Consiglio
dell'Unione europea

Bruxelles, 18 ottobre 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	18 ottobre 2023
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2023) 665 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Sesta relazione sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza

Si trasmette in allegato, per le delegazioni, il documento COM(2023) 665 final.

All.: COM(2023) 665 final

COMMISSIONE
EUROPEA

Bruxelles, 18.10.2023
COM(2023) 665 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Sesta relazione sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza

I. Introduzione

Tre anni fa la Commissione ha adottato la strategia per l'Unione della sicurezza[1] per il periodo 2020-2025, che definisce le principali priorità dell'Unione nel settore. Da allora sono stati compiuti notevoli progressi in tutti e quattro i pilastri della strategia, con l'emanazione di importanti atti legislativi in tutti i comparti, dalla protezione dei soggetti critici al potenziamento della ciberresilienza. Nel frattempo il contesto delle minacce alla sicurezza in Europa e nel suo vicinato ha tuttavia continuato ad evolversi. I recenti attentati terroristici perpetrati in una scuola in Francia e nelle vie di Bruxelles rimettono prepotentemente in luce l'urgenza di continuare ad adattare e rafforzare l'architettura di sicurezza dell'Unione. Il pericolo rappresentato dagli attacchi informatici continua a crescere, alimentato anche da malintenzionati che si schierano sui conflitti in corso. Le minacce ibride, compresa la disinformazione, non cessano di moltiplicarsi. Europol ha indicato la guerra di aggressione russa contro l'Ucraina come causa di un aumento significativo degli attacchi informatici contro obiettivi UE, compresi gravi attacchi di matrice politica coordinati da gruppi di hacker filorussi[2]. Due esempi emblematici sono stati il blocco dell'accesso a internet e l'interruzione di servizi chiave come le reti energetiche[3].

La strategia per l'Unione della sicurezza è studiata per dotare l'UE dei mezzi per resistere meglio in un contesto di minacce in costante evoluzione. Via via che ci siamo trovati confrontati alle crisi della pandemia e della guerra, gli eventi hanno dimostrato l'importanza dell'approccio adottato nella strategia: determinazione a stabilizzare un quadro complessivo dell'ecosistema di sicurezza dell'UE superando i confini tra dimensione cibernetica e dimensione fisica della sicurezza, anche in termini di contrasto della criminalità organizzata e del terrorismo, oltre alla lotta contro la radicalizzazione.

La necessità di restare vigili implica tuttavia la verifica continua della presenza di lacune nelle attività che poniamo in essere pertenere i cittadini al sicuro. La strategia ha definito i settori prioritari in cui l'Unione può apportare un valore aggiunto per sostenere gli Stati membri nella promozione della sicurezza per tutte le persone che vivono in Europa. Dalla sua adozione, tutte le azioni stabilite sono state messe in campo e ne sono state aggiunte di nuove per rispondere alle attuali sfide in materia di sicurezza.

Nell'ambito della strategia per l'Unione della sicurezza, la Commissione ha presentato complessivamente 36 iniziative legislative. Per oltre la metà di tali proposte i negoziati interistituzionali si sono già conclusi con una nuova e solida legislazione, come indicato nella tabella in allegato. Tuttavia diverse iniziative chiave proposte dalla Commissione sono ancora in fase di negoziazione al Parlamento europeo e al Consiglio. Poiché l'attuale legislatura terminerà a giugno 2024 con le elezioni europee, è necessario agire rapidamente per portare a termine questi fascicoli in sospeso, in modo che i cittadini possano beneficiare appieno dell'Unione della sicurezza. La presente sesta relazione sui progressi compiuti nell'Unione della sicurezza si concentra pertanto sulla descrizione dei fascicoli legislativi e non legislativi

[1] COM(2020) 605 final.

[2] Attacchi distribuiti di negazione del servizio (DDoS): cfr. lo "Spotlight report" di Europol: "Cyber-attacks: the apex of crime-as-a-service", 13 settembre 2023.

[3] Durante il conflitto in Ucraina i malware wiper sono stati utilizzati in modo massiccio per distruggere dati e sistemi, ad esempio per compromettere l'accesso a internet di migliaia di abbonati nell'UE o per colpire un'importante azienda energetica tedesca, che ha perso l'accesso al monitoraggio remoto di oltre 5 800 turbine eoliche. Il ruolo della cibernetica nella guerra russa contro l'Ucraina: il suo impatto e le conseguenze per i futuri conflitti armati, studio del Parlamento europeo, settembre 2023 – PE 702.594.

dell'Unione della sicurezza cruciali già adottati dalla Commissione e per la cui finalizzazione ed efficace attuazione sono necessarie azioni aggiuntive.

Per quanto riguarda gli atti legislativi dell'UE già adottati, i benefici saranno percepiti solo quando saranno stati messi in pratica. Occorre concentrarsi sul loro corretto e pieno recepimento come pure sulla loro attuazione e applicazione negli Stati membri. Nel 2023 la Commissione ha continuato a garantire che la strategia dell'UE per l'Unione della sicurezza producesse risultati, utilizzando i propri poteri istituzionali per avviare procedure di infrazione qualora gli Stati membri non avessero recepito la legislazione dell'UE o l'avessero recepita in modo errato.

La presente relazione indica in modo sintetico anche gli aspetti in merito ai quali l'azione degli Stati membri e/o delle agenzie dell'UE risulta fondamentale per ottenere risultati. Le agenzie dell'UE svolgono un ruolo essenziale nel sostenere l'attuazione delle iniziative dell'Unione della sicurezza e negli ultimi anni le loro competenze sono aumentate. La relazione illustra alcuni dei nuovi compiti principali che sono stati assegnati loro affinché forniscano un maggiore sostegno agli Stati membri nell'attuazione delle iniziative chiave nell'ambito dell'Unione della sicurezza.

Inoltre la situazione geopolitica ha messo in evidenza l'importanza che la sicurezza esterna riveste per la sicurezza interna. Un quadro interno dell'UE più forte nel settore della sicurezza è intrinsecamente legato a partenariati e cooperazioni più forti con i paesi terzi. L'UE deve continuare ad adoperarsi affinché le interazioni che porta avanti a livello mondiale contribuiscano a garantire la sicurezza dei propri cittadini.

