Consiglio
dell'Unione europea

Bruxelles, 25 marzo 2019
(OR. en)

7434/19

JAI 331
COSI 57
FRONT 120
ASIM 38
DAPIX 117
ENFOPOL 122
SIRIS 57
VISA 70
FAUXDOC 26
COPEN 128
CYBER 105
DATAPROTECT 108
CT 29
JAIEX 49
EF 124

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	21 marzo 2019
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2019) 145 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO Diciottesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza

Si trasmette in allegato, per le delegazioni, il documento COM(2019) 145 final.

All.: COM(2019) 145 final

COMMISSIONE
EUROPEA

Bruxelles, 20.3.2019
COM(2019) 145 final

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

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

{SWD(2019) 140 final}

I. INTRODUZIONE

Il presente documento è la diciottesima relazione sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza. Esso verte sugli sviluppi attinenti a due pilastri principali: affrontare il terrorismo e la criminalità organizzata e i relativi mezzi di sostegno, e rafforzare le difese e creare resilienza contro tali minacce.

In vista delle elezioni del Parlamento europeo del maggio 2019, la presente relazione sottolinea l'importante lavoro svolto a vari livelli per affrontare e prevenire le minacce informatiche e la disinformazione nel contesto elettorale. In risposta all'invito del Consiglio europeo a favore di misure volte a proteggere i sistemi democratici dell'Unione e a combattere la disinformazione nel periodo precedente le prossime elezioni, l'Unione ha compiuto notevoli progressi verso un'azione più coordinata in materia di resilienza elettorale. Tuttavia, dato il tempo a disposizione per garantire la preparazione dell'Unione prima che gli elettori europei si rechino alle urne nel maggio 2019, la Commissione invita tutti i soggetti coinvolti - le autorità governative, i partiti politici, e in particolare le piattaforme online - , a raddoppiare gli sforzi per aumentare la resilienza elettorale intesa a contrastare la disinformazione. In vista del prossimo Consiglio europeo del 21 e 22 marzo 2019, che discuterà i progressi in questo settore, la Commissione invita inoltre gli Stati membri a rafforzare il loro coordinamento per contrastare la disinformazione e garantire che le elezioni del Parlamento europeo siano tutelate.

L'UE ha compiuto notevoli progressi nei lavori svolti per realizzare un'autentica ed efficace Unione della sicurezza, e ha raggiunto accordi su una serie di iniziative legislative prioritarie che rafforzeranno la sicurezza per tutti i cittadini. Negli ultimi mesi[1], il Parlamento europeo e il Consiglio hanno raggiunto un accordo sull'interoperabilità tra i sistemi di informazione dell'UE relativi alla sicurezza, alle frontiere e alla gestione della migrazione e su nuove norme dell'UE per ridurre il margine di manovra dei terroristi e dei criminali, rendendo loro più difficile accedere ai precursori di esplosivi, finanziare le proprie attività e viaggiare senza essere individuati. In 15 delle 22 iniziative legislative presentate dalla Commissione nel settore dell'Unione della sicurezza (cfr. l'elenco di tutte le iniziative in materia nell'*Allegato I*), è stato raggiunto l'accordo: l'UE sta quindi ottenendo risultati in quello che è un settore prioritario comune per il Parlamento europeo, il Consiglio e la Commissione[2].

È necessario tuttavia compiere ulteriori sforzi. In particolare, nell'ambito dell'attuale mandato legislativo, i colegislatori devono affrontare l'urgente minaccia rappresentata dai contenuti terroristici online, raggiungendo un accordo sulla proposta della Commissione. Il Parlamento europeo e il Consiglio devono inoltre raggiungere un accordo sulla proposta della Commissione relativa a un rafforzamento della guardia di frontiera e costiera europea per aumentare la sicurezza attraverso una maggiore protezione delle frontiere esterne dell'Unione.

I tragici avvenimenti di Christchurch, in Nuova Zelanda, del 15 marzo 2019 mostrano che la minaccia terroristica resta un pericolo chiaro e presente, che essa sia alimentata da estremismo

---

[1] Questo fa seguito ai progressi compiuti precedentemente nelle attività verso un'autentica ed efficace Unione della sicurezza. Per una panoramica completa, si vedano le precedenti relazioni sul suo stato di avanzamento: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

[2] Si veda la dichiarazione comune sulle priorità legislative dell'UE per il 2018-2019: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

di estrema destra o da altre ideologie estremiste. Le difficoltà incontrate nel cercare di rimuovere contenuti in diretta streaming dalle piattaforme Internet e di impedirne la ricomparsa mette ulteriormente in evidenza l'importanza fondamentale della proposta della Commissione sui contenuti terroristici online. È essenziale che i colegislatori trovino urgentemente un accordo sulle norme proposte per la rimozione dei contenuti terroristici online. È parimenti importante, per la lotta contro il terrorismo in tutte le sue forme, che tutti gli Stati membri attuino pienamente la legislazione adottata dall'UE, in particolare in risposta agli attacchi terroristici in Europa, per ridurre il margine di manovra dei terroristi. Si tratta segnatamente delle direttive sulla lotta contro il terrorismo e sul controllo dell'acquisizione e della detenzione di armi. La Commissione lavora attivamente anche nell'ambito della lotta contro l'estremismo, con l'adozione di misure rilevanti contro l'illecito incitamento all'odio online, contro l'odio anti-islamico e contro l'antisemitismo.

La presente relazione illustra anche i progressi compiuti nell'attuazione di altri fascicoli prioritari in materia di sicurezza, in particolare per quanto riguarda le misure a sostegno della protezione degli spazi pubblici. L'attuazione completa e corretta delle misure concordate riveste la massima priorità per garantire i pieni vantaggi di un'autentica ed efficace Unione della sicurezza. La Commissione sta attivamente sostenendo gli Stati membri, anche con finanziamenti e facilitando lo scambio delle migliori prassi. Ove necessario, la Commissione inoltre si avvale appieno dei poteri conferitile dai trattati per l'attuazione del diritto dell'Unione, ricorrendo anche, se opportuno, al procedimento d'infrazione.

La commemorazione della 15ª Giornata europea in memoria delle vittime del terrorismo, l'11 marzo 2019, quindici anni dopo gli attentati di Madrid dell'11 marzo 2004 e tre anni dopo gli attacchi mortali di Bruxelles e Zaventem del 22 marzo 2016, è il contesto della presente relazione. Fornire sostegno alle vittime degli attentati terroristici è una parte importante del lavoro verso un'autentica ed efficace Unione della sicurezza. Per intensificare tale sostegno, il 31 gennaio 2019 la Commissione ha adottato una decisione relativa al finanziamento del progetto pilota "Creazione di un centro di competenza dell'UE per le vittime del terrorismo"[3]. Tale centro fungerà da polo di competenze e da piattaforma per gli operatori che si occupano di queste persone.

La Commissione accoglie con favore il contributo della relazione del Parlamento europeo sulle conclusioni e raccomandazioni della commissione speciale sul terrorismo[4] quale valido contributo all'attività congiunta per la realizzazione di un'autentica ed efficace Unione della sicurezza.

II. ATTUAZIONE DELLE PRIORITÀ LEGISLATIVE

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

Lo scambio di informazioni è un aspetto centrale del sostegno che l'UE fornisce alle autorità nazionali nella lotta contro il terrorismo e le forme gravi di criminalità. A tale riguardo, l'interoperabilità fra i sistemi di informazione a livello dell'UE segna un cambiamento radicale del modo in cui i dati vengono forniti alle autorità nazionali, garantendo che essi siano esatti e completi. I colegislatori hanno raggiunto un accordo politico sulle relative proposte legislative

[3] C (2019) 636 del 31.1.2019.

