COMMISSIONE
EUROPEA

Bruxelles, 24.7.2019
COM(2019) 353 final

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

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

I. INTRODUZIONE

Il presente documento è la diciannovesima 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.

Gli europei si aspettano, giustamente, che la loro Unione li protegga. Per la Commissione Juncker la sicurezza è stata una priorità assoluta fin dal primo giorno. Nella nuova agenda strategica 2019-2024 del Consiglio europeo, l'obiettivo di "proteggere i cittadini e le libertà" figura al primo posto tra le quattro principali priorità dell'Unione[1]. Il Consiglio europeo ha inoltre annunciato che intende sviluppare e rafforzare gli sforzi dell'Unione nella lotta contro il terrorismo e la criminalità transfrontaliera, anche migliorando la cooperazione e la condivisione di informazioni e sviluppando ulteriormente strumenti comuni.

Grazie alla stretta cooperazione tra il Parlamento europeo, il Consiglio e la Commissione, l'UE ha compiuto passi significativi nel lavoro comune per realizzare un'autentica ed efficace Unione della sicurezza, mettendo in atto una serie di iniziative legislative prioritarie e attuando un'ampia gamma di misure non legislative volte a sostenere gli Stati membri e a rafforzare la sicurezza per tutti i cittadini[2]. L'Unione ha intrapreso un'azione decisiva per ridurre il margine di manovra dei terroristi e dei criminali: vietando l'acquisizione e l'uso di talune armi da fuoco ed esplosivi e limitando l'accesso ai finanziamenti ha privato i terroristi dei mezzi per perpetrare attentati. L'UE ha inoltre potenziato la condivisione delle informazioni tra gli Stati membri e ha colmato le lacune informative e i punti deboli, continuando nel contempo a combattere la radicalizzazione, a proteggere i cittadini europei online, a far fronte alle minacce informatiche e basate sull'uso di strumenti informatici e a rafforzare la gestione delle frontiere esterne dell'Unione e la cooperazione internazionale nel settore della sicurezza.

Nel contempo, una serie di iniziative prioritarie nel settore dell'Unione della sicurezza è ancora in attesa di adozione da parte dei colegislatori. In seguito alla costituzione della nona legislatura del Parlamento europeo, avvenuta il 2 luglio 2019, la presente relazione:

- indica i casi in cui è richiesta l'azione dei colegislatori per far fronte a minacce immediate. È particolarmente urgente intervenire per **contrastare la propaganda terroristica e la radicalizzazione online**;
- definisce le iniziative prioritarie in sospeso nel settore dell'Unione della sicurezza che richiedono ulteriori interventi da parte dei colegislatori per rafforzare la **cibersicurezza** e facilitare l'accesso alle **prove elettroniche** e per portare a termine i lavori su sistemi d'informazione più solidi e intelligenti per la sicurezza, le frontiere e la gestione della migrazione;
- aggiorna sull'attività congiunta e urgente avviata nel marzo 2019 per valutare e rafforzare la **sicurezza delle reti 5G**, sulla base delle valutazioni nazionali dei rischi presentate dagli Stati membri entro il 15 luglio 2019;
- informa su un pacchetto di quattro relazioni relative al **riciclaggio di denaro**, adottato

[1] https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

[2] Per un quadro d'insieme, si vedano la scheda informativa "Unione della sicurezza: un'Europa che protegge" (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) e la diciottesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2019) 145 final del 20.3.2019).

dalla Commissione il 24 luglio 2019, che analizza gli attuali rischi e vulnerabilità in materia di riciclaggio e valuta le modalità di applicazione del pertinente quadro normativo dell'UE nei settori privato e pubblico;

- aggiorna sui progressi compiuti dal marzo 2019[3] nell'attuazione delle misure legislative nel settore dell'Unione della sicurezza; tra le principali priorità di attuazione rapida e completa da parte degli Stati membri figura la misura sull'interoperabilità dei sistemi di informazione;
- fa il punto per quanto riguarda i lavori in corso per contrastare la disinformazione e proteggere le elezioni dalle minacce basate sull'uso di strumenti informatici, gli sforzi per migliorare la preparazione e la protezione dalle minacce alla sicurezza e la cooperazione con i partner internazionali in materia di sicurezza.

II. ATTUAZIONE DELLE PRIORITÀ LEGISLATIVE

1. Prevenire la radicalizzazione online e nelle comunità

La prevenzione della radicalizzazione, sia online che nelle nostre comunità, è al centro della risposta dell'UE al terrorismo.

La terrificante sparatoria a Christchurch (Nuova Zelanda) del 15 marzo 2019 ha ricordato in modo orribile come Internet possa essere sfruttato a fini terroristici, sia dal jihadismo o dall'estremismo di estrema destra sia da qualsiasi altra ideologia estremista. La velocità e l'ampiezza con cui il video della sparatoria a Christchurch si è diffuso sulle piattaforme Internet hanno messo in evidenza l'importanza fondamentale che le piattaforme Internet dispongano di misure adeguate per arginare la rapida diffusione di contenuti di questo tipo.

In risposta alla sparatoria, il 15 maggio 2019 i capi di Stato o di governo di alcuni Stati membri e paesi terzi, il presidente Juncker e le piattaforme online hanno espresso il loro sostegno alla **"Christchurch Call to action"**[4] che definisce le azioni collettive volte a eliminare i contenuti terroristici e violenti online di stampo estremista. Altri impegni al riguardo sono stati assunti dal G7[5] e dal G20[6].

La Commissione ha già affrontato il pericolo chiaro e reale posto dai contenuti terroristici online presentando la **proposta legislativa** annunciata dal Presidente Juncker nel discorso sullo stato dell'Unione del 2018, che propone un quadro giuridico chiaro e armonizzato per impedire l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online[7]. Le misure proposte imporranno alle piattaforme Internet l'obbligo di eliminare i contenuti terroristici entro un'ora dal ricevimento di un ordine di rimozione ingiunto dalle autorità competenti di qualsiasi Stato membro. Inoltre, se una piattaforma è usata in modo improprio per diffondere contenuti terroristici, la piattaforma in questione sarà tenuta a

---

3 Si veda la diciottesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2019) 145 final del 20.3.2019).

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. Il presidente francese Emmanuel Macron e il primo ministro neozelandese Jacinda Ardern hanno invitato i leader e le piattaforme online a Parigi il 15 maggio 2019 per lanciare l'iniziativa.

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

6 In occasione del G20 di Osaka il 28 e 29 giugno 2019, i leader hanno ribadito l'impegno ad agire per proteggere le persone dal terrorismo e dall'estremismo violento che favoriscono il terrorismo via Internet (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final del 12.9.2018.

ricorrere a misure proattive per individuare tali contenuti e impedirne la ricomparsa, con norme e garanzie chiare. Le autorità degli Stati membri dovranno assicurare un'apposita capacità di contrasto dotata delle risorse necessarie per individuare efficacemente i contenuti terroristici ed emettere ordini di rimozione.

Ciò consentirà un sistema rapido ed efficace a livello di Unione e assicurerà solide garanzie, compresi meccanismi di reclamo efficaci e disposizioni per il ricorso giudiziario. Le misure proposte contribuiranno a garantire il buon funzionamento del mercato unico digitale e nel contempo aumenteranno la sicurezza, rafforzeranno la fiducia online e potenzieranno le garanzie per la libertà di espressione e di informazione.

Nel dicembre 2018 i ministri della Giustizia e degli Affari interni in seno al Consiglio hanno concordato un approccio generale sulla proposta. Il Parlamento europeo ha adottato la sua posizione in prima lettura nell'aprile 2019. **La Commissione invita entrambi i colegislatori ad avviare quanto prima negoziati interistituzionali su questa iniziativa prioritaria per rimuovere i contenuti terroristici online**, al fine di raggiungere rapidamente un accordo su un quadro normativo dell'UE con norme e garanzie chiare.

Parallelamente, la Commissione prosegue la cooperazione con le piattaforme online nel quadro del **forum dell'UE su Internet**[8]. Come annunciato dal Presidente Juncker nella riunione di Parigi del 15 maggio 2019 sulla "Christchurch Call to action", la Commissione, insieme a Europol, ha avviato i lavori sullo sviluppo di un **protocollo di crisi per l'UE** per consentire ai governi e alle piattaforme Internet di reagire in modo rapido e coordinato alla diffusione di contenuti terroristici online, ad esempio all'indomani di un attentato terroristico. Tali lavori rientrano negli sforzi intrapresi a livello internazionale per attuare la "Christchurch Call for Action". Oltre alle ulteriori discussioni con gli Stati membri e l'industria e a un'esercitazione a tavolino prevista a settembre 2019 per simulare una situazione di emergenza, il 7 ottobre 2019 la Commissione convocherà una riunione ministeriale sul forum dell'UE su Internet per approvare il protocollo di crisi per l'UE.