II. Un ambiente della sicurezza adeguato alle esigenze del futuro

Cibersicurezza e resilienza delle infrastrutture critiche

Nell'ambito dell'Unione della sicurezza l'UE è impegnata a garantire che tutti i cittadini e le imprese europei siano protetti adeguatamente, sia online sia offline, e a promuovere un ciberspazio aperto, sicuro e stabile. L'entità, la frequenza e l'impatto crescenti degli incidenti di cibersicurezza rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi e per il mercato interno. La guerra di aggressione della Russia contro l'Ucraina ha ulteriormente acuito questa minaccia e le attuali tensioni geopolitiche sono aggravate dagli interventi di una molteplicità di soggetti allineati con le autorità di governo, criminali e hacktivisti. Il sabotaggio del gasdotto Nord Stream avvenuto l'autunno scorso ha evidenziato come settori essenziali quali l'energia, le infrastrutture digitali, i trasporti e lo spazio dipendano dalla resilienza delle infrastrutture critiche. Il recente incidente che ha coinvolto un gasdotto sottomarino e un cavo dati in Estonia e Finlandia dimostra la necessità di un alto livello di preparazione per affrontare questo tipo di situazioni. Sebbene la causa del danno sia ancora poco chiara e le indagini siano in corso, la condivisione di informazioni a diversi livelli tra gli Stati membri e la Commissione è stata incoraggiante. Le interruzioni non hanno avuto effetti immediati in termini di connettività internet né per la sicurezza dell'approvvigionamento di gas a livello europeo o locale, e questo è un segno dei progressi compiuti e dell'intensificazione delle attività di preparazione degli ultimi mesi.

Pertanto è essenziale un quadro giuridico chiaro e solido per garantire la protezione e la resilienza di queste infrastrutture critiche. In questo contesto l'adozione parallela della direttiva riveduta relativa a misure per un livello comune elevato di cibersicurezza nell'Unione

(direttiva NIS 2)[4] e della direttiva relativa alla resilienza dei soggetti critici (direttiva CER)[5], entrambe entrate in vigore il 16 gennaio 2023, ha rappresentato un punto di svolta. Ora gli Stati membri sono invitati a recepire rapidamente e pienamente questi atti legislativi fondamentali, al più tardi entro il 17 ottobre 2024, per stabilire un solido quadro dell'Unione al fine di proteggerne le infrastrutture critiche dalle minacce fisiche e cibernetiche.

A luglio 2023 la Commissione ha elencato in un regolamento delegato i servizi essenziali negli 11 settori di cui alla direttiva CER[6]. Il passo successivo spetta agli Stati membri, che devono effettuare le valutazioni del rischio relative a questi servizi. In seguito alla raccomandazione del Consiglio[7] dell'8 dicembre 2022 si sono intensificati i lavori sulle prove di stress delle infrastrutture critiche, iniziando dal settore energetico, e sul rafforzamento della cooperazione con la NATO e i paesi partner più importanti. I lavori sono sfociati nel giugno 2023 in una relazione della task force UE-NATO sulla resilienza delle infrastrutture critiche, che definisce le attuali sfide di sicurezza suddivise in quattro settori chiave (energia, trasporti, infrastrutture digitali e spazio) e formula raccomandazioni per potenziare la resilienza. Il personale dell'UE e della NATO sta dando seguito alle raccomandazioni, tra cui quelle riguardanti un aumento in termini di coordinamento, condivisione delle informazioni ed esercitazioni, nel contesto del dialogo strutturato sulla resilienza.

In parallelo, il 6 settembre 2023, la Commissione ha adottato una proposta di raccomandazione del Consiglio relativa a un programma per coordinare una risposta a livello dell'Unione alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera[8]. Il 4 ottobre 2023 è stata organizzata un'esercitazione in forma di discussione, basata su uno scenario riguardante il programma, per verificarne l'applicazione pratica e fornire informazioni utili ai negoziati sulla proposta in seno al Consiglio.

In seguito agli inviti del Consiglio[9], la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS hanno effettuato varie valutazioni dei rischi e hanno elaborato scenari di rischio secondo la prospettiva della cibersicurezza. Questi lavori si sono incentrati inizialmente sui settori delle telecomunicazioni e dell'elettricità. Il coinvolgimento di tutte le pertinenti agenzie e reti, civili e militari, genera per la prima volta una valutazione completa e inclusiva a livello dell'Unione, che verrà a integrare le valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche che si stanno svolgendo a norma della direttiva NIS 2, come pure le valutazioni del rischio e le prove di stress delle infrastrutture critiche nei settori dell'energia, delle comunicazioni tramite infrastrutture digitali, dei trasporti e dello spazio. Nell'interesse del coordinamento e della coerenza, queste attività dovrebbero muovere da un terreno comune per contribuire a stabilire un approccio uniforme e dovrebbero orientare le esercitazioni future. Il successo di queste azioni dipenderà ora dall'impegno attivo degli Stati membri.

---

4 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione e direttiva (UE) 2018/1972 (direttiva NIS 2).

5 Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio.

6 C(2023) 4878 final.

7 Raccomandazione del Consiglio, dell'8 dicembre 2022, su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche.

8 COM(2023) 526 final.

9 Conclusioni del Consiglio, del 23 maggio 2022, sull'elaborazione di una posizione dell'Unione europea in materia di deterrenza informatica e appello lanciato a Nevers a favore del rafforzamento delle capacità di cibersicurezza dell'Unione adottato il 9 marzo 2022.

Il funzionamento delle economie e delle società dipende sempre più dai servizi e dai dati spaziali, soprattutto nel campo della sicurezza e della difesa. Lo spazio è un settore strategico sempre più conteso e la sua importanza per la sicurezza è cresciuta soprattutto in seguito all'invasione russa dell'Ucraina. La strategia spaziale dell'Unione europea per la sicurezza e la difesa è stata adottata a marzo 2023 per rafforzare la posizione strategica dell'Unione e la sua autonomia nello spazio. Nel 2024 la Commissione europea proporrà, come azione chiave derivante da questa strategia, una normativa dell'UE in materia di spazio che disciplini la sicurezza, la sostenibilità e la resilienza/sicurezza delle attività spaziali nell'UE.