[4] Risoluzione del Parlamento europeo del 12 dicembre 2018 sulle conclusioni e raccomandazioni della commissione speciale sul terrorismo (2018/2044(INI)).

prioritarie per realizzare l'**interoperabilità dei sistemi di informazione dell'UE** per la sicurezza, le frontiere e la gestione della migrazione[5]. Le misure proposte faranno sì che i sistemi di informazione dell'UE lavorino insieme in un modo più intelligente e mirato, nel pieno rispetto dei diritti fondamentali. Utilizzando al meglio i dati esistenti, l'interoperabilità colmerà le lacune informative e gli angoli morti aiutando a individuare le identità multiple e a contrastare le frodi d'identità. Una volta che i colegislatori avranno formalmente adottato le nuove norme, la Commissione sarà pronta a sostenere gli Stati membri nella loro attuazione. È necessaria una stretta cooperazione con le agenzie dell'UE e con tutti gli Stati membri e i paesi associati Schengen 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. In tale ottica, il 5 marzo 2019 si è svolto un primo seminario con gli esperti degli Stati membri per avviare un processo di coordinamento efficace.

In questa fase, la futura architettura dei sistemi di informazione interoperabili dell'UE comprenderà il **sistema di informazione Schengen**[6] rafforzato, l'esistente **sistema di informazione visti**[7], la recentemente concordata estensione del **sistema europeo di informazione sui casellari giudiziali**[8] ai cittadini di paesi terzi, e i recenti **sistema di ingressi/uscite dell'UE**[9] e **sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)**[10].

Nell'ambito dell'attuazione tecnica del sistema europeo di informazione e autorizzazione ai viaggi, il 7 gennaio 2019 la Commissione ha presentato una proposta contenente modifiche tecniche al relativo regolamento[11]. Le modifiche proposte riguardano gli atti giuridici relativi ai sistemi di informazione dell'UE che il sistema europeo di informazione e autorizzazione ai viaggi interrogherà nell'ambito della valutazione dei rischi in materia di sicurezza o migrazione irregolare posti dai cittadini di paesi terzi esenti dall'obbligo di visto, effettuata prima del loro viaggio nello spazio Schengen. Le modifiche proposte sono necessarie per realizzare pienamente il sistema europeo di informazione e autorizzazione ai viaggi. 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**[12]. Tale proposta prevede un più approfondito controllo dei

---

5 COM (2017) 793 final del 12.12.2017, COM (2017) 794 final del 12.12.2017, COM (2018) 478 final del 13.6.2018, COM (2018) 480 final del 13.6.2018. L'accordo politico raggiunto il 5 febbraio 2019 è stato approvato dal comitato dei rappresentanti permanenti del Consiglio il 13 febbraio 2019 e dalla commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo il 19 febbraio 2019.

6 Regolamento (UE) 2018/1860 del 28.11.2018, regolamento (UE) 2018/1861 del 28.11.2018) regolamento (UE) 2018/1862 del 28.11.2018.

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

8 I colegislatori hanno raggiunto un accordo politico su questa proposta prioritaria l'11 dicembre 2018 (COM (2017) 344 final del 29.6.2017)). Il comitato dei rappresentanti permanenti del Consiglio ha approvato l'accordo il 19 dicembre 2018, e il Parlamento europeo lo ha confermato in seduta plenaria l'11 marzo 2019.

9 Regolamento (UE) 2017/2226 del 30.11.2017.

10 Regolamento (UE) 2018/1240 del 12.9.2018 e regolamento (UE) 2018/1241 del 12.9.2018.

11 COM (2019) 4 final del 7.1.2019.

12 COM (2018) 302 final del 16.5.2018.

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 prossimo Parlamento europeo.

Nel maggio 2016 la Commissione ha proposto di ampliare l'ambito di applicazione di **Eurodac**[13] 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[14] e con la comunicazione della Commissione del 6 marzo 2019 sullo stato di attuazione dell'agenda europea sulla migrazione[15], la Commissione invita i colegislatori a procedere senza indugio all'adozione della proposta. Tale adozione consentirà 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 riguardante **Eurodac**, in merito alla quale è prossimo un accordo, prima delle elezioni del Parlamento europeo (*priorità della dichiarazione comune*);
- a portare avanti il lavoro volto a raggiungere rapidamente un accordo sulle modifiche tecniche proposte, necessarie per istituire il **sistema europeo di informazione e autorizzazione ai viaggi**.

2. Rafforzare la sicurezza attraverso una migliore gestione delle frontiere esterne

Una solida protezione delle frontiere esterne è una condizione essenziale per la sicurezza nello spazio di libera circolazione senza controlli alle frontiere interne. Si tratta di un compito che spetta agli Stati membri, che devono garantire la gestione delle loro frontiere esterne sia nel proprio interesse sia nell'interesse comune di tutti, con l'aiuto della **guardia di frontiera e costiera europea**. In risposta alle conclusioni del Consiglio europeo del giugno 2018[16], nel settembre dello stesso anno la Commissione ha proposto di potenziare le capacità della guardia di frontiera e costiera europea[17]: si tratterebbe di portare l'Agenzia a un nuovo livello operativo dotandola di un corpo permanente di 10 000 guardie di frontiera con poteri esecutivi e attrezzature proprie, nel pieno rispetto dei diritti fondamentali e della sovranità degli Stati membri.

I lavori legislativi sulla proposta procedono bene e i negoziati tra i colegislatori sono entrati nella fase cruciale. Il Parlamento europeo ha adottato il suo mandato negoziale l'11 febbraio 2019, mentre il Consiglio ha ricevuto il suo mandato il 20 febbraio 2019. Il 27 febbraio 2019

13 COM (2016) 272 final del 4.5.2016.
14 https://www.consilium.europa.eu/en/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/.
15 COM (2019) 126 final del 6.3.2019.
16 https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.
17 COM (2018) 631 final del 12.9.2018.

e il 12 marzo 2019 si sono svolte due riunioni trilaterali. La Commissione accoglie con favore e sostiene i progressi compiuti in merito a questo dossier prioritario, dimostrando che tutte le istituzioni sono impegnate nell'adozione della proposta in questione prima delle elezioni del Parlamento europeo del 2019.

Al fine di rafforzare la sicurezza attraverso una migliore gestione delle frontiere esterne, la Commissione invita il Parlamento europeo e il Consiglio:

- ad adottare la proposta legislativa volta a rafforzare la **guardia di frontiera e costiera europea** nel corso del presente mandato del Parlamento europeo (*iniziativa legata allo Stato dell'Unione 2018*).

3. Prevenire la radicalizzazione

Combattere i contenuti terroristici online rimane una sfida fondamentale nella lotta al terrorismo e nella prevenzione della radicalizzazione. Contenuti di tale tipo hanno svolto un ruolo nella maggior parte degli attentati perpetrati sul territorio europeo negli ultimi due anni, attraverso l'istigazione a commettere un attacco, le istruzioni su come realizzarlo o l'esaltazione dei risultati mortali. Al fine di affrontare il pericolo chiaro e attuale rappresentato da tali contenuti, il discorso sullo stato dell'Unione 2018 del Presidente Juncker era accompagnato da una proposta[18] di regolamento relativo ai **contenuti terroristici online**, che definisce un quadro giuridico per prevenire l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online. Pur garantendo pienamente la libertà di espressione e altri diritti fondamentali, è essenziale che le future norme prevedano misure efficaci per rimuovere i contenuti terroristici online il più rapidamente possibile, dato che i potenziali danni causati da tali contenuti aumentano ogni ora che questo materiale resta online.

Mentre il Consiglio ha adottato il suo mandato negoziale nel dicembre 2018, il Parlamento europeo sta ancora lavorando, e si spera adotti il suo mandato negoziale nel corso di marzo 2019[19]. La Commissione invita entrambi i colegislatori a raggiungere un accordo sulla normativa proposta nel corso del presente mandato del Parlamento europeo, data l'importanza fondamentale di un quadro regolamentare dell'UE per la rimozione dei contenuti terroristici online con regole e garanzie chiare.