Inoltre, la Commissione continua ad adoperarsi per **sostenere gli Stati membri e gli attori locali nella prevenzione e nella lotta alla radicalizzazione** sul campo nelle comunità locali di tutta Europa. A tal fine sono necessari sforzi sostenibili a lungo termine che coinvolgano tutti i soggetti interessati a livello locale, nazionale e dell'UE. Il **comitato direttivo per le azioni dell'Unione in materia di prevenzione e di lotta alla radicalizzazione**, istituito nell'agosto 2018 per fornire consulenza alla Commissione sulle modalità per rafforzare la risposta politica dell'UE in questo settore, ha tenuto la sua seconda riunione il 17 giugno 2019 per esaminare ulteriori azioni in settori prioritari quali la radicalizzazione nelle carceri e la lotta alle ideologie estremiste. Poiché gli operatori in prima linea e di prossimità si trovano spesso nella posizione migliore per individuare i primi segnali di allarme della radicalizzazione e i modi per affrontarla, la **rete per la sensibilizzazione alla radicalizzazione**[9], finanziata dall'UE, continua a sostenere il personale di prima linea,

[8] Avviato nel 2015, il **forum dell'UE su Internet** riunisce i ministri degli Affari interni dell'UE, l'industria di Internet e altri portatori di interessi per collaborare in un partenariato volontario volto a contrastare l'uso improprio di Internet da parte di gruppi terroristici e a proteggere i cittadini.

[9] Nel 2011 la Commissione ha istituito la **rete per la sensibilizzazione alla radicalizzazione** al fine di riunire gli operatori in prima linea e di prossimità. Nel 2015 la Commissione ha potenziato la rete istituendo il centro di eccellenza della rete per la sensibilizzazione alla radicalizzazione al fine di sviluppare servizi più mirati di orientamento, sostegno e consulenza per i portatori di interessi degli Stati membri e aumentare le competenze e le capacità dei diversi attori. Per ulteriori informazioni sulle attività della rete per la sensibilizzazione alla radicalizzazione si rinvia al seguente indirizzo: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

mettendo in collegamento circa 5 000 operatori della società civile, delle scuole e delle forze di polizia, nonché coordinatori nazionali e responsabili politici.

La recente collaborazione degli operatori in prima linea all'interno della rete ha portato a una comprensione più approfondita delle sfide poste dall'estremismo di estrema destra. Quest'anno la rete di sensibilizzazione alla radicalizzazione pubblicherà schede informative per aiutare i responsabili politici e gli operatori del settore a individuare le principali forme e manifestazioni dell'estremismo islamico a di estrema destra, quali narrazioni, linguaggio, forme, simboli, tipologie e strategie chiave. Infine, poiché gli attori locali e le **città** sono in prima linea nella prevenzione e nel contrasto della radicalizzazione, la Commissione sostiene le iniziative di lotta alla radicalizzazione condotte dalle città. In seguito alla conferenza intitolata "Le città dell'UE contro la radicalizzazione" tenutasi il 26 febbraio 2019, l'8 luglio 2019 si è tenuta la prima riunione di un gruppo pilota di circa 20 città ospitata dal sindaco di Strasburgo per intensificare lo scambio di buone pratiche e rafforzare gli sforzi delle città in questo settore.

Parallelamente, sono in corso lavori per sostenere i paesi partner nell'affrontare la radicalizzazione che può portare al terrorismo, anche nelle carceri.

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

- ad avviare negoziati sulla proposta legislativa volta a prevenire la diffusione di **contenuti terroristici online**, onde raggiungere rapidamente un accordo su un quadro normativo dell'UE con norme e garanzie chiare.

2. Rafforzare la cibersicurezza

La cibersicurezza rimane una sfida fondamentale per la sicurezza. L'Unione europea ha compiuto importanti progressi[10] nella lotta contro le minacce informatiche "classiche" aventi ad oggetto sistemi e dati, attuando le azioni definite nella comunicazione congiunta[11] del settembre 2017 dal titolo "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE". Tra queste azioni figura il regolamento UE sulla cibersicurezza,[12], che conferisce un mandato permanente all'agenzia dell'Unione europea per la cibersicurezza, rafforzandone il ruolo, e istituisce un quadro dell'UE per la certificazione della cibersicurezza. La Commissione ha inoltre affrontato i requisiti specifici per settore, ad esempio mediante la raccomandazione sulla cibersicurezza nel settore dell'energia, adottata il 3 aprile 2019[13]. Tuttavia, poiché l'attività di soggetti malintenzionati continua ad aumentare riguardo a una vasta gamma di obiettivi e vittime, gli sforzi per contrastare la criminalità informatica e rafforzare la cibersicurezza restano prioritari per l'azione dell'UE.

---

10 Per maggiori informazioni, si rinvia all'opuscolo "Building strong cybersecurity in the European Union: resilience, deterrence, defence": https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

11 JOIN(2017) 450 final del 13.9.2017.

12 Il regolamento UE sulla cibersicurezza (regolamento (UE) 2019/881 del 17 aprile 2019) introduce per la prima volta norme a livello dell'UE per la certificazione della cibersicurezza di prodotti, processi e servizi. Inoltre affida un nuovo mandato permanente all'agenzia dell'UE per la cibersicurezza (ENISA), cui assegna maggiori risorse affinché possa raggiungere gli obiettivi. Per maggiori informazioni sull'invito a presentare proposte, si rinvia al seguente indirizzo: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

13 C(2019) 2400 final del 3.4.2019 e SWD(2019) 1240 final del 3.4.2019.

Il Parlamento europeo e il Consiglio devono ancora raggiungere un accordo sull'iniziativa prioritaria della Commissione relativa al **Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e alla rete dei centri nazionali di coordinamento**[14]. La proposta mira a sostenere le capacità tecnologiche e industriali in materia di cibersicurezza e ad aumentare la competitività del settore della sicurezza informatica dell'Unione. Entrambi i colegislatori hanno adottato i rispettivi mandati negoziali nel marzo 2019. Poiché non è stato possibile concludere i negoziati interistituzionali prima della fine del precedente mandato del Parlamento europeo, quest'ultimo ha adottato formalmente la sua posizione in prima lettura. Nel frattempo le discussioni tra gli Stati membri in sede di Consiglio proseguono, con particolare attenzione all'interazione tra la proposta di regolamento che istituisce il Centro di competenza sulla cibersicurezza e la relativa rete, da un lato, e i programmi Orizzonte Europa e Europa digitale, dall'altro. **La Commissione invita entrambi i colegislatori a riprendere e concludere rapidamente i negoziati interistituzionali su questa iniziativa prioritaria per migliorare la cibersicurezza.**

Nel frattempo, la Commissione continua a **sostenere la ricerca e l'innovazione** in materia di cibersicurezza, mettendo a disposizione 135 milioni di EUR nell'attuale quadro finanziario pluriennale per progetti in settori quali la cibersicurezza delle infrastrutture critiche, la sicurezza intelligente e la gestione della privacy, e strumenti specificamente destinati ai cittadini e alle piccole e medie imprese[15]. Nel luglio 2019 la Commissione ha pubblicato un nuovo invito a presentare proposte nell'ambito del programma "Meccanismo per collegare l'Europa", mettendo a disposizione 10 milioni di EUR a favore dei principali soggetti individuati dalla direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)[16], quali i gruppi europei di intervento per la sicurezza informatica in caso di incidente, gli operatori di servizi essenziali (ad esempio banche, ospedali, fornitori di servizi, ferrovie, compagnie aeree, fornitori di nomi di dominio) e varie autorità pubbliche. Per la prima volta è data la possibilità alle autorità europee di certificazione della cibersicurezza di presentare domanda per tale programma al fine di consentire loro di attuare il regolamento UE sulla cibersicurezza.

Il 17 maggio 2019 il Consiglio ha adottato un **regime sanzionatorio** che consente all'UE di imporre misure restrittive mirate volte a scoraggiare e contrastare gli attacchi informatici che costituiscono una minaccia esterna per l'UE e i suoi Stati membri. Il nuovo regime sanzionatorio fa parte del **pacchetto di strumenti della diplomazia informatica dell'UE**[17], in cui è definita la risposta diplomatica comune dell'UE alle attività informatiche dolose.[18] Il pacchetto permette all'UE di avvalersi pienamente delle misure previste dalla politica estera e di sicurezza comune per scoraggiare e contrastare le attività informatiche dolose.

---

14 COM(2018) 630 final del 12.9.2018.

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Direttiva (UE) 2016/1148 del 6 luglio 2016.

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/it/pdf

18 Tali attività comprendono gli attacchi informatici e i tentati attacchi informatici con effetti potenzialmente significativi, che comportano ad esempio l'accesso ai sistemi di informazione o l'intercettazione di dati mediante infrastrutture digitali quali le reti 5G (si veda anche la sezione III sul miglioramento della sicurezza delle infrastrutture digitali).