Sul versante esterno, un'infrastruttura sicura è alla base della resilienza dell'economia mondiale e delle catene di approvvigionamento[10] e per questo motivo la strategia Global Gateway dell'UE racchiude in sé una forte dimensione di sicurezza. Date le interconnessioni tra le infrastrutture dell'UE e quelle dei paesi partner, una cooperazione internazionale più intensa è essenziale per rafforzare la ciberresilienza globale e sostenere un ciberspazio libero, aperto, sicuro e protetto.

Legge sulla ciberresilienza

Ai fini della cibersicurezza europea, è fondamentale garantire che i consumatori e le aziende possano contare su prodotti digitali sicuri. La Commissione ha cercato di rispondere a quest'esigenza con la proposta di legge sulla ciberresilienza[11], adottata il 15 settembre 2022. L'atto legislativo introdurrebbe obblighi orizzontali per la cibersicurezza dei prodotti con elementi digitali per un periodo di cinque anni o per la durata prevista del prodotto (a seconda di quale sia il periodo più breve). Creerebbe le condizioni per la progettazione e lo sviluppo di prodotti con elementi digitali sicuri garantendo che i prodotti hardware e software siano immessi sul mercato con il minor numero di vulnerabilità possibile. Si tratterebbe di una svolta decisiva nell'innalzamento dei livelli europei di cibersicurezza in tutti i settori e tale atto legislativo diventerebbe probabilmente un punto di riferimento internazionale, offrendo all'industria della cibersicurezza dell'Unione chiari vantaggi nei mercati globali. Il Parlamento europeo e il Consiglio hanno adottato la rispettiva posizioni a luglio 2023 e i negoziati dovrebbero avanzare rapidamente.

Anche la certificazione della cibersicurezza svolge un ruolo cruciale nell'aumentare la fiducia nei prodotti e nei servizi TIC, consentendo ai consumatori, alle imprese e alle autorità di effettuare scelte informate con un livello adeguato di cibersicurezza. I lavori su tale certificazione avanzano e il sistema europeo di certificazione della cibersicurezza basato sui criteri comuni è in fase di valutazione nell'ambito della procedura di comitato. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sta preparando una proposta di sistema europeo di certificazione della sicurezza dei servizi cloud, in discussione in seno al gruppo europeo per la certificazione della cibersicurezza. L'intenso lavoro svolto con esperti di diversi settori, consumatori e fornitori dovrebbe condurre a un solido approccio giuridico e tecnico in grado di offrire le necessarie garanzie di sicurezza in ottemperanza del diritto dell'Unione, degli impegni internazionali e degli obblighi nel quadro dell'OMC. L'ENISA sta inoltre preparando una proposta di sistema per le reti 5G (EU5G) e il portafoglio europeo di identità digitale. Le iniziative concertate di tutti gli Stati membri sono essenziali per potenziare la sicurezza generale dei prodotti, dei servizi e dei processi TIC.

Regolamenti sulla sicurezza delle informazioni e sulla cibersicurezza nelle istituzioni, negli organi e negli organismi dell'UE

[10] JOIN(2021) 30 final.
[11] COM(2022) 454 final.

Proposti insieme nel marzo 2022, i regolamenti per disciplinare la cibersicurezza e la sicurezza delle informazioni nelle istituzioni proprie dell'Unione sono progrediti a ritmi diversi. Lo scorso giugno è stato raggiunto un accordo politico sul regolamento sulla cibersicurezza, che ha permesso di rafforzare la posizione di cibersicurezza della totalità delle istituzioni, degli organi e degli organismi dell'UE, a dimostrazione dell'importanza che l'UE attribuisce alla rapida attuazione di questa proposta. Particolarmente preoccupanti in questa situazione sono i progressi inaspettatamente lenti della proposta parallela sulla sicurezza delle informazioni, essenziale per completare un solido quadro legislativo per le istituzioni, gli organi e gli organismi dell'UE. Entrambe le proposte dovrebbero essere adottate prima delle elezioni del Parlamento europeo, per rendere l'amministrazione europea credibile e resiliente nell'attuale contesto geopolitico. Un insieme minimo di regole e norme in materia di sicurezza delle informazioni per le istituzioni, gli organi e gli organismi dell'UE creerebbe certezza per tutte le parti coinvolte e garantirebbe una protezione coerente contro le crescenti minacce alle loro informazioni, classificate e non classificate UE. Nel complesso queste nuove regole fornirebbero una base stabile per lo scambio sicuro di informazioni tra le istituzioni, gli organi e gli organismi dell'UE e con gli Stati membri, con pratiche e misure standardizzate per proteggere i flussi di informazioni. Servono a rispondere ai molteplici inviti del Consiglio ad aumentare la resilienza delle istituzioni, degli organi e degli organismi dell'UE e a tutelare in maniera migliore il processo decisionale dell'Unione dalle interferenze dolose.

Regolamento sulla cibersolidarietà

Basato sul preesistente solido quadro strategico, politico e legislativo, la proposta di regolamento sulla cibersolidarietà[12], adottata dalla Commissione il 18 aprile 2023, dovrebbe migliorare il rilevamento delle minacce informatiche e rafforzare la resilienza e la preparazione a tutti i livelli dell'ecosistema di cibersicurezza dell'UE. Tali obiettivi dovrebbero essere realizzati mediante tre azioni principali:

(1) l'introduzione di un ***ciberscudo europeo*** per sviluppare e rafforzare le capacità comuni di rilevamento e di conoscenza situazionale, composto da centri operativi di sicurezza nazionali ("SOC nazionali") e transfrontalieri ("SOC transfrontalieri");
(2) la creazione di un ***meccanismo per le emergenze di cibersicurezza*** al fine di sostenere gli Stati membri a prepararsi e a rispondere agli incidenti significativi e su vasta scala in materia di cibersicurezza e a porvi riparo immediato. Il sostegno per rispondere agli incidenti includerebbe una riserva dell'UE per la cibersicurezza, che sarebbe anche a disposizione delle istituzioni, degli organi e degli organismi dell'UE e dei paesi terzi associati al programma Europa digitale, a condizione che il loro accordo di associazione al programma lo preveda;
(3) l'istituzione di un ***meccanismo europeo di riesame degli incidenti di cibersicurezza*** finalizzato al riesame e alla valutazione di specifici incidenti significativi o su vasta scala. Il riesame successivo all'incidente dovrebbe essere coordinato e preparato dall'ENISA.