Parallelamente, la Commissione continua a fornire sostegno agli Stati membri nei loro sforzi volti a **prevenire la radicalizzazione**. Un apposito meccanismo di cooperazione dell'UE, che riunisce rappresentanti nazionali, contribuisce a garantire che il sostegno a livello dell'UE risponda alle esigenze degli Stati membri[20]. Tra gli esempi recenti figurano una conferenza sulle "Città dell'UE contro la radicalizzazione", organizzata congiuntamente con il Comitato delle regioni il 26 febbraio 2019. Il 13 marzo 2019 la Commissione ha organizzato una riunione di esperti con i responsabili politici nazionali al fine di individuare misure pratiche

---

18 COM (2018) 640 final del 12.9.2018.

19 La commissione per il mercato interno e la protezione dei consumatori del Parlamento europeo ha votato il suo parere il 4 marzo 2019. La commissione per la cultura e l'istruzione del Parlamento europeo ha votato la sua relazione l'11 marzo 2019. La commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo dovrebbe votare la sua relazione il 21 marzo 2019..

20 Le esigenze degli Stati membri relative alla prevenzione della radicalizzazione sono state individuate, per la prima volta, nei cosiddetti orientamenti strategici per le azioni di prevenzione dell'UE per il 2019. Gli orientamenti strategici sono consultabili al seguente indirizzo: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

per sostenere ulteriormente i servizi penitenziari e di sospensione condizionale. I risultati di questo lavoro faranno parte di un manuale che la rete di sensibilizzazione al problema della radicalizzazione sta preparando in materia di riabilitazione e reinserimento di terroristi, di combattenti stranieri dopo il loro rientro e di soggetti radicalizzati in carcere (cfr. anche la sezione IV.4 sulla dimensione esterna).

Al fine di prevenire la radicalizzazione, la Commissione invita il Parlamento europeo:

- ad adottare, in via prioritaria, il mandato negoziale sulla proposta legislativa volta a prevenire la diffusione di **contenuti terroristici online**, in modo che i colegislatori raggiungano un accordo sulla normativa durante l'attuale mandato del Parlamento europeo (*iniziativa legata allo Stato dell'Unione 2018*).

4. Rafforzare la cibersicurezza

Le classiche minacce informatiche ai sistemi e ai dati sono sempre in crescita. Nel 2018 si è registrato un aumento delle attività di soggetti malintenzionati, con una diversità di obiettivi e di persone offese. La lotta alla criminalità informatica e il rafforzamento della cibersicurezza rimangono pertanto una priorità per l'azione dell'UE. L'Unione europea ha compiuto progressi tangibili nel rafforzamento della cibersicurezza, attuando le azioni definite nella comunicazione congiunta del settembre 2017[21] dal titolo "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE".

Il 12 marzo 2019, la plenaria del Parlamento europeo ha confermato l'accordo politico raggiunto dai colegislatori in merito al **regolamento sulla cibersicurezza**. Con l'entrata in vigore prevista nel maggio 2019, tale regolamento aumenterà le capacità nel settore della cibersicurezza e la preparazione degli Stati membri e delle imprese. Esso istituirà un quadro dell'UE in materia di certificazione della cibersicurezza per i prodotti, i sistemi e i servizi delle tecnologie dell'informazione e della comunicazione. Accrescerà inoltre la collaborazione e il coordinamento tra Stati membri e istituzioni, agenzie e organismi dell'UE, in particolare l'agenzia rinominata Agenzia dell'Unione europea per la cibersicurezza.

Ulteriori progressi sono tuttavia necessari in merito alla proposta della Commissione del settembre 2018 riguardante il **Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento**[22]. 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. Il Parlamento europeo e il Consiglio hanno adottato i loro mandati negoziali il 13 marzo 2019. La prima riunione trilaterale ha anch'essa avuto luogo il 13 marzo 2019. La Commissione invita i colegislatori a raggiungere rapidamente un accordo sulla normativa proposta.

L'UE ha compiuto progressi significativi verso una maggiore operatività della **risposta diplomatica comune dell'UE alle attività informatiche dolose** (il "pacchetto di strumenti della diplomazia informatica"), in reazione all'invito del Consiglio europeo[23] di proseguire i lavori sulla capacità di risposta agli attacchi informatici e di deterrenza per mezzo di misure restrittive. L'8 marzo 2019, l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e la Commissione hanno presentato una proposta congiunta di regolamento del

21 JOIN (2017) 450 final del 13.9.2017.
22 COM (2018) 630 final del 12.9.2018.
23 Si vedano le conclusioni del Consiglio europeo di giugno 2018 e di ottobre 2018.

Consiglio concernente misure restrittive per contrastare gli attacchi informatici che minacciano l'Unione o gli Stati membri. La Commissione e l'Alto rappresentante chiedono la rapida adozione della proposta in questione per rafforzare la resilienza dell'Unione contro gli attacchi informatici.

Al fine di rafforzare la cibersicurezza, la Commissione e l'Alto rappresentante invitano il Consiglio:

- ad adottare il regolamento del Consiglio concernente **misure restrittive per contrastare gli attacchi informatici** che minacciano l'Unione o gli Stati membri.

5. Ridurre il margine di manovra dei terroristi

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, finanziare le proprie attività e viaggiare senza essere individuati.

Il 14 febbraio 2019 il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sulla proposta di regolamento relativo alle **restrizioni all'immissione sul mercato e all'uso di precursori di esplosivi**[24]. Una volta applicabile il regolamento apporterà miglioramenti significativi all'attuale quadro legislativo, limitando l'accesso ai precursori di esplosivi pericolosi che potrebbero essere utilizzati impropriamente per costruire ordigni artigianali. Il regolamento colmerà le lacune in materia di sicurezza adottando misure quali il divieto di sostanze chimiche supplementari, controlli obbligatori nei casellari giudiziali delle persone che chiedono il rilascio di una licenza per l'acquisto di sostanze soggette a restrizioni, e chiarendo che le regole previste per gli operatori economici si applicano anche alle imprese che operano online.

Inoltre, nell'ambito degli sforzi volti a combattere il finanziamento del terrorismo, i colegislatori hanno raggiunto un accordo sulla proposta di direttiva per **agevolare l'uso di informazioni finanziarie e di altro tipo** a fini di prevenzione, accertamento, indagine o perseguimento di reati gravi[25]. Una volta adottata e attuata formalmente, la direttiva accorderà a specifiche autorità di contrasto e uffici per il recupero dei beni accesso diretto alle informazioni sui conti bancari contenute nei registri nazionali centralizzati dei conti bancari. La direttiva potenzierà inoltre la cooperazione tra le unità di informazione finanziaria e le autorità di contrasto nazionali e faciliterà l'accesso di Europol alle informazioni finanziarie.

Sulla base di ciò, la Commissione rifletterà ancora sulla cooperazione tra le unità di informazione finanziaria dei vari Stati membri, anche nell'ambito della prossima relazione sulla cooperazione tra le unità di informazione finanziaria, come previsto dalla quinta direttiva antiriciclaggio[26]. Inoltre, come richiesto sempre dalla quinta direttiva antiriciclaggio, la Commissione sta valutando gli aspetti relativi alla potenziale interconnessione fra i registri

---

24 COM (2018) 209 final del 17.4.2018.

25 I colegislatori hanno raggiunto un accordo politico sulla proposta della Commissione il 12 febbraio 2019 (COM (2018) 213 final del 17.4.2018). Tale accordo è stato approvato dal comitato dei rappresentanti permanenti del Consiglio il 20 febbraio 2019 e dalla commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo il 26 febbraio 2019.

26 L'articolo 65, paragrafo 2, della direttiva (UE) 2018/843 del 19.6.2018 stabilisce che entro il 1º giugno 2019 la Commissione valuta il quadro per la cooperazione delle unità di informazione finanziaria con i paesi terzi nonché gli ostacoli e le opportunità per migliorare la cooperazione tra le unità di informazione finanziaria nell'Unione, inclusa la possibilità di istituire un meccanismo di coordinamento e supporto.

nazionali centralizzati dei conti bancari e i sistemi di reperimento dei dati nell'UE. La Commissione sta inoltre esaminando misure di confisca non basate su condanne nell'Unione. Infine, e anche in risposta ad una richiesta del Parlamento europeo[27], la Commissione continuerà a valutare la necessità, la fattibilità tecnica e la proporzionalità di misure aggiuntive per tracciare il finanziamento del terrorismo nell'UE.