Oltre alle minacce informatiche contro i sistemi e i dati, l'UE sta anche intervenendo per affrontare le complesse e multiformi sfide poste dalle **minacce ibride**[19]. Il Consiglio europeo, nelle conclusioni del 21 giugno 2019[20], ha sottolineato che *"[l]'UE deve garantire una risposta coordinata alle minacce ibride e informatiche e intensificare la sua cooperazione con i pertinenti attori internazionali"*. La Commissione si compiace del fatto che la lotta alle minacce ibride è anche una priorità della presidenza finlandese del Consiglio e che, durante la riunione informale dei ministri della Giustizia e degli Affari interni tenutasi a Helsinki il 18-19 luglio 2019, si è svolta una discussione politica sulle minacce ibride basata su scenari. Analoghe discussioni sulle minacce ibride basate su scenari hanno avuto luogo tra i direttori per la politica di difesa dell'UE il 7 e l'8 luglio 2019 e tra i direttori politici dell'UE il 9 e il 10 luglio 2019, i cui risultati saranno comunicati ai ministri degli Affari esteri e della Difesa in una sessione informale congiunta che si terrà il 29 e il 30 agosto 2019.

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

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

3. Migliorare l'accesso delle autorità di contrasto alle prove elettroniche

L'UE ha preso ulteriori provvedimenti per privare i terroristi e i criminali dei mezzi per agire, rendendo loro più difficile accedere ai precursori di esplosivi[21], finanziare le proprie attività[22] e viaggiare senza essere individuati[23].

I negoziati sulle proposte della Commissione dell'aprile 2018 volte a migliorare l'**accesso delle autorità di contrasto alle prove elettroniche** dovrebbero essere portati a termine il più rapidamente possibile: oltre la metà di tutte le indagini penali attualmente implicano una richiesta transfrontaliera di accesso a prove elettroniche[24]. Il Consiglio ha adottato la sua posizione negoziale in merito alla proposta di regolamento per migliorare l'accesso a livello transfrontaliero alle prove elettroniche nelle indagini penali[25], e alla proposta di direttiva

---

19 Si vedano la relazione sull'attuazione del quadro congiunto per contrastare le minacce ibride del 2016 e la comunicazione congiunta del 2018 "Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride" (SWD(2019) 200 final del 28.5.2019). Si veda anche la proposta legislativa del settembre 2016 relativa a un regolamento che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso (rifusione) (COM(2016) 616 final del 28.9.2016).

20 https://data.consilium.europa.eu/doc/document/ST-9-2019-INIT/it/pdf

21 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.

22 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.

23 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.

24 Le prove elettroniche sono necessarie per circa l'85% delle indagini penali, e per due terzi di queste indagini è necessario richiedere tali prove da prestatori di servizi online con sede in un'altra giurisdizione. Si veda la valutazione d'impatto che accompagna la proposta legislativa (SWD(2018) 118 final del 17.4.2018).

25 COM(2018) 225 final del 17.4.2018. Il 7 dicembre 2018 il Consiglio ha adottato il mandato negoziale sulla proposta di regolamento in sede di Consiglio "Giustizia e affari interni".

recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali[26]. Data l'importanza cruciale di un accesso efficiente alle prove elettroniche ai fini delle indagini e del perseguimento di reati transfrontalieri come il terrorismo o la criminalità informatica, la Commissione esorta il Parlamento europeo a portare avanti con urgenza la proposta affinché i colegislatori possano adoperarsi per una rapida adozione.

Parallelamente, la Commissione sta lavorando per migliorare e assicurare le garanzie necessarie nell'ambito dello **scambio internazionale di prove elettroniche** nel contesto dei negoziati in corso per un secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica e dei negoziati con gli Stati Uniti, in linea con i mandati negoziali forniti dal Consiglio nella sessione del Consiglio "Giustizia e affari interni" del 6 e 7 giugno 2019[27]. La Commissione ha partecipato all'ultima tornata di negoziati relativi a un secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, tenutasi dal 9 all'11 luglio 2019. La Commissione e le autorità statunitensi stanno preparando, a livello tecnico, l'avvio formale dei negoziati per un accordo UE-USA sull'accesso transfrontaliero alle prove elettroniche.

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

- ad adottare il suo mandato negoziale sulle proposte legislative relative alle **prove elettroniche** per avviare rapidamente i triloghi con il Consiglio. *(Priorità della dichiarazione comune)*

4. Predisporre sistemi d'informazione più solidi e intelligenti per la sicurezza, le frontiere e la gestione della migrazione

In seguito all'adozione delle norme sull'**interoperabilità dei sistemi di informazione**[28], che colmeranno le lacune e i punti deboli contribuendo a individuare le identità multiple e a contrastare la frode di identità, la Commissione ha prontamente avviato una serie di iniziative volte a sostenere gli Stati membri nel processo di attuazione, anche attraverso il finanziamento ove necessario, nonché con seminari per facilitare lo scambio di competenze e di buone pratiche. La stretta cooperazione tra le agenzie dell'UE, tutti gli Stati membri e i paesi associati a Schengen sarà fondamentale per conseguire l'ambizioso obiettivo di raggiungere la piena interoperabilità dei sistemi di informazione dell'UE per la sicurezza, le frontiere e la gestione della migrazione entro il 2020.

Questo obiettivo richiede inoltre la rapida e completa attuazione della legislazione recentemente adottata per istituire i nuovi sistemi di informazione – il sistema di ingressi/uscite dell'UE[29] e il sistema europeo di informazione e autorizzazione ai viaggi[30] – e

[26] COM(2018) 226 final del 17.4.2018. L'8 marzo 2019 il Consiglio ha adottato la posizione negoziale sulla proposta di direttiva in sede di Consiglio "Giustizia e affari interni".

[27] https://www.consilium.europa.eu/it/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[28] Regolamento (UE) 2019/817 del 20.5.2019 e regolamento (UE) 2019/818 del 20.5.2019.

[29] Regolamento (UE) 2017/2226 del 30 novembre 2017.

[30] Regolamento (UE) 2018/1240 del 12 settembre 2018 e regolamento (UE) 2018/1241 del 12 settembre 2018.

per rafforzare il sistema d'informazione Schengen[31] ed estendere il sistema europeo di informazione sui casellari giudiziali[32] ai cittadini di paesi terzi. La nuova architettura per sistemi d'informazione più solidi e intelligenti per la sicurezza, le frontiere e la gestione della migrazione farà la differenza sul campo se tutti i componenti saranno pienamente attuati a livello di Unione e da ciascuno Stato membro, secondo il calendario concordato.

Al tempo stesso, sono necessari ulteriori interventi da parte dei colegislatori per completare i lavori relativi a sistemi d'informazione più solidi e intelligenti per la sicurezza, le frontiere e la gestione della migrazione. Nell'ambito dell'attuazione tecnica del **sistema europeo di informazione e autorizzazione ai viaggi**, il 7 gennaio 2019 la Commissione ha presentato due proposte contenenti modifiche tecniche al relativo regolamento[33] necessarie per la piena istituzione del sistema. La Commissione invita i colegislatori a portare avanti il lavoro sulle modifiche tecniche al fine di raggiungere un accordo il prima possibile, consentendo in tal modo una rapida e tempestiva attuazione del sistema europeo di informazione e autorizzazione ai viaggi per renderlo operativo all'inizio del 2021.

Nel maggio 2018 la Commissione ha presentato una proposta volta a **rafforzare l'attuale sistema di informazione visti**[34]. Tale proposta prevede un più approfondito controllo dei precedenti personali dei richiedenti il visto e mira a colmare il vuoto informativo attraverso un migliore scambio di informazioni tra gli Stati membri. Il Consiglio ha adottato il suo mandato negoziale il 19 dicembre 2018 e, il 13 marzo 2019, il Parlamento europeo ha votato in plenaria la sua relazione sulla proposta, concludendo così la sua prima lettura. La Commissione chiede un rapido avvio dei negoziati tra i colegislatori nell'ambito del Parlamento europeo recentemente costituito.

Nel maggio 2016 la Commissione ha proposto di ampliare l'ambito di applicazione di **Eurodac**[35] includendo non solo l'identificazione dei richiedenti asilo, ma anche dei cittadini di paesi terzi il cui soggiorno è irregolare e di coloro che entrano illegalmente nell'UE. In linea con le conclusioni del Consiglio europeo del dicembre 2018[36] e con la comunicazione della Commissione del 6 marzo 2019 sullo stato di attuazione dell'agenda europea sulla migrazione[37], la Commissione invita i colegislatori a procedere all'adozione della proposta. Tale adozione è necessaria per consentire ad Eurodac di diventare parte della futura architettura dei sistemi di informazione interoperabili dell'UE, integrando in tal modo i dati fondamentali dei cittadini di paesi terzi il cui soggiorno è irregolare e di coloro che sono entrati illegalmente nell'UE.

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

- ad adottare la proposta legislativa sull'**Eurodac** *(priorità della dichiarazione congiunta)*;
- a portare avanti i lavori per raggiungere rapidamente un accordo sulle modifiche tecniche proposte, necessarie per istituire il **sistema europeo di informazione e autorizzazione ai viaggi**.

[31] Regolamento (UE) 2018/1860 del 28 novembre 2018, regolamento (UE) 2018/1861 del 28 novembre 2018 e regolamento (UE) 2018/1862 del 28 novembre 2018.
[32] Regolamento (UE) 2019/816 del 17 aprile 2019.
[33] COM(2019)3 final e COM(2019) 4 final del 7.1.2019.
[34] COM(2018) 302 final del 16.5.2018.
[35] COM(2016) 272 final del 4.5.2016.
[36] https://www.consilium.europa.eu/it/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
[37] COM(2019) 126 final del 6.3.2019.