La discussione in seno al Consiglio e al Parlamento europeo è stata avviata. La conclusione dei negoziati prima della fine dell'attuale legislatura darebbe un forte impulso alle iniziative volte a proteggere i cittadini e le imprese in tutta l'Unione.

Accademia per le competenze in materia di cibersicurezza

[12] COM(2023) 209 final.

Via via che le minacce informatiche aumentano, l'UE ha urgente necessità di professionisti con capacità e competenze per prevenire, individuare e scoraggiare i ciberattacchi e difendersi da essi. Il fabbisogno di forza lavoro nel settore della cibersicurezza è attualmente stimato in 883 000 professionisti, mentre nel 2022 i posti vacanti si aggiravano tra i 260 000 e i 500 000. Tutte le fasce della società dovrebbero essere incoraggiate a contribuire a colmare la penuria ma, in particolare nel 2022, le donne hanno rappresentato solo il 20 % dei laureati in cibersicurezza e il 19 % degli specialisti in tecnologie dell'informazione e della comunicazione. Il 18 aprile 2023[13], nell'ambito dell'Anno europeo delle competenze, la Commissione ha adottato un'iniziativa, accolta favorevolmente dagli Stati membri[14], volta alla costituzione di un'Accademia per le competenze in materia di cibersicurezza per colmare la carenza di talenti nel settore. L'Accademia per le competenze in materia di cibersicurezza dovrebbe riunire le iniziative esistenti in tale materia e migliorare il coordinamento. La Commissione incoraggia gli Stati membri, le autorità regionali e locali, come pure i soggetti pubblici europei, ad adottare strategie o iniziative dedicate alle competenze in materia di cibersicurezza, o a integrare tali competenze in strategie o iniziative pertinenti di portata più ampia (ad esempio, cibersicurezza, competenze digitali, occupazione ecc.) Anche il coinvolgimento dei portatori di interessi privati sarà essenziale per ridurre la carenza di competenze in materia di cibersicurezza e la relativa scarsità di manodopera in Europa.

Droni

L'uso doloso dei droni è un'altra minaccia in aumento per gli spazi pubblici e le infrastrutture critiche. Gli incidenti che coinvolgono i droni sono sempre più frequenti all'interno e all'esterno dell'Unione e le soluzioni anti-droni costituiscono uno strumento fondamentale per le autorità di contrasto e altre autorità pubbliche dell'Unione, oltre che per gli operatori privati di infrastrutture critiche. Allo stesso tempo l'uso legittimo dei droni offre un contributo importante alla duplice transizione verde e digitale[15]. Come annunciato nella strategia 2.0 per i droni adottata a novembre 2022, la Commissione ha adottato recentemente una comunicazione sulle modalità per contrastare le potenziali minacce poste dai droni; la comunicazione è accompagnata da due manuali che contengono orientamenti pratici sugli aspetti tecnici fondamentali[16]. L'iniziativa mira a tracciare un quadro politico completo e armonizzato e a definire una comprensione comune delle norme vigenti per combattere le possibili minacce poste dai droni e per adattarsi, se necessario, ai rapidi sviluppi della tecnologia. Gli Stati membri e gli operatori privati sono invitati a collaborare strettamente con la Commissione per garantire la piena attuazione dell'iniziativa.

Sicurezza marittima e aerea

Le attività illecite, come la pirateria, gli atti di depredazione armata in mare, il traffico di migranti e la tratta di esseri umani, il traffico di armi e stupefacenti, come pure il terrorismo, continuano a costituire una sfida per la sicurezza marittima e sono aggravate da minacce in evoluzione, tra cui gli attacchi ibridi e i ciberattacchi. Il 10 marzo 2023 la Commissione e l'alto rappresentante hanno adottato una comunicazione congiunta sull'aggiornamento della strategia per la sicurezza marittima dell'UE[17], che dovrebbe ora essere attuata in conformità del piano d'azione aggiornato.

---

[13] COM(2023) 207 final.
[14] Conclusioni del Consiglio del 22 maggio 2023 sulla politica dell'UE in materia di ciberdifesa.
[15] COM(2022) 652 final.
[16] COM(2023) 659 final.
[17] JOIN(2023) 8 final.

Per quel che riguarda il settore della sicurezza aerea, il 2 febbraio 2023 la Commissione ha adottato il documento di lavoro dei suoi servizi "Adoperarsi per una politica di sicurezza aerea rafforzata e più resiliente"[18], che riporta un programma ambizioso per 1) modernizzare l'architettura normativa in materia di sicurezza aerea, 2) promuovere l'elaborazione e l'adozione di soluzioni più innovative e 3) aggiornare la sicurezza aerea di base, in modo che gli aeroporti dell'Unione possano beneficiare appieno delle nuove tecnologie all'avanguardia per affrontare le minacce di massima priorità. Entro due anni devono essere attuate 14 azioni faro.

La Commissione invita il Parlamento europeo e il Consiglio a concludere con urgenza, e in ogni caso prima della fine dell'attuale legislatura, i negoziati relativi ai fascicoli seguenti:

- proposta di legge sulla ciberresilienza;
- proposta di regolamento sulla cibersolidarietà;
- regolamento proposto sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'UE.

La Commissione invita gli Stati membri a:

- portare avanti in via prioritaria il recepimento della direttiva sulla resilienza dei soggetti critici, e le prove di stress delle infrastrutture critiche del settore energetico;
- adottare la raccomandazione del Consiglio relativa a un programma per coordinare una risposta alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera;
- recepire pienamente e con urgenza la direttiva NIS 2 per potenziare la cibersicurezza di soggetti essenziali e importanti;
- impegnarsi attivamente nell'esecuzione di valutazioni dei rischi di cibersicurezza e nella costruzione di scenari di rischio per le infrastrutture critiche e le catene di approvvigionamento;
- dare seguito all'Accademia per le competenze in materia di cibersicurezza mostrando un impegno deciso a livello europeo e dedicando strategie o iniziative nazionali alle competenze in materia di cibersicurezza con il coinvolgimento dei principali portatori di interessi, comprese le autorità regionali e locali;
- collaborare con gli operatori privati e con la Commissione per garantire l'attuazione di tutte le azioni elencate nella comunicazione sul contrasto alle potenziali minacce poste dai droni;
- attuare il piano d'azione della strategia per la sicurezza marittima dell'UE e riferire regolarmente sui risultati ottenuti;
- attuare le 14 azioni faro identificate per migliorare la sicurezza aerea.