Nell'ambito dei lavori volti a contrastare le frodi documentali, il 19 febbraio 2019 i colegislatori hanno raggiunto un accordo provvisorio sulla proposta di regolamento per rafforzare la **sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno**[28], in modo che non possano essere utilizzati in modo fraudolento da criminali e terroristi. La commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo ha confermato tale accordo l'11 marzo 2019. Una volta adottato, il regolamento introdurrà elementi minimi di sicurezza per le carte di identità, compresi identificatori biometrici (un'immagine del volto e due impronte digitali) su un microchip senza contatto. Ciò migliorerà significativamente la sicurezza delle carte d'identità nazionali e dei titoli di soggiorno, rendendo più difficile per i terroristi e altri criminali l'uso improprio o la falsificazione di tali documenti per accedere o spostarsi nell'UE. Documenti d'identità più sicuri contribuiranno a rafforzare la gestione delle frontiere esterne dell'UE. Al tempo stesso, documenti più sicuri e affidabili agevoleranno ai cittadini dell'UE l'esercizio del diritto di libera circolazione.

Sono tuttavia necessari ulteriori progressi in merito alle proposte della Commissione dell'aprile 2018 sull'**accesso alle prove elettroniche**, dal momento che più della metà delle indagini penali comprende oggi una richiesta transfrontaliera di accesso a tali prove[29]. Il Consiglio ha adottato il suo mandato negoziale per una proposta di regolamento[30] per migliorare l'accesso a livello transfrontaliero alle prove elettroniche nelle indagini penali, e per una proposta di direttiva[31] recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali. Al Parlamento europeo, tuttavia, vi sono stati progressi molto limitati sulle proposte dalla loro adozione da parte della Commissione nell'aprile 2018. Data l'importanza cruciale di un accesso efficiente alle prove elettroniche ai fini del perseguimento di reati transfrontalieri come il terrorismo o la criminalità informatica, la Commissione esorta il Parlamento europeo a portare avanti la proposta.

Parallelamente, la Commissione sta lavorando alle sue **iniziative internazionali sull'accesso alle prove elettroniche** nell'ambito 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. Pertanto, il 5 febbraio 2019 la Commissione ha

---

27 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.

28 COM (2018) 212 final del 17.4.2018.

29 Le prove elettroniche sono necessarie per circa l'85% delle indagini penali, e per due terzi di queste indagini vi è la necessità di 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).

30 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".

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

adottato raccomandazioni [32]sui mandati di negoziato per entrambe le iniziative internazionali. Il Consiglio sta attualmente discutendo i progetti di mandato, anche in occasione della sessione del Consiglio "Giustizia e affari interni" del 7-8 marzo 2019. La Commissione invita il Consiglio ad adottare la decisione che autorizza la partecipazione ai negoziati su un secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica e la decisione che autorizza l'avvio di negoziati con gli Stati Uniti sull'accesso transfrontaliero alle prove elettroniche. È importante procedere rapidamente con i negoziati, al fine di far progredire la cooperazione internazionale sulla condivisione delle prove elettroniche, garantendo nel contempo la compatibilità con il diritto dell'UE e con i conseguenti obblighi degli Stati membri, e tenendo conto anche degli sviluppi futuri del diritto dell'UE.

Al fine di ridurre il margine di manovra dei terroristi, la Commissione invita:

- il **Parlamento europeo** ad adottare con urgenza il suo mandato negoziale sulle proposte legislative in materia di **prove elettroniche**, al fine di avviare senza indugio discussioni trilaterali con il Consiglio (*priorità della dichiarazione comune*);
- il **Consiglio** ad adottare la decisione che autorizza la partecipazione ai negoziati su un **secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica** e la decisione che autorizza l'avvio di **l'avvio di negoziati con gli Stati Uniti** sull'accesso transfrontaliero alle prove elettroniche.

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

La capacità di soggetti esterni e interni di interferire nelle discussioni pubbliche e di manipolare le elezioni è più reale che mai e potrebbe aumentare ulteriormente con le prossime elezioni del Parlamento europeo. Le possibili conseguenze - l'indebolimento o la delegittimazione delle istituzioni democratiche - rappresentano una grave e crescente minaccia strategica. Esse rappresentano una parte cruciale delle sfide in materia di sicurezza che l'UE si trova oggi a dover affrontare a livello transfrontaliero, e richiedono una risposta congiunta e transfrontaliera.

Le campagne elettorali per le elezioni del Parlamento europeo inizieranno concretamente a marzo. In vista del Consiglio europeo del 21 e 22 marzo 2019, la Commissione invita gli Stati membri a rafforzare il loro coordinamento e lo scambio di informazioni per contrastare la disinformazione e proteggere le elezioni contro le minacce basate sull'uso di strumenti informatici. Gli Stati membri dovrebbero sfruttare appieno gli strumenti e i canali di informazione forniti dall'UE, in particolare il recentemente istituito sistema di allarme rapido[33]. Inoltre, in considerazione delle preoccupazioni generate dalla situazione attuale, la Commissione esorta le piattaforme online a intensificare i loro sforzi in tutti gli Stati membri per contribuire a garantire l'integrità delle elezioni del Parlamento europeo del maggio 2019.

---

32 COM (2019) 70 final del 5.2.2019 e COM (2019) 71 final del 5.2.2019.

33 Nell'ambito del piano d'azione contro la disinformazione presentato dalla Commissione e dall'Alto rappresentante nel dicembre 2018 (vedi sotto), il sistema di allarme rapido sarà una piattaforma per gli Stati membri, le istituzioni dell'UE e i partner per condividere informazioni sulle campagne di disinformazione in corso, e consentirà loro di coordinare le loro risposte. Il sistema si baserà esclusivamente su informazioni open source e non riservate.

Per sostenere e incoraggiare tali sforzi, la Commissione e l'Alto rappresentante continuano ad agire lungo due filoni complementari per affrontare le minacce basate sull'uso di strumenti informatici: la lotta contro la disinformazione e il rafforzamento della resilienza elettorale.

1. Misure contro la disinformazione

L'esposizione dei cittadini alla disinformazione su larga scala, comprese le informazioni fuorvianti o completamente false, può costituire una grave minaccia basata sull'uso di strumenti informatici e rappresenta una grande sfida per le prossime elezioni europee. La Commissione sta monitorando da vicino l'attuazione delle azioni indicate nella sua **comunicazione dell'aprile 2018 sulla lotta alla disinformazione online**[34].

La Commissione sta inoltre monitorando da vicino i progressi compiuti nell'ambito del **codice di buone pratiche sulla disinformazione**, firmato da rappresentanti delle piattaforme online, dei principali social network, degli inserzionisti e dell'industria pubblicitaria nell'ottobre 2018 (vedi sotto). La Commissione effettuerà una valutazione globale al termine del periodo iniziale di 12 mesi di applicazione del codice. Qualora l'attuazione e l'impatto del codice di buone pratiche risultino insoddisfacenti, la Commissione può proporre ulteriori misure, anche di natura legislativa.

Sulla base di questo lavoro, e in risposta all'invito dei leader al Consiglio europeo del giugno 2018 di proteggere i sistemi democratici dell'Unione, nel dicembre 2018 la Commissione e l'Alto rappresentante hanno presentato un **piano d'azione congiunto contro la disinformazione**[35]. Il piano d'azione sottolinea che, secondo la **cellula dell'UE per l'analisi delle minacce ibride,** la disinformazione proveniente dalla Federazione russa rappresenta la minaccia più grave per l'UE, in quanto è sistematica, ben finanziata e condotta su una scala diversa rispetto ad altri paesi. Per affrontare la minaccia rappresentata dalla disinformazione, il piano d'azione prevede un aumento delle risorse destinate alla lotta contro tale fenomeno, in particolare per le **task force di comunicazione strategica** del Servizio europeo per l'azione esterna (SEAE), compresa la task force di comunicazione strategica per l'Est[36]. Il piano d'azione prevede anche un aumento delle risorse destinate a questi ambiti e chiede un rafforzamento per i prossimi due anni.