III. RAFFORZARE LA SICUREZZA DELLE INFRASTRUTTURE DIGITALI

La resilienza delle nostre infrastrutture digitali è fondamentale per i governi, le imprese, la sicurezza dei nostri dati personali e il funzionamento delle nostre istituzioni democratiche. Le **reti di quinta generazione (5G)** che saranno realizzate nei prossimi anni costituiranno la spina dorsale digitale delle nostre società e delle nostre economie, collegando miliardi di cittadini, oggetti e sistemi, anche in settori critici quali l'energia, i trasporti, il settore bancario e la sanità, nonché i sistemi di controllo industriale che trasmettono informazioni sensibili e che forniscono sostegno ai sistemi di sicurezza.

Con profitti a livello mondiale stimati a 225 miliardi di euro nel 2025, il 5G è una risorsa fondamentale per l'Europa per competere nel mercato globale e **la sicurezza delle reti 5G è essenziale per garantire l'autonomia strategica dell'Unione**. Garantire un livello elevato di cibersicurezza richiede misure concertate a livello sia nazionale che europeo, poiché qualsiasi vulnerabilità delle reti 5G di uno Stato membro si ripercuoterà sull'Unione nel suo insieme.

Forte del sostegno dei capi di Stato o di governo espresso durante il Consiglio europeo del marzo 2019[38], il 26 marzo 2019 la Commissione ha presentato una **raccomandazione sulla cibersicurezza delle reti 5G**[39], che indica una serie di azioni per valutare i rischi per la cibersicurezza delle reti 5G e per rafforzare le misure preventive. Le raccomandazioni si basano su una valutazione coordinata dei rischi e su misure coordinate di gestione dei rischi a livello di UE, su un quadro efficace per la cooperazione e lo scambio di informazioni e su una conoscenza comune della situazione delle reti di comunicazione critiche nell'UE.

Come **prima fase** del processo avviato dalla raccomandazione, entro il 15 luglio 2019 tutti gli Stati membri hanno completato la **valutazione nazionale dei rischi** e hanno presentato i loro risultati alla Commissione e all'agenzia dell'UE per la cibersicurezza, o hanno annunciato che lo avrebbero fatto a breve. Le valutazioni nazionali dei rischi hanno seguito una serie di orientamenti e un modello comune per riferire sui risultati, concordati dagli Stati membri e dalla Commissione al fine di promuovere la coerenza e facilitare lo scambio di informazioni sui risultati nazionali a livello dell'UE. I parametri valutati in tutti gli Stati membri comprendono:

- le principali minacce che incombono sulle reti 5G e gli attori di tali minacce;
- il grado di sensibilità di componenti e funzioni delle reti 5G e di altre risorse;
- vari tipi di vulnerabilità, comprese quelle tecniche e quelle che potrebbero derivare dalla catena di approvvigionamento 5G.

Inoltre il lavoro sulle valutazioni nazionali dei rischi ha coinvolto diversi soggetti competenti degli Stati membri, quali, a seconda delle competenze nazionali, le autorità per la cibersicurezza, le telecomunicazioni, i servizi di sicurezza e di intelligence, consolidandone la cooperazione e il coordinamento. Parallelamente e tenuto conto del rispettivo calendario nazionale per la diffusione del 5G, alcuni Stati membri hanno già adottato misure per rafforzare i requisiti di sicurezza applicabili in questo settore, mentre molti altri hanno manifestato l'intenzione di prendere in considerazione nuove misure nel prossimo futuro.

[38] https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/it/pdf
[39] C(2019) 2335 final del 26.3.2019.

Sulla base dei risultati delle valutazioni nazionali dei rischi, entro il 1º ottobre 2019 le autorità per la cibersicurezza degli Stati membri in seno al gruppo di cooperazione per la sicurezza delle reti e dei sistemi informativi[40] elaboreranno un **riesame congiunto dei rischi a livello dell'UE** che costituirà la seconda fase del processo avviato dalla raccomandazione. Su tale base, e come terza fase, il gruppo di cooperazione preparerà, entro il 31 dicembre 2019, una **serie di misure di attenuazione comuni dell'Unione** per far fronte ai rischi individuati. La Commissione e l'agenzia dell'Unione europea per la cibersicurezza continueranno a sostenere l'attuazione della raccomandazione.

I lavori del gruppo di cooperazione per la sicurezza delle reti e dei sistemi informativi sono sostenuti da varie altre entità. L'Organismo dei regolatori europei delle comunicazioni elettroniche sta preparando un'indagine su tutte le misure di sicurezza esistenti potenzialmente rilevanti per il 5G. Un nuovo gruppo di esperti ad hoc in seno all'agenzia dell'UE per la cibersicurezza ha avviato i lavori sulla revisione del panorama delle minacce per il 5G. Inoltre, a seguito dell'entrata in vigore del regolamento sulla cibersicurezza, il 27 giugno 2019 la Commissione e l'agenzia dell'UE per la cibersicurezza adotteranno tutte le misure necessarie per istituire il quadro di certificazione a livello dell'UE. Nel giugno 2019 gli Stati membri si sono inoltre riuniti in seno al comitato delle norme per discutere in merito alla cibersicurezza e alla normalizzazione in risposta alla raccomandazione che invita a esaminare le future sfide per la normalizzazione della cibersicurezza, comprese le reti 5G, e a iniziative politiche adeguate a livello dell'UE.

Infine, la sicurezza delle reti 5G riveste importanza strategica per l'Unione. Anche gli investimenti esteri nei settori strategici, l'acquisizione di beni, tecnologie e infrastrutture critici nell'Unione e la fornitura di apparecchiature fondamentali possono mettere a rischio la sicurezza dell'Unione.

Il nuovo **quadro dell'UE per il controllo degli investimenti esteri diretti**[41] è entrato in vigore il 10 aprile 2019. Nei prossimi 18 mesi la Commissione e gli Stati membri adotteranno le misure necessarie per garantire che l'Unione possa dare piena applicazione al regolamento sul controllo degli investimenti a partire dall'11 ottobre 2020.

IV. ANTIRICICLAGGIO

La capacità dei criminali e dei terroristi di trasferire fondi tra conti bancari nel giro di poche ore consente loro di preparare più facilmente i loro atti di terrore o di riciclare illegalmente i proventi di reato nei vari Stati membri. Per far fronte a questa sfida, l'Unione ha sviluppato un

[40] Il gruppo di cooperazione per la sicurezza delle reti e dei sistemi informativi è stato istituito ai sensi della direttiva UE 2016/1148, del 6 luglio 2016, sulla sicurezza delle reti e dei sistemi informativi. Come previsto dalla raccomandazione, è stato istituito un apposito flusso di lavoro nell'ambito del gruppo di cooperazione per la sicurezza delle reti e dei sistemi informativi, guidato da diversi Stati membri. Il gruppo si è già riunito tre volte, nei mesi di aprile, maggio e luglio 2019, per scambiare informazioni sugli approcci nazionali e per discutere come agevolare la preparazione della valutazione coordinata dei rischi dell'UE.

[41] Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione. Il nuovo quadro crea un meccanismo di cooperazione grazie al quale gli Stati membri e la Commissione potranno scambiarsi informazioni ed esprimere le loro preoccupazioni relative a investimenti specifici. Inoltre consentirà alla Commissione di esprimere pareri nel caso in cui un investimento minacci la sicurezza o l'ordine pubblico di più di uno Stato membro o nel caso in cui un investimento possa compromettere un progetto o un programma di interesse collettivo per l'UE. Lo Stato membro in cui ha luogo l'investimento ha l'ultima parola su come trattare l'investimento.

solido **quadro normativo per contrastare il riciclaggio di denaro e il finanziamento del terrorismo**, in linea con le norme internazionali adottate dal Gruppo di azione finanziaria internazionale.

Data la necessità di tenere il passo con l'evoluzione delle tendenze, gli sviluppi tecnologici e l'adattamento dell'inventiva dei criminali per sfruttare eventuali lacune o punti deboli del sistema, il 24 luglio 2019 la Commissione ha adottato un **pacchetto di quattro relazioni** che analizzano i rischi e le vulnerabilità attuali connessi al riciclaggio di denaro e valutano le modalità di applicazione del quadro da parte dei soggetti interessati sia del settore privato che di quello pubblico[42].