III. Far fronte alle minacce in evoluzione

Le nuove tensioni geopolitiche hanno dimostrato chiaramente che la sfida alla sicurezza per l'UE non solo è in aumento, ma è sempre più volatile e accentuata dalla natura ibrida di molte minacce. La sicurezza deve rispondere anche ai cambiamenti della società e della tecnologia. Durante la pandemia di COVID-19 si sono potenziate le occasioni per i criminali informatici

[18] SWD(2023) 37 final.

e in particolare si è aggravata la minaccia posta dal materiale pedopornografico online. Criminali e malintenzionati sono sempre pronti a sfruttare gli sviluppi tecnologici. A fronte di queste minacce, spesso complesse e multidimensionali, è necessaria un'azione forte e coerente dell'UE.

Regolamento sulla lotta contro l'abuso sessuale su minori online

La valutazione della minaccia della criminalità organizzata su internet eseguita da Europol ha rivelato che nel 2022 lo sfruttamento e l'abuso sessuale di minori sono aumentati ulteriormente in termini di frequenza e gravità, mentre i criminali seguitano a sfruttare le possibilità tecniche per dissimulare azioni e identità[19]. L'attuale sistema di protezione dei minori basato sulla rilevazione volontaria e la segnalazione da parte delle imprese si è rivelato insufficiente. La rilevazione volontaria e la segnalazione da parte delle imprese è consentita, subordinatamente all'ottemperanza del regolamento generale sulla protezione dei dati (GDPR), da un regolamento provvisorio, che scadrà ad agosto 2024. A maggio 2022 la Commissione ha proposto un regolamento[20] per contrastare l'uso improprio dei servizi online a fini di abuso sessuale su minori. Il quadro proposto pone un forte accento sulla prevenzione. Le imprese sarebbero obbligate a valutare il rischio di abusi sessuali su minori attraverso i loro sistemi e ad adottare misure preventive. Come misura di ultima istanza, solo in caso di rischio significativo, le autorità giudiziarie nazionali o le autorità amministrative indipendenti potrebbero emettere ordini di rilevazione destinati ai prestatori di servizi. Un nuovo centro indipendente dell'UE agevolerebbe gli sforzi dei prestatori di servizi, fungendo da centro di competenza, fornendo informazioni attendibili sul materiale individuato, ricevendo e analizzando le segnalazioni di abusi sessuali su minori online da parte dei prestatori per individuare quelle errate e fornendo sostegno alle vittime. È essenziale che le nuove norme siano adottate e attuate al più presto per proteggere i minori da ulteriori abusi, impedire che il materiale ricompaia online e assicurare i colpevoli alla giustizia. In sede di Consiglio e Parlamento sono in corso negoziati con l'obiettivo di trovare un accordo sul fascicolo prima della fine della legislatura.

Direttiva sulla lotta alla violenza contro le donne e alla violenza domestica

La ciberviolenza contro le donne, anche nel contesto domestico, è emersa come forma nuova di violenza che, attraverso internet e gli strumenti informatici, si diffonde e si amplifica oltre i confini dei singoli Stati membri. A marzo 2022 la Commissione ha proposto una direttiva per contrastare la violenza contro le donne e la violenza domestica, che comprende norme specifiche sulla violenza online e misure per colmare le lacune relative alla protezione, all'accesso alla giustizia e alla prevenzione. L'adozione e l'attuazione tempestive fornirebbero agli Stati membri strumenti supplementari per combattere questa forma di criminalità. I colegislatori hanno avviato i negoziati interistituzionali nel luglio 2023 e puntano a concluderli prima della fine dell'attuale legislatura.

Cibersicurezza delle reti 5G

La sicurezza delle reti 5G è una delle principali priorità della Commissione e una componente essenziale della strategia per l'Unione della sicurezza. Le reti 5G costituiscono un'infrastruttura centrale, fondamento di un'ampia gamma di servizi essenziali per il funzionamento del mercato interno e per funzioni sociali ed economiche di vitale importanza. Il 15 giugno 2023 le autorità degli Stati membri dell'UE rappresentate nel gruppo di

[19] Valutazione della minaccia della criminalità organizzata su internet, Europol, 2023.
[20] COM(2022) 209 final.

cooperazione NIS, con il sostegno della Commissione e dell'ENISA, hanno pubblicato una seconda relazione sullo stato di avanzamento dell'attuazione del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G. Secondo la relazione 24 Stati membri hanno adottato o stanno preparando misure legislative che conferiscono alle autorità nazionali il potere di effettuare una valutazione dei fornitori e di imporre restrizioni, e 10 Stati membri hanno imposto tali restrizioni. Sono tuttavia necessarie ulteriori azioni per scongiurare la presenza di vulnerabilità per l'Unione nel suo complesso che abbiano ripercussioni negative potenzialmente gravi sulla sicurezza dei singoli utenti e delle imprese in tutta l'Unione come pure sulle infrastrutture critiche dell'Unione. Occorre che tutti gli Stati membri attuino senza indugio il pacchetto di strumenti. Lo stesso giorno la Commissione ha adottato una comunicazione sull'attuazione del pacchetto di strumenti da parte degli Stati membri, sulle comunicazioni istituzionali della Commissione e sulle attività di finanziamento dell'Unione. Nella comunicazione si sottolineano le forti preoccupazioni in merito ai rischi per la sicurezza dell'UE posti dai fornitori di apparecchiature di comunicazione sulle reti mobili Huawei e ZTE. In questo contesto la Commissione sta adottando misure per evitare l'esposizione delle proprie comunicazioni istituzionali alle reti mobili che utilizzano Huawei e ZTE come fornitori. Gli appalti escluderanno nuovi servizi di connettività basati su apparecchiature di tali fornitori e la Commissione collaborerà con gli Stati membri e con gli operatori delle telecomunicazioni affinché tali fornitori siano esclusi progressivamente dagli attuali servizi di connettività delle sedi della Commissione. La Commissione sta inoltre valutando come i programmi e gli strumenti di finanziamento dell'Unione possano rispecchiare tale decisione nel totale rispetto del diritto dell'Unione.