Il piano d'azione prevede misure concrete per contrastare la disinformazione, compresa la creazione di un **sistema di allarme rapido**. In vista delle elezioni del Parlamento europeo, tale sistema di allarme rapido è stato istituito nel marzo 2019 tra le istituzioni e gli Stati membri dell'UE, al fine di facilitare la condivisione dei dati e le valutazioni delle campagne di disinformazione e di segnalare le minacce derivanti dalla disinformazione.

Il piano d'azione prevede inoltre un attento monitoraggio dell'attuazione del summenzionato codice di buone pratiche firmato dalle piattaforme online. Il 29 gennaio 2019, la Commissione ha pubblicato le **relazioni presentate dai firmatari del codice di buone pratiche** – Google, Facebook, Twitter, Mozilla e le associazioni del settore pubblicitario. La Commissione ha

---

34 COM (2018) 236 final del 26.4.2018, cui ha fatto seguito la relazione d'attuazione COM (2018) 794 final del 5.12.2018.

35 JOIN (2018) 36 final del 5.12.2018.

36 Dalla sua istituzione nel 2015, la task force di comunicazione strategica per l'Est ha catalogato, analizzato e messo in luce quasi 5 000 esempi di disinformazione da parte della Federazione russa, denunciando numerose narrazioni di disinformazione, smascherando gli strumenti, le tecniche e le intenzioni delle campagne di disinformazione e sensibilizzando il pubblico al riguardo.

accolto con favore i progressi compiuti, ma ha anche invitato i firmatari a intensificare gli sforzi in vista delle elezioni del Parlamento europeo del 2019[37].

Il 28 febbraio 2019 la Commissione ha pubblicato **le relazioni presentate da Facebook, Google e Twitter** sui progressi compiuti nel gennaio 2019 riguardo ai loro impegni in materia di lotta contro la disinformazione. In queste relazioni le piattaforme non hanno fornito dettagli sufficienti a dimostrare che in tutti gli Stati membri dell'UE si stanno attuando nuove politiche e nuovi strumenti in modo tempestivo e con risorse sufficienti. Vi sono chiaramente margini di miglioramento per tutti i firmatari[38]. Più specificamente, la Commissione chiede alle piattaforme di garantire la trasparenza dei messaggi di propaganda politica entro l'inizio della campagna delle elezioni europee in tutti gli Stati membri dell'UE, per consentire un accesso adeguato ai dati delle piattaforme a fini di ricerca e di verifica dei fatti e per garantire una corretta cooperazione tra le piattaforme e i singoli Stati membri attraverso i punti di contatto nel sistema di allarme rapido.

La Commissione riferirà nuovamente il 20 marzo 2019 sull'attuazione del summenzionato codice di buone pratiche.

2. Rafforzamento della resilienza elettorale

Il 12 settembre 2018 la Commissione ha adottato un pacchetto di misure volte a rafforzare la resilienza dei sistemi elettorali. Tali misure sono indirizzate agli Stati membri, e ai partiti politici europei e nazionali e alle fondazioni politiche europee e nazionali, e comprendono una raccomandazione relativa alle reti di cooperazione in materia elettorale, alla trasparenza online, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione, nonché orientamenti sull'applicazione del diritto dell'Unione in materia di protezione dei dati[39], e una modifica legislativa che rende più rigorose le norme sul finanziamento dei partiti politici europei.

Il Parlamento europeo ha accolto con favore il pacchetto nella risoluzione adottata il 28 ottobre 2018. Il Consiglio ha a sua volta accolto con favore queste misure nelle sue conclusioni del 19 febbraio 2019 "Assicurare elezioni europee libere e corrette", che esprimono un impegno comune da parte di tutti gli Stati membri a favore di un approccio europeo coordinato per la tutela dell'integrità delle prossime elezioni europee. Il Consiglio "Giustizia e affari interni" ha fatto il punto della situazione il 7 marzo 2019.

La modifica del regolamento relativo allo **statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee**[40] introduce la possibilità di imporre sanzioni per l'uso illegale di dati personali in caso di deliberata influenza sull'esito delle elezioni del Parlamento europeo. A seguito dell'accordo politico[41] del gennaio 2019, il 12 marzo 2019 la plenaria del Parlamento europeo ha approvato il testo della modifica, che dovrebbe acquisire forza di legge prima delle elezioni del Parlamento europeo del 2019.

---

37 Per maggiori dettagli consultare: http://europa.eu/rapid/press-release_IP-19-746_it.htm.

38 Per maggiori dettagli consultare: http://europa.eu/rapid/press-release_STATEMENT-19-1379_it.htm.

39 COM (2018) 638 final del 12.9.2018.

40 COM (2018) 636 final del 12.9.2018.

41 L'accordo politico raggiunto dai colegislatori il 16 gennaio 2018 è stato approvato dal comitato dei rappresentanti permanenti del Consiglio il 25 gennaio 2019 e dalla commissione per gli affari costituzionali del Parlamento europeo il 29 gennaio 2019.

La raccomandazione relativa alle **reti di cooperazione in materia elettorale, alla trasparenza online, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione nel contesto delle elezioni del Parlamento europeo**[42] è rivolta ai partiti politici nazionali ed europei ed alle fondazioni politiche nazionali ed europee, e presenta misure concrete per i soggetti rilevanti in questi ambiti. Ai fini dell'attuazione della raccomandazione le reti nazionali per le questioni elettorali hanno designato punti di contatto che partecipino a una **rete europea di cooperazione in materia elettorale**, che serva per dare l'allarme su eventuali minacce, per lo scambio di migliori pratiche fra le reti nazionali, per discutere soluzioni comuni alle sfide individuate e per incoraggiare progetti e iniziative comuni fra le reti nazionali. Alla prima riunione della rete, il 21 gennaio 2019, i partecipanti hanno convenuto sulla necessità fondamentale di un approccio globale per garantire l'integrità delle elezioni, mantenendo nel contempo un dibattito democratico aperto e condizioni di parità a livello politico. La seconda riunione della rete europea di cooperazione in materia elettorale, svoltasi il 27 febbraio 2019, si è incentrata su temi legati al monitoraggio e all'attuazione rilevanti nel contesto elettorale, compresa la protezione dei dati, la regolamentazione dei media, le attività di contrasto, la trasparenza e i media sociali, e il coinvolgimento dei vari portatori di interessi nelle attività di monitoraggio. In tale contesto sono state gettate le basi per la partecipazione dei membri della rete a un esercizio di resilienza informatica, subito dopo la prossima riunione prevista per il 5 aprile 2019.

Il 19 febbraio 2019 si è tenuto un **seminario sul tema "Rafforzare la resilienza informatica delle elezioni"**, organizzato congiuntamente dal Parlamento europeo e dalla Commissione, per migliorare la sicurezza e la resilienza dei sistemi e delle infrastrutture elettorali contro la costante evoluzione delle minacce basate sull'uso di strumenti informatici. Le autorità nazionali degli Stati membri incaricate della sicurezza informatica, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione e le piattaforme online hanno discusso misure incentrate su azioni urgenti e pertinenti per garantire l'integrità delle elezioni del Parlamento europeo del 2019.

Le istituzioni dell'UE e gli Stati membri collaborano inoltre strettamente ad altre **attività di sensibilizzazione** volte a tutelare l'integrità del processo elettorale e al coinvolgimento degli operatori del settore pubblico e privato, compresi i media, le piattaforme online e la società civile.

Al fine di contrastare la disinformazione e garantire la resilienza elettorale, la Commissione e l'Alto rappresentante invitano gli Stati membri:

- ad attuare con prontezza e decisione le azioni previste dal **piano d'azione congiunto contro la disinformazione** di dicembre 2018.

IV. ATTUAZIONE DI ALTRI FASCICOLI PRIORITARI IN MATERIA DI SICUREZZA

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

L'attuazione completa e corretta delle misure concordate riveste la massima priorità per garantire i pieni vantaggi di un'autentica ed efficace Unione della sicurezza. La Commissione sta attivamente sostenendo gli Stati membri, anche con finanziamenti e facilitando lo scambio delle migliori prassi. Ove necessario, la Commissione inoltre si avvale appieno dei poteri

[42] C (2018) 5949 final del 12.9.2018.

conferitile dai trattati per l'attuazione del diritto dell'Unione, ricorrendo anche, se opportuno, al procedimento d'infrazione.

