione invita il Consiglio:

- ad adottare l'autorizzazione all'avvio di negoziati per un accordo tra l'UE e la **Nuova Zelanda** sullo scambio di dati personali per la lotta contro le forme gravi di criminalità e il terrorismo,
- ad adottare l'autorizzazione all'avvio di negoziati per un accordo tra l'UE e il **Giappone** sul trasferimento dei dati del codice di prenotazione,
- ad adottare la proposta di **decisione del Consiglio relativa alla posizione da adottare a nome dell'UE nell'ambito dell'Organizzazione per l'aviazione civile internazionale** per quanto riguarda gli standard e le pratiche raccomandate sui dati del codice di prenotazione.

VI. CONCLUSIONE

La presente relazione descrive la vasta gamma di misure che l'UE ha adottato per affrontare le minacce comuni europee e rafforzare la sicurezza collettiva. I progressi compiuti verso un'autentica ed efficace Unione della sicurezza, guidati dall'idea condivisa secondo cui il modo migliore per rispondere alle sfide in materia di sicurezza è lavorare insieme e con i

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en.

[76] Il piano d'azione comune prevede azioni mirate ai cinque obiettivi seguenti: un quadro solido per la lotta contro il terrorismo; una prevenzione e un contrasto efficaci dell'estremismo violento; uno scambio di informazioni e una cooperazione operativa efficaci; lo sviluppo di capacità per contrastare il riciclaggio di denaro e il finanziamento del terrorismo; il rafforzamento della protezione dei cittadini e dell'infrastruttura.

paesi terzi, sono il risultato di una stretta cooperazione tra un ampio spettro di attori, che permette di alimentare la fiducia reciproca, condividere le risorse e affrontare le minacce congiuntamente: a tutti i livelli di governo, dalle città e dagli altri attori locali, passando per le regioni e le autorità nazionali fino al livello dell'UE con il Parlamento europeo e il Consiglio, con la partecipazione delle autorità pubbliche, delle agenzie dell'UE, di soggetti privati e della società civile e con l'uso di competenze, strumenti e risorse provenienti da diversi settori, tra cui la politica dei trasporti, il mercato unico digitale o la politica di coesione. In questo modo l'operato per l'Unione della sicurezza viene integrato nella protezione dei diritti fondamentali, tutelando e promuovendo i nostri valori.

Il lavoro verso un'autentica ed efficace Unione della sicurezza deve continuare. Occorre raggiungere rapidamente un accordo su importanti iniziative pendenti: 1) la proposta legislativa sulla rimozione dei contenuti terroristici online; 2) la proposta legislativa volta a migliorare l'accesso delle autorità di contrasto alle prove elettroniche; 3) la proposta legislativa che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento; 4) le proposte legislative pendenti sui sistemi di informazione più solidi e intelligenti per la gestione della sicurezza, delle frontiere e della migrazione. Le misure e gli strumenti concordati devono essere convertiti in realtà operative concrete grazie a un'attuazione tempestiva e completa della legislazione dell'UE da parte di tutti gli Stati membri, in modo da sfruttarne tutti i vantaggi per la sicurezza. È essenziale in particolare che tutti gli Stati membri attuino la legislazione recentemente convenuta sull'interoperabilità dei sistemi di informazione dell'UE per la gestione della sicurezza, delle frontiere e della migrazione, al fine di conseguire l'ambizioso obiettivo di una piena interoperabilità entro il 2020. Infine l'Europa deve continuare a vigilare sulle minacce emergenti e sull'evoluzione delle minacce esistenti, e a lavorare all'unisono per rafforzare la sicurezza di tutti i cittadini.