Il pacchetto comprende una **valutazione della potenziale interconnessione fra i registri nazionali centralizzati dei conti bancari e i sistemi di reperimento dei dati** nell'UE. Tali sistemi centralizzati nazionali consentono l'identificazione di qualsiasi persona fisica o giuridica che detenga o controlli conti di pagamento, conti bancari e cassette di sicurezza — informazioni che sono spesso cruciali per le autorità competenti nella lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. La quinta direttiva antiriciclaggio[43] impone agli Stati membri di mettere in atto tali sistemi centralizzati nazionali e fornirne accesso diretto alle loro unità di informazione finanziaria. Le norme recentemente adottate per facilitare l'uso delle informazioni finanziarie per contrastare la criminalità grave[44] forniscono alle autorità di contrasto designate e agli uffici per il recupero dei beni accesso diretto ai rispettivi registri nazionali centralizzati dei conti bancari. Su tale base, e come previsto dalla direttiva antiriciclaggio, la relazione valuta varie soluzioni informatiche a livello dell'UE, già operative o in fase di sviluppo, che possono servire da modello per una possibile interconnessione dei sistemi nazionali centralizzati. Poiché una futura interconnessione a livello di UE dei meccanismi centralizzati faciliterebbe l'accesso alle informazioni finanziarie e la cooperazione transfrontaliera delle autorità competenti, la Commissione intende consultare ulteriormente i portatori di interessi, i governi, le unità di informazione finanziaria, le autorità di contrasto e gli uffici per il recupero dei beni, quali potenziali "utenti finali" di un possibile sistema di interconnessione.

Nell'ambito della riflessione della Commissione sul lavoro delle unità di informazione finanziaria, una relazione che valuta la **cooperazione tra le unità di informazione finanziaria** esamina la cooperazione sia all'interno dell'Unione sia con i paesi terzi[45]. Essa individua alcune carenze che probabilmente persisteranno fino a quando i compiti e gli obblighi di cooperazione transfrontaliera delle unità di informazione finanziaria saranno definiti più chiaramente nel quadro giuridico dell'UE in materia di lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. La valutazione evidenzia inoltre la necessità di un meccanismo più forte per coordinare e sostenere la cooperazione e l'analisi transfrontaliere.

---

42 Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM (2019) 370 final del 24.7.2019), Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts (COM(2019) 372 final del 24.7.2019), Report on the assessment of recent alleged money laundering cases involving EU credit institutions (COM(2019) 373 final del 24.7.2019), Report assessing the framework for cooperation between Financial Intelligence Units (COM(2019) 371 final del 24.7.2019).

43 Direttiva (UE) 2015/849 del 20 maggio 2015.

44 Direttiva (UE) 2019/1153 del 20 giugno 2019.

45 Tale valutazione è richiesta dall'articolo 65, paragrafo 2, della direttiva (UE) 2018/843 del 30 maggio 2018 (quinta direttiva antiriciclaggio).

Al di là delle attività in corso, e anche in risposta ad una richiesta del Parlamento europeo[46], la Commissione continuerà a valutare la necessità, la fattibilità tecnica e la proporzionalità di misure aggiuntive per tracciare il finanziamento del terrorismo nell'UE[47].

V. ATTUAZIONE DI ALTRI FASCICOLI PRIORITARI IN MATERIA DI SICUREZZA

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

Il raggiungimento di un accordo sulle misure nel quadro dell'Unione della sicurezza non rappresenta la conclusione del processo; è di vitale importanza garantirne successivamente l'attuazione rapida e completa da parte degli Stati membri, in modo da poter beneficiare appieno dei vantaggi attesi. A tal fine, la Commissione sta attivamente sostenendo gli Stati membri, anche con finanziamenti e facilitando lo scambio delle migliori prassi. Ove necessario, tuttavia, la Commissione è pronta ad avvalersi appieno dei poteri conferitile dai trattati per l'attuazione del diritto dell'Unione, ricorrendo anche, se opportuno, al procedimento d'infrazione.

Il termine per l'attuazione della **direttiva UE sul codice di prenotazione**[48] è scaduto il 25 maggio 2018. Ad oggi 25 Stati membri hanno notificato il recepimento integrale alla Commissione[49]. Nonostante le procedure di infrazione avviate il 19 luglio 2018, due Stati membri non hanno ancora recepito integralmente la direttiva[50]. In parallelo, la Commissione continua a sostenere gli Stati membri nei loro sforzi per completare lo sviluppo dei rispettivi sistemi di codice di prenotazione, anche agevolando lo scambio di informazioni e di migliori pratiche.

Il termine per il recepimento della **direttiva sulla lotta contro il terrorismo**[51] è scaduto l'8 settembre 2018. Ad oggi 22 Stati membri hanno notificato il recepimento integrale alla Commissione. Tre Stati membri non hanno ancora comunicato l'adozione di una legislazione nazionale che recepisce integralmente la direttiva, nonostante le procedure di infrazione avviate il 22 novembre 2018[52].

Il termine per il recepimento della **direttiva relativa al controllo dell'acquisizione e della detenzione di armi**[53] è scaduto il 14 settembre 2018. Ad oggi 8 Stati membri hanno notificato il pieno recepimento alla Commissione. 20 Stati membri non hanno ancora comunicato l'adozione di misure nazionali che recepiscono integralmente la direttiva, nonostante le

---

46 Nella sua relazione finale adottata nel dicembre 2018, la commissione speciale sul terrorismo del Parlamento europeo ha chiesto l'istituzione di un sistema europeo di controllo delle transazioni finanziarie dei terroristi, mirato alle transazioni compiute da soggetti legati al terrorismo e al suo finanziamento all'interno dell'area unica dei pagamenti in euro.

47 Si veda la diciottesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2019) 145 final del 20.3.2019).

48 Direttiva (UE) 2016/681 del 27 aprile 2016.

49 I riferimenti alla notifica di recepimento completa tengono conto delle dichiarazioni degli Stati membri e non pregiudicano il controllo del recepimento da parte dei servizi della Commissione.

50 La Slovenia ha notificato il recepimento parziale. La Spagna non ha notificato il recepimento (situazione al 24 luglio 2019).

51 Direttiva (UE) 2017/541 del 15 marzo 2017.

52 La Polonia ha notificato il recepimento parziale. La Grecia e il Lussemburgo non hanno notificato il recepimento (situazione al 24 luglio 2019).

53 Direttiva (UE) 2017/853 del 17 maggio 2017.

procedure di infrazione avviate il 22 novembre 2018[54].

Per quanto riguarda il recepimento nel diritto nazionale della **direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie**[55], il termine per il recepimento è scaduto il 6 maggio 2018. Ad oggi 20 Stati membri hanno notificato il pieno recepimento alla Commissione[56]. Sette Stati membri non hanno ancora comunicato l'adozione di misure nazionali che recepiscono integralmente la direttiva, nonostante le procedure di infrazione avviate dalla Commissione il 19 luglio 2018[57].

Gli Stati membri avevano tempo fino al 9 maggio 2018 per recepire nel diritto nazionale la **direttiva sulla sicurezza delle reti e dei sistemi informativi**[58]. Ad oggi 26 Stati membri hanno notificato il recepimento integrale alla Commissione e due Stati membri hanno recepito parzialmente la direttiva[59]. Inoltre, entro il 9 novembre 2018, gli Stati membri erano tenuti a individuare gli operatori di servizi essenziali in linea con la direttiva. Entro il 9 maggio 2019 la Commissione avrebbe dovuto presentare al Parlamento europeo e al Consiglio una relazione per valutare la coerenza dell'approccio all'individuazione degli operatori di servizi essenziali individuati nel territorio degli Stati membri. Tuttavia, poiché un certo numero di Stati membri non ha ancora presentato informazioni complete sul processo di individuazione, la Commissione ha dovuto posticipare la sua relazione.

La Commissione sta valutando il recepimento della **quarta direttiva antiriciclaggio**[60] e nel contempo sta lavorando per verificare che gli Stati membri ne attuino le norme. La Commissione ha avviato procedimenti di infrazione contro 24 Stati membri, ritenendo che le comunicazioni da questi trasmesse non dimostrino un recepimento integrale della direttiva[61].

---

54 Il Belgio, la Cechia, l'Estonia, la Lituania, la Polonia, il Portogallo, la Svezia e il Regno Unito hanno notificato un recepimento parziale. La Germania, l'Irlanda, la Grecia, la Spagna, Cipro, il Lussemburgo, l'Ungheria, i Paesi Bassi, la Romania, la Slovenia, la Slovacchia e la Finlandia non hanno notificato il recepimento (situazione al 24 luglio 2019).

55 Direttiva (UE) 2016/680 del 27 aprile 2016.

56 20 Stati membri hanno completato il recepimento (situazione al 24 luglio 2019).

57 La Lettonia, il Portogallo, la Slovenia e la Finlandia hanno notificato il recepimento parziale. La Grecia e la Spagna non hanno notificato il recepimento. Sebbene la Germania abbia notificato il recepimento integrale, la Commissione ritiene che tale recepimento non sia completo (situazione al 24 luglio 2019).

58 Direttiva (UE) 2016/1148 del 27 aprile 2016.

59 Il Belgio e l'Ungheria hanno recepito parzialmente la direttiva (situazione al 24 luglio 2019).

60 Direttiva (UE) 2015/849 del 20 maggio 2015.

61 Belgio, Bulgaria, Cechia, Danimarca, Germania, Estonia, Irlanda, Spagna, Francia, Italia, Cipro, Lettonia, Lituania, Ungheria, Paesi Bassi, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia, Svezia e Regno Unito (situazione al 24 luglio 2019).