Per quanto riguarda l'attuazione della **direttiva UE sui dati del codice di prenotazione**[43], il 19 luglio 2018 la Commissione ha avviato procedimenti di infrazione nei confronti di 14 Stati membri per omessa comunicazione dell'adozione di una normativa nazionale diretta a recepire pienamente la direttiva[44] – uno strumento essenziale nella lotta al terrorismo e alle forme gravi di criminalità. Da allora, nove Stati membri hanno notificato il pieno recepimento[45]. Gli Stati membri che non hanno ancora proceduto al pieno recepimento hanno ricevuto pareri motivati (Spagna il 24 gennaio 2019, Paesi Bassi e Finlandia il 7 marzo 2019). In parallelo, la Commissione continua a sostenere gli Stati membri nei loro sforzi per completare lo sviluppo dei rispettivi sistemi di codici di prenotazione, anche agevolando lo scambio di informazioni e di migliori pratiche.

Il termine per il recepimento della **direttiva sulla lotta contro il terrorismo**[46] è scaduto l'8 settembre 2018. Il 22 novembre 2018 la Commissione ha avviato procedimenti di infrazione nei confronti di 16 Stati membri per omessa comunicazione dell'adozione di una normativa nazionale diretta a recepire pienamente la direttiva. Da allora, nove Stati membri hanno notificato il pieno recepimento[47]. La Commissione esorta i restanti sette Stati membri ad adottare quanto prima le misure necessarie[48].

Il termine per il recepimento della **direttiva relativa al controllo dell'acquisizione e della detenzione di armi**[49] è scaduto il 14 settembre 2018. Finora, sei Stati membri hanno notificato il pieno recepimento[50] e cinque Stati membri un recepimento parziale[51]. 22 Stati membri[52], compresi quelli che hanno notificato un recepimento parziale, hanno ricevuto lettere di costituzione in mora della Commissione il 22 novembre 2018.

Per quanto riguarda la **direttiva sulla protezione dei dati nell'ambito delle attività di contrasto**[53]**,** il 19 luglio 2018 la Commissione ha avviato procedimenti di infrazione nei confronti di 19 Stati membri a causa dell'omessa comunicazione dell'adozione di una normativa nazionale che garantisca il pieno recepimento dell'atto nel diritto nazionale[54].

---

43 Direttiva (UE) 2016/681 del 27.4.2016.

44 Bulgaria, Repubblica ceca, Estonia, Grecia, Spagna, Francia, Cipro, Lussemburgo, Paesi Bassi, Austria, Portogallo, Romania, Slovenia e Finlandia.

45 Bulgaria, Estonia, Grecia, Francia, Cipro, Lussemburgo, Austria, Portogallo, Romania (situazione all'11 marzo 2019).

46 Direttiva (UE) 2017/541 del 15.3.2017.

47 Bulgaria, Repubblica ceca, Germania, Estonia, Spagna, Francia, Croazia, Italia, Lettonia, Lituania, Ungheria, Malta, Paesi Bassi, Austria, Portogallo, Slovacchia, Finlandia e Svezia hanno notificato il recepimento (situazione all'11 marzo 2019).

48 Belgio, Polonia, Romania e Slovenia hanno notificato un recepimento parziale. Grecia, Cipro e Lussemburgo non hanno trasmesso alcuna notifica (situazione all'11 marzo 2019).

49 Direttiva (UE) 2017/853 del 17.5.2017.

50 Danimarca, Francia, Croazia, Italia, Malta e Austria (situazione all'11 marzo 2019).

51 Repubblica ceca, Estonia, Lituania, Portogallo e Regno Unito (situazione all'11 marzo 2019).

52 Belgio, Bulgaria, Repubblica ceca, Germania, Estonia, Irlanda, Grecia, Spagna, Cipro, Lettonia, Lituania, Lussemburgo, Ungheria, Paesi Bassi, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia, Svezia e Regno Unito (situazione all'11 marzo 2019).

53 Direttiva (UE) 2016/680 del 27.4.2016.

54 Belgio, Bulgaria, Repubblica ceca, Estonia, Grecia, Spagna, Francia, Croazia, Cipro, Lettonia, Lituania, Lussemburgo, Ungheria, Paesi Bassi, Polonia, Portogallo, Romania, Slovenia e Finlandia. La

Attualmente, 17 Stati membri hanno notificato il pieno recepimento e cinque Stati membri un recepimento parziale[55]. Finora sono state chiusi i procedimenti contro sei Stati membri[56], mentre nove Stati membri hanno ricevuto un parere motivato il 25 gennaio 2019[57].

La Commissione dovrebbe riferire in merito alla coerenza dell'identificazione degli operatori di servizi essenziali entro il 9 maggio 2019. In base alle notificazioni degli Stati membri, si è stabilito che la **direttiva sulla sicurezza delle reti e dei sistemi informativi**[58] è stata pienamente recepita in 25 Stati membri e recepita parzialmente in uno Stato membro[59]. Nel gennaio 2019 la Commissione ha chiuso i procedimenti di infrazione per mancata comunicazione nei confronti di sei Stati membri[60]. Nove Stati membri[61] sono oggetto di un procedimento di infrazione per mancata comunicazione del pieno recepimento della direttiva. Nell'ambito del recepimento della direttiva sulla sicurezza delle reti e dei sistemi informativi, gli Stati membri dovevano presentare alla Commissione entro il 9 novembre 2018 informazioni relative agli operatori di servizi essenziali identificati sul loro territorio. La Commissione sta ora valutando tali informazioni trasmesse dagli Stati membri[62].

La Commissione sta inoltre valutando il recepimento della **quarta direttiva antiriciclaggio**[63], e sta lavorando al tempo stesso per verificare che gli Stati membri ne attuino le norme. La Commissione ha avviato procedimenti di infrazione contro tutti e 28 gli Stati membri, ritenendo che le comunicazioni da questi ricevute non costituiscano un pieno recepimento della direttiva[64]. Essa continuerà ad avvalersi dei suoi poteri, se necessario, per garantire la piena attuazione della direttiva.

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

Commissione sta ricevendo le risposte degli Stati membri, comprese le notifiche della normativa interessata, attualmente oggetto di esame (situazione all'11 marzo 2019).

55 Belgio, Germania, Estonia, Irlanda, Francia, Croazia, Italia, Lituania, Lussemburgo, Ungheria, Malta, Austria, Polonia, Romania, Slovacchia, Svezia e Regno Unito hanno notificato il pieno recepimento. Repubblica ceca, Portogallo, Finlandia, Slovenia e Paesi Bassi hanno notificato un recepimento parziale. La Danimarca ha inoltre completato il recepimento (situazione all'11 marzo 2019).

56 Belgio, Francia, Croazia, Lituania, Lussemburgo, Ungheria (situazione all'11 marzo 2019).
Grecia, Cipro, Spagna, Slovenia, Portogallo, Repubblica ceca, Bulgaria, Lettonia e Paesi Bassi (situazione all'11 marzo 2019).

58 Direttiva (UE) 2016/1148 del 27.4.2016.

59 Bulgaria, Repubblica ceca, Danimarca, Germania, Grecia, Estonia, Irlanda, Spagna, Francia, Croazia, Italia, Cipro, Lettonia, Lituania, Malta, Paesi Bassi, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia, Svezia e Regno Unito hanno notificato il pieno recepimento. L'Ungheria ha notificato un recepimento parziale. Belgio e Lussemburgo non hanno notificato alla Commissione alcuna misura nazionale di recepimento (situazione all'11 marzo 2019).

60 Irlanda, Spagna, Francia, Croazia, Paesi Bassi e Portogallo (situazione all'11 marzo 2019).

61 Bulgaria, Belgio, Danimarca, Lettonia, Lituania, Lussemburgo, Ungheria, Austria e Romania (situazione all'11 marzo 2019).