Accesso ai dati per azioni di contrasto efficaci

Nell'odierna era digitale quasi tutti i reati presentano una componente digitale. Tecnologie e strumenti, compresi quelli necessari a soddisfare le esigenze della nostra società in termini di cibersicurezza, protezione dei dati e riservatezza, sono utilizzati anche per scopi criminosi. Questa realtà rende sempre più difficile portare avanti azioni di contrasto efficaci in tutta l'UE allo scopo di salvaguardare la sicurezza pubblica e di prevenire, rilevare, indagare e perseguire i reati. Nonostante siano stati compiuti sforzi significativi a livello dell'Unione e nazionale, anche tramite la legislazione e le iniziative di sviluppo delle capacità e di innovazione, persistono problemi giuridici e tecnici. La Commissione, unitamente alla presidenza del Consiglio, ha istituito un gruppo ad alto livello sull'accesso ai dati per un'efficace azione di contrasto, allo scopo di fornire una piattaforma collaborativa per un'ampia gamma di portatori di interessi ed esperti, volta a esaminare le sfide che le autorità di contrasto si trovano ad affrontare (ad esempio, crittografia, conservazione dei dati, 5G e standardizzazione). La Commissione si attende che entro giugno 2024 il gruppo ad alto livello formuli raccomandazioni equilibrate, solide e realizzabili, che rispecchino la complessità di questi temi, anche dalla prospettiva della cibersicurezza e da quella della protezione dei dati. Gli Stati membri e gli esperti partecipanti sono quindi incoraggiati a impegnarsi attivamente in tale processo e ad adoperarsi per trovare soluzioni efficaci, legittime e accolte da tutti.

Minacce ibride

In un contesto geopolitico in cui le minacce ibride sono sempre più complesse e sofisticate, la bussola strategica dell'UE per la sicurezza e la difesa[21] (bussola strategica) ha fornito una valutazione condivisa delle minacce e delle sfide cui l'Unione deve far fronte unitamente a un piano d'azione strategico. L'aumento dei comportamenti dolosi compiuti nel ciberspazio da

[21] Documento 7371/22 del Consiglio.

Stati e soggetti non statali, anche nel contesto della guerra contro l'Ucraina, ha reso ancor più evidente il fatto che il settore del ciberspazio rientra nella politica estera e della sicurezza. I rischi potenziali di azioni dolose e di disinformazione richiedono una particolare vigilanza nei periodi elettorali, anche in vista delle elezioni europee del 2024.

Considerati gli elevati rischi di effetti di ricaduta, l'UE ha continuato a svolgere attività di sviluppo delle capacità informatiche e a promuovere partenariati con i paesi terzi, anche tramite appositi ciberdialoghi, per contribuire attivamente alla propria resilienza complessiva. Sono stati elaborati, rivisti e rafforzati diversi strumenti per aumentare la capacità dell'Unione di far fronte efficacemente alle minacce ibride, come descritto nella settima relazione sullo stato di avanzamento dei lavori sulle minacce ibride pubblicata il 14 settembre 2023[22]. Tra tali strumenti figurano:

- il pacchetto di strumenti dell'UE contro le minacce ibride, che garantisce un quadro per una risposta coordinata e ben informata alle minacce e alle campagne ibride;
- i lavori in corso per la creazione di gruppi di risposta rapida dell'UE alle minacce ibride, che sostengano a breve termine e in modo mirato gli Stati membri, i paesi partner e le missioni e operazioni della politica di sicurezza e di difesa comune (PSDC);
- il protocollo rivisto dell'UE per contrastare le minacce ibride ("EU Playbook")[23], che descrive i processi e le strutture dell'Unione riguardanti le minacce e le campagne ibride;
- gli orientamenti di attuazione rivisti del quadro relativo a una risposta diplomatica comune alle attività informatiche dolose[24] ("pacchetto di strumenti della diplomazia informatica"), che permettono di elaborare strategie durature, mirate, coerenti e coordinate contro gli autori di minacce informatiche persistenti;
- il pacchetto di strumenti sulla manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri, per rafforzare gli strumenti esistenti volti a prevenire e scoraggiare tale manipolazione e a rispondervi;
- la politica di ciberdifesa dell'UE[25] per potenziare le capacità di ciberdifesa, aumentare la conoscenza situazionale e coordinare tutte le opzioni difensive disponibili al fine di rafforzare la resilienza, rispondere ai ciberattacchi e garantire la solidarietà e l'assistenza reciproca.

Gli Stati membri sono pertanto incoraggiati a proseguire e rafforzare la cooperazione in questo settore, assicurando l'efficace attuazione dei pacchetti di strumenti citati sopra, anche con esercitazioni periodiche, e trovando un accordo sul concetto di "gruppi di risposta rapida alle minacce ibride" che fornisca indicazioni sul modo in cui procedere verso l'istituzione di tali gruppi.

L'IA nel contesto delle attività di contrasto

L'intelligenza artificiale (IA) è diventata rapidamente una componente comune della vita quotidiana. Gli effetti dell'uso dell'IA sulla cibercriminalità e sulla cibersicurezza non sono ancora del tutto noti, ma è chiaro che si profileranno nuove sfide. Da un lato l'IA, utilizzata in modo sicuro e controllato, può comportare vantaggi; dall'altro, nelle mani di soggetti malintenzionati, può essere pericolosa, ad esempio aiutando i criminali a dissimulare la propria identità in reati quali il terrorismo o l'abuso sessuale su minori. È quindi essenziale

[22] SWD(2023) 315 final.
[23] SWD(2023) 116 final.
[24] 10289/23 dell'8 giugno 2023.
[25] JOIN(2022) 49 final.

che le autorità si tengano aggiornate sugli sviluppi per prevenire gli abusi e rispondere agli usi impropri[26]. I negoziati sulla normativa sull'intelligenza artificiale proposta, che mirano ad affrontare questi problemi, sono entrati in una fase cruciale in cui i colegislatori discutono questioni tecniche e politiche che determineranno le interazioni con questa tecnologia negli anni a venire. Sarà fondamentale trovare soluzioni equilibrate, soprattutto per quanto riguarda le applicazioni ad alto rischio, tra cui quelle nell'ambito delle attività di contrasto.