La Commissione invita gli Stati membri ad adottare con urgenza, e a comunicarle, le misure necessarie per recepire integralmente nel diritto nazionale le seguenti direttive:

- la **direttiva UE sui dati del codice di prenotazione**: uno Stato membro non ha ancora notificato il recepimento nel diritto nazionale e uno Stato membro deve completare la notifica del recepimento[62];
- la **direttiva sulla lotta contro il terrorismo**: due Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e uno Stato membro deve completare la notifica del recepimento[63];
- la **direttiva relativa al controllo dell'acquisizione e della detenzione di armi**: 12 Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e otto Stati membri devono completare la notifica del recepimento[64];
- la **direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie**: due Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e cinque Stati membri devono completare la notifica del recepimento[65];
- la **direttiva sulla sicurezza delle reti e dei sistemi informativi**: due Stati membri devono ancora completare la notifica di recepimento[66];
- la **quarta direttiva antiriciclaggio**: 24 Stati membri devono ancora completare la notifica del recepimento[67].

2. Lotta contro la disinformazione e protezione delle elezioni da altre minacce basate sull'uso di strumenti informatici

Proteggere i processi e le istituzioni democratiche dalla disinformazione e dalle interferenze correlate è una sfida importante per le società di tutto il mondo. Per far fronte a questa situazione, l'UE ha messo in atto un **quadro solido per un'azione coordinata contro la disinformazione**, nel pieno rispetto dei valori europei e dei diritti fondamentali[68]. Come indicato nella comunicazione congiunta del 14 giugno 2019 sull'attuazione del piano d'azione contro la disinformazione[69], i lavori su vari aspetti complementari hanno contribuito a ridurre lo spazio per la disinformazione e a preservare l'integrità delle elezioni del Parlamento europeo.

---

62 La Slovenia ha notificato il recepimento parziale. La Spagna non ha notificato il recepimento (situazione al 24 luglio 2019).

63 La Polonia ha notificato un recepimento parziale. La Grecia e il Lussemburgo non hanno notificato il recepimento (situazione al 24 luglio 2019).

64 Il Belgio, la Cechia, l'Estonia, la Lituania, la Polonia, il Portogallo, la Svezia e il Regno Unito hanno notificato un recepimento parziale. La Germania, l'Irlanda, la Grecia, la Spagna, Cipro, il Lussemburgo, l'Ungheria, i Paesi Bassi, la Romania, la Slovenia, la Slovacchia e la Finlandia non hanno notificato il recepimento (situazione al 24 luglio 2019).

65 La Lettonia, il Portogallo, la Slovenia e la Finlandia hanno notificato il recepimento parziale. La Grecia e la Spagna non hanno notificato il recepimento. Sebbene la Germania abbia notificato il recepimento integrale, la Commissione ritiene che tale recepimento non sia completo (situazione al 24 luglio 2019).

66 Il Belgio e l'Ungheria hanno recepito parzialmente la direttiva (situazione al 24 luglio 2019).

67 Belgio, Bulgaria, Cechia, Danimarca, Germania, Estonia, Irlanda, Spagna, Francia, Italia, Cipro, Lettonia, Lituania, Ungheria, Paesi Bassi, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia, Svezia e Regno Unito (situazione al 24 luglio 2019).

68 Si veda il piano d'azione contro la disinformazione (JOIN(2018) 36 final del 5.12.2018).

69 JOIN(2019) 12 final del 14.6.2019.

Il Consiglio europeo, nelle conclusioni del 21 giugno 2019[70], ha accolto con favore l'intenzione della Commissione di procedere a una valutazione approfondita dell'attuazione degli impegni assunti dalle piattaforme online e da altri firmatari nel quadro del **codice di buone pratiche sulla disinformazione**[71] e ha invitato la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza a valutare costantemente e a rispondere adeguatamente alla *"continua evoluzione delle minacce e [a]l crescente rischio di interferenze dolose e manipolazioni online, associati allo sviluppo dell'intelligenza artificiale e di tecniche di raccolta dati"*.

La Commissione e l'alto rappresentante faranno progredire i lavori in questo settore, in linea con le conclusioni del Consiglio europeo. Nel marzo 2019 la Commissione e l'alto rappresentante hanno istituito un **sistema di allarme rapido** tra le istituzioni dell'UE e gli Stati membri per facilitare la condivisione delle informazioni relative alle campagne di disinformazione e coordinare le risposte. La prima riunione dei punti di contatto degli Stati membri dopo le elezioni del Parlamento europeo si è svolta a Tallinn il 3 e 4 giugno 2019. Per rafforzare ulteriormente il sistema di allarme rapido, nell'autunno 2019 l'alto rappresentante e la Commissione, in stretta cooperazione con gli Stati membri, rivedranno il funzionamento di tale sistema. Svilupperanno inoltre una metodologia comune per l'analisi e lo smascheramento di campagne di disinformazione nonché partenariati più forti con partner internazionali come il G7 e la NATO.

I lavori proseguono anche in seno alla **rete europea di cooperazione in materia elettorale**[72] che ha tenuto una prima riunione il 7 giugno 2019 per fare il punto sulle elezioni del Parlamento europeo. Tali riflessioni e ulteriori contributi delle autorità nazionali competenti, dei partiti politici e delle piattaforme online serviranno da base per una relazione approfondita della Commissione sulle elezioni del Parlamento europeo che sarà adottata nell'ottobre 2019. Gli Stati membri hanno fatto ricorso alla rete per elezioni diverse da quelle del Parlamento europeo, il che mette in luce la più ampia utilità della rete per garantire l'integrità della democrazia nell'UE.

La Commissione continuerà inoltre a monitorare e promuovere l'attuazione degli impegni assunti dalle piattaforme nel **codice di buone pratiche sulla disinformazione**. Le relazioni fornite da Google, Twitter e Facebook nell'ambito del codice di buone pratiche mostrano che tutte le piattaforme hanno preso provvedimenti prima delle elezioni del

---

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf. L'invito del Consiglio europeo si basa sui contributi forniti dalla presidenza rumena del Consiglio, dalla Commissione e dall'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza in merito agli insegnamenti tratti per quanto riguarda la disinformazione e il garantire elezioni libere ed eque, compresa la comunicazione congiunta sull'attuazione del piano d'azione contro la disinformazione.

71 Il codice di buone pratiche è stato firmato dalle piattaforme online Facebook, Google e Twitter, Mozilla, dagli inserzionisti e dal settore pubblicitario nell'ottobre 2018 e stabilisce norme di autoregolamentazione per combattere la disinformazione. Esso mira a conseguire gli obiettivi fissati dalla comunicazione della Commissione dell'aprile 2018 dal titolo "Contrastare la disinformazione online: un approccio europeo" (COM/2018/236 final del 26.4.2018), stabilendo un'ampia gamma di impegni, dalla trasparenza nella pubblicità politica alla chiusura dei conti falsi e alla demonetizzazione dei vettori di disinformazione.

72 La rete europea di cooperazione in materia elettorale riunisce i punti di contatto delle omologhe reti nazionali delle autorità competenti per le questioni elettorali e delle autorità incaricate di monitorare e far rispettare le norme relative alle attività online pertinenti al contesto elettorale. La rete di cooperazione europea in materia elettorale serve a segnalare le minacce, a scambiare le migliori pratiche tra le reti nazionali, a discutere soluzioni comuni per individuare le sfide e a incoraggiare progetti e esercitazioni comuni tra le reti nazionali.

Parlamento europeo etichettando gli annunci pubblicitari di natura politica e rendendoli pubblicamente accessibili attraverso la consultazione di apposite biblioteche. Nel contempo, il gruppo dei regolatori europei per i servizi di media audiovisivi ha individuato margini di miglioramento[73]. In particolare, manca ancora l'accesso ai dati grezzi dettagliati necessari per un monitoraggio globale. Le piattaforme dovrebbero infine consentire alla comunità dei ricercatori un accesso effettivo ai dati, in linea con le norme in materia di protezione dei dati personali. Entro la fine dell'anno la Commissione effettuerà una valutazione globale dell'attuazione di tutti gli impegni assunti nell'ambito del codice di buone pratiche durante i suoi primi 12 mesi. Su tale base, la Commissione può prendere in considerazione ulteriori azioni, anche di natura normativa, per migliorare la risposta dell'UE a lungo termine alla disinformazione.

3. Preparazione e protezione

Rafforzare le difese e sviluppare la resilienza contro le minacce alla sicurezza è un aspetto importante dei lavori per la creazione di un'autentica ed efficace Unione della sicurezza. Tra questi figurano il sostegno della Commissione agli Stati membri e alle loro autorità locali per il rafforzamento della **protezione degli spazi pubblici**[74], il sostegno agli Stati membri per il rafforzamento della preparazione contro i **rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare**[75], l'attuazione dei due piani d'azione in questo settore e l'analisi delle esigenze di sviluppo, nel quadro di rescEU, di capacità di risposta[76]. Per quanto riguarda l'evoluzione delle minacce chimiche[77], la Commissione, in cooperazione con gli Stati membri e in consultazione con i partner internazionali, ha elaborato un elenco di sostanze chimiche estremamente problematiche in termini di uso improprio a fini terroristici. L'elenco UE funge da base per ulteriori attività volte a ridurre l'accessibilità a tali sostanze chimiche e per una collaborazione con i costruttori per migliorare le capacità di rilevamento.