62 Bulgaria, Cipro, Repubblica ceca, Germania, Danimarca, Estonia, Spagna, Finlandia, Francia, Croazia, Ungheria, Irlanda, Italia, Lituania, Malta, Paesi Bassi, Polonia, Portogallo, Slovacchia, Svezia e Regno Unito (situazione all'11 marzo 2019).

63 Direttiva (UE) 2015/849 del 20.5.2015.

64 La Commissione ha avviato procedimenti di infrazione nei confronti di tutti gli Stati membri per omessa comunicazione della normativa nazionale diretta a recepire pienamente la direttiva, poiché, secondo la valutazione, ha concluso che alcune disposizioni della direttiva non erano state recepite.

- la **direttiva UE sui dati del codice di prenotazione**: tre Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e due Stati membri devono completare la notifica del recepimento[65];
- la **direttiva sulla sicurezza delle reti e dei sistemi informativi**: due Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e uno Stato membro deve completare la notifica del recepimento[66];
- la **direttiva sulla lotta contro il terrorismo**: tre Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e quattro Stati membri devono completare la notifica del recepimento[67];
- la **direttiva relativa al controllo dell'acquisizione e della detenzione di armi**: 17 Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e cinque Stati membri devono completare la notifica del recepimento[68];
- la **direttiva sulla protezione dei dati nell'ambito delle attività di contrasto**: cinque Stati membri non hanno ancora notificato il recepimento nel diritto nazionale e cinque Stati membri devono completare la notifica del recepimento[69], e
- la **quarta direttiva antiriciclaggio**: uno Stato membro deve ancora completare la notifica del recepimento[70].

2. Protezione degli spazi pubblici - Buone pratiche raccomandate

Fra le misure pratiche volte a migliorare la protezione e la resilienza contro il terrorismo, la Commissione continua a sostenere gli Stati membri e le autorità locali nella **protezione degli spazi pubblici** In applicazione del piano d'azione dell'ottobre 2017 per migliorare la

65 Spagna, Paesi Bassi e Finlandia non hanno ancora comunicato il recepimento. La Repubblica ceca e la Slovenia hanno comunicato il recepimento parziale e non hanno ancora completato la notifica del recepimento (situazione all'11 marzo 2019). 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.

66 Belgio e Lussemburgo non hanno ancora comunicato il recepimento. L'Ungheria ha comunicato il recepimento parziale e non ha ancora completato la notifica del recepimento (situazione all'11 marzo 2019).

67 Grecia, Cipro e Lussemburgo non hanno ancora comunicato il recepimento. Belgio, Polonia, Romania e Slovenia hanno comunicato il recepimento parziale e non hanno ancora completato la notifica del recepimento (situazione all'11 marzo 2019).

68 Belgio, Bulgaria, Germania, Irlanda, Grecia, Spagna, Cipro, Lettonia, Lussemburgo, Ungheria, Paesi Bassi, Polonia, Romania, Slovenia, Slovacchia, Finlandia e Svezia non hanno ancora comunicato il recepimento. La Repubblica ceca, l'Estonia, la Lituania, il Portogallo e il Regno Unito hanno comunicato il recepimento parziale e non hanno ancora completato la notifica del recepimento (situazione all'11 marzo 2019). 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.

69 Bulgaria, Grecia, Spagna, Cipro e Lettonia non hanno ancora comunicato il recepimento. La Repubblica ceca, il Portogallo, i Paesi Bassi, la Finlandia e la Slovenia hanno comunicato il recepimento parziale e devono ancora completare la notifica del recepimento (situazione all'11 marzo 2019).

70 La Romania ha comunicato il recepimento parziale e deve ancora completare la notifica del recepimento. Tutti gli altri Stati membri hanno notificato il pieno recepimento. Tuttavia, secondo la valutazione della Commissione, vi sono ancora alcune disposizioni della direttiva il cui recepimento non sembra essere stato pienamente completato (situazione all'11 marzo 2019).

protezione degli spazi pubblici[71], il lavoro si concentra sullo sviluppo e la raccolta di orientamenti e buone pratiche. Lavorando insieme ad autorità pubbliche e operatori privati di spazi pubblici nel cosiddetto Forum degli operatori[72], la Commissione ha individuato buone pratiche per vari provvedimenti che tutti gli operatori e le autorità pubbliche coinvolti nella protezione degli spazi pubblici possono attuare per rafforzare la sicurezza[73]. Tali pratiche costituiscono le basi per indirizzare il lavoro futuro in tutti i settori pertinenti per la protezione degli spazi pubblici (cfr. riquadro sottostante).

Buone pratiche per le autorità pubbliche e gli operatori privati per rafforzare la sicurezza degli spazi pubblici

Valutazione e pianificazione

- Predisporre ed effettuare valutazioni delle vulnerabilità per individuare potenziali punti deboli contro gli attacchi da parte di soggetti esterni o interni.
- Elaborare e attuare un piano di sicurezza per la struttura o per l'evento, che preveda misure di preparazione, di emergenza e di ripristino, e che individui le misure di sicurezza appropriate per l'ambiente della struttura o dell'evento. Le misure di sicurezza devono essere efficaci, discrete, proporzionate e su misura per i diversi ambienti, tenendo conto del loro funzionamento specifico.
- Nominare e formare una persona responsabile del coordinamento e dell'attuazione delle misure di sicurezza contenute nel piano di sicurezza.
- Elaborare e attuare un piano di gestione delle crisi.

Sensibilizzazione e formazione

- Organizzare campagne di sensibilizzazione dei cittadini sulla segnalazione di comportamenti sospetti e su come reagire nel caso di un attacco che comprometta la sicurezza di una struttura o di un evento.
- Elaborare e attuare un programma interno di sensibilizzazione alla sicurezza per tutti i dipendenti di una struttura.
- Elaborare e attuare un programma interno di sensibilizzazione alle minacce che contribuisca a proteggere le strutture o gli eventi contro i diversi tipi di minacce interne, quali il sabotaggio, il furto commerciale o gli attacchi terroristici.
- Elaborare programmi di formazione di base in materia di sicurezza per tutto il personale e intraprendere azioni specifiche di formazione in materia di sicurezza, contribuendo allo sviluppo di una cultura della sicurezza d'impresa. Sviluppare attività che motivino i dipendenti ad attuare pratiche di sicurezza valide e a mantenere un elevato livello di vigilanza in materia di sicurezza.
- Organizzare periodicamente esercitazioni di sicurezza che aiutino a individuare il livello di preparazione per scoraggiare e rispondere a un attacco.

Protezione fisica

- Valutare i problemi di sicurezza e di protezione fisica sin dall'inizio del processo di progettazione di un nuovo impianto o evento.

---

71 COM (2017) 612 final del 18.10.2017.

72 Il Forum pubblico-privato degli operatori, istituito nel quadro del piano d'azione dell'ottobre 2017 per migliorare la protezione degli spazi pubblici, riunisce responsabili politici ed operatori degli Stati membri di diversi settori, come eventi di massa e intrattenimento, ospitalità, centri commerciali, sportivi e culturali, snodi di trasporto e altri ancora.

73 Per maggiori dettagli sulle buone pratiche, consultare il documento di lavoro dei servizi della Commissione "Buone pratiche per migliorare la protezione degli spazi pubblici" (SWD (2019) 140 del 20.3.2019).

- Valutare i necessari controlli di accesso e le barriere, evitando al contempo di creare nuove vulnerabilità. I controlli di accesso e le barriere non dovrebbero modificare i rischi e creare nuovi obiettivi.
- Valutare la tecnologia più appropriata per il rilevamento di esplosivi, armi da fuoco e armi bianche, e degli agenti chimici, biologici, radiologici e nucleari.