La Commissione invita il Parlamento europeo e il Consiglio a concludere con urgenza, e in ogni caso prima della fine dell'attuale legislatura, i negoziati interistituzionali relativi ai fascicoli in sospeso seguenti:

- proposta di regolamento sulla lotta contro l'abuso sessuale su minori online;
- proposta di direttiva sulla lotta alla violenza contro le donne e alla violenza domestica;
- proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale).

La Commissione invita gli Stati membri a:

- attuare integralmente e senza indugio il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G;
- sostenere i lavori del gruppo ad alto livello sull'accesso ai dati per azioni di contrasto efficaci, al fine di formulare raccomandazioni chiare, solide e realizzabili per far fronte in modo proporzionato alle sfide attuali e previste;
- adoperarsi, in collaborazione con l'alto rappresentante, per garantire l'efficace attuazione del pacchetto di strumenti dell'UE contro le minacce ibride, il pacchetto di strumenti della diplomazia informatica rivisto e il pacchetto di strumenti sulla manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri, anche con esercitazioni periodiche e considerando le dinamiche mondiali;
- raggiungere un accordo sul concetto di "gruppi di risposta rapida alle minacce ibride".

IV. Tutelare i cittadini europei dal terrorismo e dalla criminalità organizzata

Il rischio che eventi a livello mondiale o locale provochino nuove ondate di terrorismo è sempre presente. Nel contempo la criminalità organizzata e il traffico di stupefacenti sono tra le minacce più gravi alla sicurezza dell'UE. Per intensificare l'impegno dell'Unione nella lotta contro queste minacce, è in corso un lavoro collettivo volto ad attuare la strategia dell'UE per la lotta alla criminalità organizzata[27], la strategia dell'UE per la lotta alla tratta di esseri umani[28], l'agenda e il piano d'azione dell'UE in materia di droga[29] e il programma dell'UE di lotta al terrorismo[30]. Per far fronte al preoccupante peggioramento della situazione relativamente alla criminalità organizzata e al traffico di droga, è tuttavia necessario che gli

[26] Cfr. ad esempio la relazione di Europol pubblicata il 17 aprile 2023: "ChatGPT - the impact of Large Language Models on Law Enforcement".
[27] COM(2021) 170 final.
[28] COM(2021) 171 final.
[29] COM(2020) 606 final.
[30] COM(2020) 795 final.

Stati membri e l'UE intensifichino ulteriormente le attività al fine di rafforzare la risposta collettiva alle reti criminali e di tutelare meglio le vittime di reato; una tabella di marcia dell'UE per contrastare il traffico di droga e la criminalità organizzata è in corso di pubblicazione contemporaneamente alla presente relazione[31]

Nel settore dell'antiterrorismo l'UE sta rafforzando anche il pacchetto di strumenti per l'azione esterna[32], sfruttando appieno i dialoghi ad alto livello sulla lotta al terrorismo, la rete di esperti in materia di antiterrorismo/sicurezza nelle delegazioni dell'UE, come pure mediante i contatti nei forum multilaterali, ad esempio come copresidente del Forum globale contro il terrorismo.

Traffico di stupefacenti

Grazie al nuovo mandato dell'Agenzia dell'Unione europea sulle droghe, che si applicherà a partire da luglio 2024, l'UE sarà attrezzata meglio per affrontare un complesso problema sanitario e di sicurezza che interessa milioni di persone nell'UE e sul piano mondiale. La Commissione sta rivedendo[33] i regolamenti sui precursori di droghe[34] per parare le principali criticità emerse dalla valutazione del 2020[35], che ha evidenziato la necessità di rispondere alla sfida rappresentata dai precursori di progettazione[36] per ridurre l'offerta di droghe illegali.

A fronte dell'aumento senza precedenti della disponibilità di droghe illecite in Europa, la lotta al traffico di stupefacenti deve tuttavia intensificarsi, in collaborazione con i partner internazionali. Sono necessari provvedimenti supplementari da parte degli Stati membri e dell'UE per smantellare le reti della criminalità e tutelare meglio le vittime di reati. La Commissione ha presentato recentemente una tabella di marcia dell'UE per contrastare il traffico di droga e la criminalità organizzata, che prevede 17 azioni in quattro settori prioritari: rafforzare la resilienza dei centri logistici con un'Alleanza europea dei porti, smantellare le reti criminali, aumentare le attività di prevenzione e intensificare la cooperazione con i partner internazionali. L'attuazione di queste azioni è prevista per il 2024 e il 2025.

Armi da fuoco

Il traffico di armi da fuoco alimenta la criminalità organizzata all'interno dell'UE e nei paesi del vicinato. Si stima che ben 35 milioni di armi da fuoco illegali siano detenute da civili nell'UE e circa 630 000 armi da fuoco risultano rubate o smarrite nel sistema d'informazione Schengen. Con lo sviluppo dei servizi di consegna rapida dei pacchi e di nuove tecnologie come la stampa 3D, il traffico di armi da fuoco assume forme nuove che permettono di sfuggire ai controlli. Anche la guerra di aggressione della Russia contro l'Ucraina ha aumentato il rischio di proliferazione delle armi da fuoco. A ottobre 2022 la Commissione ha adottato una proposta per aggiornare la legislazione vigente in materia di importazione, esportazione e transito di armi da fuoco ad uso civile, al fine di colmarne le lacune normative che rischiano di aumentare il numero di armi da fuoco introdotte illegalmente e sviate nell'UE[37]. A medio termine queste nuove norme contribuiranno a ridurre il rischio di elusione

---

31 COM(2023) 641 final.

32 Come richiesto dalla bussola strategica e dalle conclusioni del Consiglio "Affrontare la dimensione esterna di una minaccia terroristica e di estremismo violento in costante evoluzione", concentrandosi sulla dimensione esterna, adottata nel giugno 2022.