---

73 Il gruppo dei regolatori europei per i servizi di media audiovisivi riunisce i responsabili o i rappresentanti ad alto livello degli organismi nazionali di regolamentazione indipendenti nel settore dei servizi audiovisivi, per fornire consulenza alla Commissione circa l'attuazione della direttiva dell'UE sui servizi di media audiovisivi (direttiva 2010/13/UE del 10 marzo 2010). Nella sua ultima riunione del 20 e 21 giugno 2019 a Bratislava, il gruppo ha presentato i risultati dei lavori svolti finora in materia di disinformazione, con particolare attenzione alle elezioni del Parlamento europeo del 2019 e ai relativi settori di messaggi pubblicitari di natura politica e di sensibilizzazione.

74 Si vedano le "Buone pratiche per le autorità pubbliche e gli operatori privati per rafforzare la sicurezza degli spazi pubblici", indicate nella diciottesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2019) 145 final del 20.3.2019). Queste si basano sul piano d'azione dell'ottobre 2017 per migliorare la protezione degli spazi pubblici (COM(2017) 612 final del 18.10.2017). Il 5 giugno 2019 si è svolta la terza riunione del Forum degli operatori del Forum dell'UE sulla protezione degli spazi pubblici. Ha riunito rappresentanti degli Stati membri dell'UE e operatori privati di spazi pubblici, rappresentati da 14 associazioni europee che coprono i settori ricettivo, degli spettacoli dal vivo, della musica e dell'intrattenimento, dei parchi di divertimento e delle attrazioni, dell'aviazione, dei trasporti ferroviari, dei centri commerciali, delle telecomunicazioni, dei servizi di sicurezza privati e dei produttori di apparecchiature di sicurezza.

75 In particolare attuando il piano d'azione dell'ottobre 2017 per rafforzare la preparazione contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare (COM (2017) 610 final del 18.10.2017).

76 Si veda l'articolo 12, paragrafo 2, della decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile, modificata dalla decisione (UE) 2019/420 del 13 marzo 2019.

77 Si vedano le azioni rafforzate contro le minacce chimiche indicate nella quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2018) 470 final del 13.6.2018).

Le tecnologie per gli aeromobili senza equipaggio consentono un'ampia gamma di operazioni possibili. Con un rapido sviluppo negli ultimi anni sul mercato dei sistemi aeromobili senza equipaggio destinati a fini militari, civili e amatoriali, i **droni** rappresentano un'opportunità, ma anche una crescente minaccia per la sicurezza delle infrastrutture critiche (compreso il trasporto aereo), degli spazi ed eventi pubblici, dei siti sensibili e delle persone. In Europa, i droni sono stati utilizzati per perturbare il traffico aereo e le operazioni di contrasto, sorvegliare infrastrutture critiche e praticare il contrabbando nelle carceri e oltre frontiera.

La Commissione sostiene gli Stati membri nella lotta alla crescente minaccia rappresentata dai droni per i cittadini e le funzioni fondamentali della società, senza volerne eliminare l'uso benefico, ad esempio nelle operazioni di risposta alle emergenze. Per attenuare il rischio dell'uso dannoso dei droni, la Commissione ha recentemente adottato **norme comuni a livello dell'UE sul funzionamento sicuro dei droni**[78], che comprendono disposizioni che impongono la registrazione degli operatori e consentono l'identificazione a distanza. Inoltre, la Commissione sostiene gli Stati membri monitorando le tendenze nell'evoluzione della minaccia rappresentata dai droni, finanziando i progetti di ricerca pertinenti e le misure di rafforzamento delle capacità e agevolando gli scambi tra gli Stati membri e gli altri portatori di interessi. Per intensificare tale sostegno, il 17 ottobre 2019 la Commissione organizzerà una conferenza internazionale ad alto livello per contrastare i rischi posti dai droni.

In risposta all'esigenza di avere una visione ampia della politica dell'UE per la **protezione delle infrastrutture critiche**[79], il 23 luglio 2019 la Commissione ha presentato una valutazione della direttiva sulle infrastrutture critiche europee[80] quale quadro giuridico per l'identificazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. Dalla valutazione è emerso che il contesto in cui operano le infrastrutture critiche in Europa è notevolmente mutato da quando la direttiva è entrata in vigore, compresi gli sviluppi legislativi in settori particolarmente interessati dalla direttiva, come l'energia[81], e che, essendo cambiato il panorama, le disposizioni della direttiva sono pertinenti solo in parte. Nel contempo, gli Stati membri hanno continuato a sostenere la politica dell'UE in materia di protezione delle infrastrutture critiche che rispetta la sussidiarietà e apporta un valore aggiunto.

4. Dimensione esterna

Data la natura transfrontaliera e globale della maggior parte delle minacce che incombono sulla nostra Unione, la cooperazione con le organizzazioni internazionali e i paesi partner al di fuori dell'UE è parte integrante dell'attività volta a conseguire un'autentica ed efficace Unione della sicurezza.

---

78 Regolamento di esecuzione (UE) 2019/947 della Commissione, del 24 maggio 2019, relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio (GU L 152 dell'11.6.2019, pag. 45).

79 La valutazione globale del 2017 della politica di sicurezza dell'UE (SWD(2017) 278 final del 26.7.2017) ha evidenziato la necessità di un'ampia visione della politica di protezione delle infrastrutture critiche dell'UE.

80 L'obiettivo della direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, è quello di rafforzare la protezione delle infrastrutture critiche dell'Unione europea.

81 In particolare il regolamento (UE) 2017/1938 del Parlamento europeo e del Consiglio, del 25 ottobre 2017, concernente misure volte a garantire la sicurezza dell'approvvigionamento di gas e il regolamento (UE) 2019/941 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sulla preparazione ai rischi nel settore dell'energia elettrica.

L'effetto leva dei benefici della cooperazione multilaterale contribuisce notevolmente a tale attività e comprende la cooperazione tra l'UE e l'ONU, recentemente rafforzata con il **quadro in materia di antiterrorismo tra le Nazioni Unite e l'Unione europea** firmato a New York il 24 aprile 2019, in occasione del secondo dialogo politico ad alto livello ONU-UE sull'antiterrorismo[82]. Il quadro promuove la cooperazione in materia di rafforzamento delle capacità per contrastare il terrorismo e prevenire e combattere l'estremismo violento in Africa, nel Medio Oriente e in Asia. Il quadro individua le aree per la cooperazione ONU-UE e le priorità fino al 2020.

La **cooperazione in materia di sicurezza con i Balcani occidentali** rappresenta una particolare priorità regionale, con l'attuazione di una serie di azioni prioritarie in materia di sicurezza individuate nella strategia per i Balcani occidentali del 2018[83]. A tal fine, il 4 aprile 2019 la Commissione ha organizzato la prima riunione della task force interagenzie per i Balcani occidentali, che ha permesso ai rappresentanti di sette agenzie dell'UE di condividere le loro esperienze e di rafforzare la cooperazione operativa con i partner della regione, anche per quanto riguarda la lotta contro la criminalità organizzata, il terrorismo, le armi da fuoco, la droga, il traffico di migranti e la tratta di esseri umani. Sono stati avviati sondaggi sui rischi ibridi con tutti i sei paesi dei Balcani occidentali. Un altro esempio concreto della cooperazione con la regione è l'accordo tra l'UE e l'Albania sullo status della guardia di frontiera e costiera europea, entrato in vigore il 1º maggio 2019, che è stato rapidamente seguito dall'invio delle squadre dell'Agenzia europea della guardia di frontiera e costiera alla frontiera con la Grecia. Si tratta del primo accordo di questo tipo concluso con un paese terzo e del primo invio delle squadre in un paese terzo. Accordi analoghi dovrebbero essere presto firmati con altri paesi della regione.

Inoltre, nel luglio 2019 è stato inviato in Albania un ufficiale di collegamento Europol per assistere ulteriormente le autorità albanesi nei loro sforzi per prevenire e combattere la criminalità organizzata. Per intensificare la lotta contro il traffico di armi da fuoco, il 27 giugno 2019 la Commissione ha presentato una valutazione del piano d'azione 2015-2019 **sul traffico di armi da fuoco** tra l'UE e la regione dell'Europa sudorientale[84]. La valutazione dimostra il valore aggiunto della cooperazione, ma sottolinea che sono necessari ulteriori sforzi, ad esempio l'istituzione di centri di coordinamento nazionali efficienti in materia di armi da fuoco o l'armonizzazione della raccolta di informazioni e la presentazione di relazioni sui sequestri di armi da fuoco.