Cooperazione

- Designare punti di contatto e chiarire i rispettivi ruoli e responsabilità nell'ambito della cooperazione pubblico-privato in materia di sicurezza (ad esempio tra operatori, servizi di sicurezza privati e autorità di contrasto), anche con l'obiettivo di migliorare la comunicazione e la cooperazione su base regolare.
- Instaurare una comunicazione e una cooperazione affidabili e tempestive, che consentano uno scambio di informazioni specifiche sui rischi e sulle minacce tra le autorità pubbliche responsabili, le autorità di contrasto locali e il settore privato.
- Coordinare il lavoro sulla protezione degli spazi pubblici a livello locale, regionale e nazionale, e impegnarsi in attività di comunicazione e scambi di buone pratiche a tutti i livelli, anche a livello dell'UE.
- Le autorità pubbliche, insieme agli operatori, dovrebbero elaborare e mettere a disposizione raccomandazioni pratiche e materiale orientativo per individuare, attenuare o rispondere alle minacce alla sicurezza.

3. Vulnerabilità delle infrastrutture digitali

La resilienza digitale è fondamentale per proteggere le attività generali dei nostri governi, la ricerca industriale, la proprietà intellettuale, i piani aziendali, le nostre elezioni, le istituzioni democratiche e i nostri dati personali. Una delle questioni principali legate alla cibersicurezza, e che sta suscitando un diffuso interesse nel dibattito pubblico nell'UE, riguarda le reti di quinta generazione (5G). In occasione del recente Consiglio ministeriale informale sulle telecomunicazioni, tenutosi a Bucarest il 1º marzo 2019, i ministri hanno espresso il proprio sostegno a un approccio europeo coordinato per rafforzare la resilienza digitale nell'UE in relazione alle reti 5G. L'infrastruttura delle reti 5G costituisce una base importante per l'economia digitale. Oltre ai servizi per i consumatori, la tecnologia 5G è concepita per fornire, ed è previsto che fornisca, servizi essenziali per la corretta operatività dei settori verticali, quali la mobilità, l'energia e la salute. Le norme applicabili alle reti 5G sono globali, e le apparecchiature e i dispositivi saranno offerti da una serie di fornitori a livello mondiale.

La diffusione delle reti 5G nei prossimi anni segna un cambiamento radicale rispetto alle reti precedenti. La conservazione dei dati nel *cloud* consentirà la connessione di miliardi di dispositivi dell'Internet degli oggetti, e di alimentare nuove innovazioni nell'ambito dell'intelligenza artificiale, creando opportunità per i cittadini e le imprese. La cibersicurezza è pertanto di particolare importanza, poiché le vulnerabilità potrebbero essere sfruttate causando potenzialmente danni molto gravi. E dato che Internet non conosce frontiere, una violazione della sicurezza in uno Stato membro potrebbe avere ripercussioni su molti altri.

Per scongiurare le possibili gravi implicazioni in termini di sicurezza delle infrastrutture digitali critiche va definito un approccio comune dell'UE alla sicurezza delle reti 5G. Per avviare questo processo, dopo il Consiglio europeo del 21 e 22 marzo 2019 la Commissione pubblicherà una raccomandazione relativa a un approccio comune dell'UE ai rischi per la sicurezza delle reti 5G, basato 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 Le possibili misure esaminate dovrebbero includere l'applicazione delle tecnologie quantistiche per la sicurezza delle reti così come per la protezione dei dati conservati[74].

Il 12 marzo 2019 il Parlamento europeo ha adottato una risoluzione sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'UE e sulla possibile azione a livello di UE per ridurre tali minacce.

4. Dimensione esterna

I negoziati tra l'UE e il Canada su un **accordo riveduto sui dati del codice di prenotazione** procedono bene. Il prossimo vertice UE-Canada che si terrà a Montreal l'11-12 aprile 2019 potrebbe dare un impulso positivo ai negoziati.

La Commissione sta lavorando con le autorità degli Stati Uniti per preparare la prossima valutazione congiunta dell'**accordo tra gli Stati Uniti d'America e l'Unione europea sulle registrazioni dei nominativi dei passeggeri**[75], in linea con le disposizioni dello stesso accordo. Sono inoltre già in corso i lavori per la quinta verifica congiunta dell'**accordo tra l'Unione europea e gli Stati Uniti d'America sul programma di controllo delle transazioni finanziarie dei terroristi**[76]. Tale verifica congiunta, nell'ambito della quale verranno riesaminate le disposizioni dell'accordo riguardanti le salvaguardie, i controlli e la reciprocità, servirà anche a valutare il valore del programma come strumento antiterrorismo sia per l'UE che per gli Stati Uniti.

Gli sviluppi della situazione in corso in Siria hanno messo maggiormente in evidenza la questione dei **combattenti stranieri** attualmente presenti o trattenuti nelle zone di conflitto. L'UE può, se richiesto, fornire sostegno agli Stati membri, nello specifico per quanto riguarda lo scambio di informazioni e il sostegno alle indagini penali, e in particolare la cooperazione con partner internazionali e attraverso Europol, mettendo anche a frutto le competenze e le migliori pratiche in materia di riabilitazione e reinserimento sviluppate nel contesto della rete di sensibilizzazione al problema della radicalizzazione. L'Unione europea può inoltre fornire sostegno allo sviluppo delle capacità dei paesi terzi particolarmente colpiti dal fenomeno del ritorno dei combattenti stranieri. La decisione di rimpatriare o meno i combattenti stranieri e le loro famiglie dalle zone di conflitto spetta agli Stati membri interessati.

L'UE e l'Egitto hanno copresieduto la riunione plenaria del gruppo di lavoro per l'Africa orientale del **Forum globale contro il terrorismo**, tenutasi a Nairobi il 20 febbraio 2019, che ha visto un alto tasso di partecipazione dei settori giudiziario e di polizia di Somalia, Kenya, Sudan, Uganda, Gibuti, Somalia, Etiopia, Yemen e Tanzania.

V. CONCLUSIONI

L'UE ha compiuto notevoli progressi nel lavoro comune per un'autentica ed efficace Unione della sicurezza, con l'adozione di una serie di iniziative legislative prioritarie da parte del Parlamento europeo e del Consiglio negli ultimi mesi e settimane. È necessario tuttavia compiere ulteriori sforzi in vista delle elezioni del Parlamento europeo del maggio 2019 per

---

74 Si veda anche la comunicazione dal titolo "Iniziativa europea per il *cloud computing* — Costruire un'economia competitiva dei dati e della conoscenza in Europa" (COM (2016) 178 final del 19.4.2016).

75 GU L 215 dell'11.8.2012, pag. 5.

76 GU L 195 del 27.7.2010, pag. 5.

far fronte a urgenti requisiti di sicurezza. In particolare, la Commissione invita i colegislatori ad avviare i negoziati sulle norme proposte per la rimozione dei contenuti terroristici online non appena il Parlamento europeo avrà adottato il suo mandato negoziale, al fine di raggiungere un accordo ancora durante l'attuale mandato del Parlamento europeo. Per quanto riguarda la proposta relativa al rafforzamento della guardia di frontiera e costiera europea, i negoziati sono già nella fase delle discussioni trilaterali, cosa che dimostra che tutte le istituzioni sono impegnate ad adottare tale atto prima delle elezioni del Parlamento europeo. La Commissione invita inoltre gli Stati membri ad attuare tutte le misure concordate nell'ambito dell'Unione della sicurezza per garantire che abbiano piena efficacia per la sicurezza di tutti i cittadini.

Inoltre, dati i tempi stretti per garantire la preparazione dell'Unione prima che gli elettori europei si rechino alle urne a maggio 2019, la Commissione invita tutti i soggetti coinvolti a raddoppiare gli sforzi per aumentare la resilienza elettorale ai fini della lotta contro la disinformazione. In vista del Consiglio europeo del 21 e 22 marzo 2019, è necessario che gli Stati membri intensifichino il coordinamento e lo scambio di informazioni per contrastare la disinformazione e proteggere le elezioni da altre minacce basate sull'uso di strumenti informatici, sfruttando appieno gli strumenti che l'UE fornisce a tal fine. Allo stesso tempo, le piattaforme online devono intensificare i propri sforzi in tutti gli Stati membri per contribuire a garantire l'integrità delle elezioni del Parlamento europeo del maggio 2019. La Commissione continuerà a sostenere e incoraggiare questi lavori nelle settimane e nei mesi a venire per tutelare l'integrità delle elezioni del Parlamento europeo.