L'UE attribuisce pari priorità allo sviluppo della **cooperazione con i paesi del Medio Oriente e dell'Africa settentrionale** nel settore della sicurezza. L'UE ha avviato un dialogo sulla sicurezza con la Tunisia e l'Algeria. L'UE e la Tunisia hanno tenuto il terzo dialogo sulla sicurezza e la lotta al terrorismo il 12 giugno a Tunisi, mentre il 12 novembre 2018 si è svolto ad Algeri il secondo dialogo UE-Algeria sulla sicurezza e la lotta al terrorismo. Sono in corso colloqui con il Marocco per avviare un dialogo strutturato sulla sicurezza, a seguito del recente Consiglio di associazione del 27 giugno, in cui l'UE e il Marocco hanno riconosciuto l'importanza di approfondire la cooperazione in materia di sicurezza per far fronte alle sfide comuni. Parallelamente sono in corso discussioni per sviluppare un dialogo strutturato sulla

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf
83 COM(2018) 65 final del 6.2.2018.
84 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_en.pdf

sicurezza con l'Egitto, come confermato anche dall'ultimo incontro tra alti funzionari UE-Egitto tenutosi il 10 luglio al Cairo.

Sulla base del mandato conferitole dal Consiglio, la Commissione ha avviato colloqui informali con la maggior parte dei paesi **del Medio Oriente e dell'Africa settentrionale** per avviare negoziati formali per un accordo internazionale per lo scambio di dati personali tra l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (**Europol**) e le pertinenti autorità competenti dei paesi **del Medio Oriente e dell'Africa settentrionale** al fine di combattere le forme gravi di criminalità e il terrorismo. In tale contesto, la Commissione sta anche promuovendo la conclusione di accordi di lavoro direttamente tra Europol e le autorità partner nei paesi **del Medio Oriente e dell'Africa settentrionale**, al fine di fornire un quadro formale per una cooperazione regolare a livello strategico.

L'UE e gli **Stati Uniti** sono uniti da uno stretto partenariato strategico per far fronte alle minacce comuni e rafforzare la sicurezza. Nella riunione ministeriale "Giustizia e affari interni" del 19 giugno 2019, l'UE e gli Stati Uniti hanno ribadito che la lotta al terrorismo rientra tra le loro principali priorità. Per quanto riguarda l'accordo UE-USA relativo al codice di prenotazione[85], entrambe le parti ne hanno ribadito l'importanza e si sono impegnate ad avviare una valutazione congiunta nel settembre 2019 per esaminarne l'attuazione, in linea con le disposizioni dell'accordo stesso. Entrambe le parti si sono inoltre impegnate a intensificare i loro sforzi congiunti nella lotta al terrorismo, anche ampliando la condivisione delle informazioni raccolte in zone di combattimento per utilizzo nelle indagini e azioni penali.

Per intensificare tale cooperazione, il 10 luglio 2019 la Commissione, in collaborazione con il coordinatore antiterrorismo dell'UE, ha ospitato a Bruxelles un seminario ad alto livello sulle informazioni del campo di battaglia. Tale seminario ha riunito funzionari di alto livello dei ministeri degli Stati membri della Difesa, dell'Interno e della Giustizia, degli Stati Uniti, di Europol, Eurojust e rappresentanti delle organizzazioni internazionali per scambiarsi opinioni sull'uso delle informazioni del campo di battaglia e riflettere insieme sulle sfide procedurali, giuridiche e operative cui sono attualmente confrontati per cercare di individuare i terroristi e consegnarli alla giustizia. L'UE e gli Stati Uniti hanno inoltre tenuto a Bruxelles, il 14-15 maggio 2019, un dialogo per lo sviluppo delle capacità chimiche, biologiche, radiologiche e nucleari per coordinare gli sforzi volti a ridurre le minacce derivanti dalle armi di distruzione di massa e rafforzare la sicurezza chimica, biologica, radiologica e nucleare a livello globale.

L'**accordo tra l'UE e gli Stati Uniti sul programma di controllo delle transazioni finanziarie dei terroristi**[86] è in vigore dal 2010 e disciplina il trasferimento e il trattamento di dati a fini di individuazione, controllo e azione penale nei confronti di terroristi e reti terroristiche. L'accordo contiene garanzie che assicurano la protezione dei dati dei cittadini dell'UE e prevede verifiche congiunte periodiche delle disposizioni riguardanti le salvaguardie, i controlli e la reciprocità. In una relazione di valutazione periodica[87] pubblicata il 22 luglio 2019 la Commissione ha osservato che è certa che l'accordo, comprese le sue salvaguardie e controlli essenziali, sia correttamente applicato. La Commissione si compiace della costante trasparenza delle autorità statunitensi nella condivisione delle informazioni,

[85] GU L 215 dell'11.8.2012, pag. 5.
[86] GU L 195 del 27.7.2010, pag. 5.
[87] COM(2019) 342 final del 22.7.2019.

illustrando in tal modo il valore del programma di controllo delle transazioni finanziarie dei terroristi nei nostri sforzi congiunti di lotta al terrorismo. Le informazioni fornite nell'ambito dell'accordo sono state utili per portare avanti indagini specifiche riguardanti gli attentati terroristici sul territorio europeo, compresi gli attentati a Stoccolma, Barcellona e Turku nel 2017. Gli Stati membri ed Europol hanno aumentato il loro uso del meccanismo e i dati del programma di controllo delle transazioni finanziarie dei terroristi hanno generato un numero di indizi investigativi sette volte più elevato rispetto al precedente periodo di riferimento. La prossima verifica congiunta dell'accordo è prevista per il 2021.

Per quanto riguarda la cooperazione internazionale sullo scambio di **dati del codice di prenotazione a fini di lotta al terrorismo e alle forme gravi di criminalità**, l'UE e il Canada, in occasione del 17º vertice UE-Canada svoltosi a Montreal il 17 e 18 luglio 2019, hanno espresso compiacimento per la conclusione dei negoziati per un nuovo accordo sul codice di prenotazione. Sebbene il Canada abbia fatto presente il proprio obbligo di esame giuridico, le parti si sono impegnate, fatto salvo tale esame, a concludere l'accordo quanto prima riconoscendo il ruolo fondamentale di tale accordo per rafforzare la sicurezza e garantire al tempo stesso la tutela della vita privata e la protezione dei dati personali. Per quanto riguarda l'accordo vigente tra l'UE e l'Australia sul codice di prenotazione dei passeggeri[88], nell'agosto 2019 si terrà una visita di una squadra dell'UE a Canberra nell'ambito del riesame congiunto e della valutazione congiunta dell'accordo.

La Commissione sta inoltre collaborando con gli Stati membri in seno al Consiglio per definire la posizione dell'UE in vista della 40ª sessione dell'assemblea dell'**Organizzazione dell'aviazione civile internazionale (ICAO)** che si terrà dal 24 settembre al 4 ottobre 2019. L'assemblea stabilirà una direzione politica e fornirà istruzioni al consiglio dell'ICAO sui lavori tecnici relativi alle norme ICAO per il trattamento dei dati del codice di prenotazione. Il Consiglio ha approvato un documento informativo preparato dalla Commissione che illustra la posizione dell'Unione in merito ai principi fondamentali su cui dovrebbe basarsi qualsiasi futura norma internazionale sui dati del codice di prenotazione. Il documento informativo sarà presentato all'organo per rispetto dei membri diversi dagli Stati membri dell'UE.

VI. CONCLUSIONI

Grazie alla stretta cooperazione tra il Parlamento europeo, il Consiglio, gli Stati membri e la Commissione, l'UE negli ultimi anni ha compiuto notevoli progressi nel lavoro congiunto per realizzare un'autentica ed efficace Unione della sicurezza, concordando una serie di iniziative legislative prioritarie. Inoltre gli Stati membri, con il sostegno della Commissione, stanno attuando una serie di misure operative non legislative per rafforzare la sicurezza per tutti i cittadini. Nel contempo, una serie di iniziative prioritarie pendenti nel settore dell'Unione della sicurezza richiedono un ulteriore intervento dei colegislatori per far fonte alle minacce immediate. La Commissione invita il Parlamento europeo e il Consiglio ad adottare le misure necessarie per raggiungere rapidamente un accordo sulle proposte legislative per contrastare la propaganda terroristica e la radicalizzazione online, rafforzare la cibersicurezza, facilitare l'accesso alle prove elettroniche e completare il lavoro su sistemi di informazione più solidi e intelligenti per la sicurezza, le frontiere e la gestione della migrazione.

[88] GU L 186 del 14.7.2012, pag. 4.

La Commissione invita gli Stati membri ad attuare rapidamente e integralmente tutti gli atti legislativi adottati nel settore dell'Unione della sicurezza per garantirne gli effetti benefici. Invita inoltre gli Stati membri a proseguire e intensificare il lavoro fondamentale sulle misure pratiche per rafforzare la sicurezza delle infrastrutture digitali, contrastare la disinformazione e altre minacce basate sull'uso di strumenti informatici, aumentare la preparazione e la protezione e potenziare la cooperazione con i partner al di fuori dell'Unione per far fronte alle minacce comuni. Nel loro insieme, queste misure rafforzano la sicurezza di tutti i cittadini.