33 Precursori di droghe - legislazione dell'UE (norme rivedute) (europa.eu)

34 Regolamento (CE) n. 273/2004 del Parlamento europeo e del Consiglio, dell'11 febbraio 2004, relativo ai precursori di droghe e regolamento (CE) n. 111/2005 del Consiglio, del 22 dicembre 2004, recante norme per il controllo del commercio dei precursori di droghe tra la Comunità e i paesi terzi.

35 COM(2020) 768 final.

36 Piano d'azione in materia di droga, azione 23 (COM(2020) 606).

37 COM(2022) 480 final.

degli embarghi in caso di esportazione di armi da fuoco ad uso civile e ad aumentare i controlli sulle importazioni da paesi terzi. I colegislatori devono ancora adottare la rispettiva posizione su questo fascicolo e l'obiettivo è trovare un accordo prima della fine della legislatura.

Tratta di esseri umani

La tratta di esseri umani è una forma particolarmente grave di criminalità organizzata nonché una pesante violazione dei diritti fondamentali. Le vittime della tratta sono trasferite nell'UE principalmente a fini di sfruttamento sessuale e lavorativo, ma anche per forzarle all'accattonaggio, ad atti criminosi e altro. A dicembre 2022 la Commissione ha proposto la modifica della direttiva anti-tratta[38] al fine di aggiornarne le norme per correggere i limiti del quadro giuridico vigente. In particolare, l'ambito di applicazione della direttiva modificata includerebbe, una volta adottato l'atto, il matrimonio forzato e l'adozione illegale; vi sarebbe introdotto un riferimento esplicito alla dimensione online della tratta di esseri umani. Si introdurrebbe un regime obbligatorio di sanzioni per gli autori di reato e si formalizzerebbe l'istituzione di meccanismi di orientamento nazionali volti a migliorare l'identificazione tempestiva e la segnalazione transfrontaliera per offrire assistenza e sostegno alle vittime. L'utilizzo consapevole di servizi offerti da vittime di tratta diverrebbe un reato e la raccolta annuale di dati sulla tratta di esseri umani, pubblicati da Eurostat, diventerebbe obbligatoria. Il Consiglio ha adottato l'orientamento generale a giugno 2023, mentre il Parlamento europeo deve ancora adottare la posizione. Sarà necessario agire rapidamente per trovare un accordo prima della fine della legislatura.

Reati contro l'ambiente

La criminalità ambientale è diventata una minaccia mondiale che annualmente cresce a un tasso stimato tra il 5 % e il 7 %. I notevoli profitti che possono essere generati, le lacune giuridiche di uno Stato membro rispetto a un altro e il basso rischio di essere scoperti sono tutti elementi di attrazione per la criminalità organizzata. Europol rileva indicazioni del fatto che i proventi di queste attività sono utilizzati per finanziare il terrorismo. A dicembre 2021 la Commissione ha adottato una proposta per sostituire la direttiva del 2008 sulla tutela penale dell'ambiente. La proposta è incentrata sul perfezionamento e sull'aggiornamento delle definizioni delle categorie di reati ambientali e sulla definizione dei tipi e livelli di sanzioni effettive, proporzionate e dissuasive comminabili alle persone fisiche e giuridiche. Tra i nuovi reati figurano quelli legati alla deforestazione illegale, alle violazioni della legislazione dell'UE in materia di sostanze chimiche, all'estrazione illegale di acque superficiali o sotterranee e al riciclaggio illegale delle navi. La proposta mira a rafforzare in modo significativo la catena di applicazione della legge e la cooperazione transfrontaliera tra le autorità degli Stati membri e gli organi e organismi dell'UE. Il Parlamento europeo e il Consiglio hanno adottato la rispettiva posizione sulla proposta e sono in corso negoziati che dovrebbero concludersi entro la fine dell'anno. Occorre che sia attuato un piano d'azione riveduto[39] contro il traffico illegale di specie selvatiche per rafforzare ulteriormente la prevenzione e le attività di contrasto.

Recupero e confisca dei beni

Privare i criminali dei loro proventi illeciti è fondamentale per contrastare la criminalità organizzata. Per questo motivo, oltre alla proposta che consente alle autorità di contrasto di

[38] COM(2022) 732 final.
[39] COM(2022) 581 final.

accedere alle informazioni sui conti bancari in tutta l'UE[40] (per la quale è stato raggiunto un accordo politico nel giugno 2023), a maggio 2022 la Commissione ha presentato una proposta riguardante il recupero e la confisca dei beni[41] per rafforzare le capacità di reperimento, identificazione, congelamento, confisca e gestione dei beni. Le disposizioni principali della proposta riguardano le condizioni per le indagini finanziarie, i poteri e gli strumenti supplementari degli uffici per il recupero dei beni e misure di congelamento e confisca più efficaci per una serie più ampia di reati. Una delle nuove fattispecie di reato per le quali saranno applicabili tali misure è la violazione delle misure restrittive dell'Unione. A dicembre 2022 la Commissione ha adottato una proposta distinta per armonizzare le definizioni penali della violazione delle misure restrittive dell'Unione e le relative sanzioni. L'efficace attuazione e applicazione delle misure restrittive dell'Unione resta una priorità assoluta per la Commissione, rafforzata dal lavoro della task force "Freeze and Seize" da essa istituita in risposta alla guerra di aggressione della Russia contro l'Ucraina. Su entrambe le proposte il Parlamento europeo e il Consiglio hanno adottato la rispettiva posizione con l'obiettivo di trovare un accordo entro la fine di quest'anno.

Pacchetto antiriciclaggio

Il riciclaggio è collegato praticamente a tutte le attività criminose che generano proventi illeciti nell'UE[42] ed è quindi un elemento essenziale nell'ambito della lotta alla criminalità nell'UE. A luglio 2021 la Commissione ha presentato proposte ambiziose per rafforzare le misure dell'UE volte a prevenire il riciclaggio e il finanziamento del terrorismo[43], con quattro proposte legislative tese a rafforzare la prevenzione e la rilevazione di tentativi da parte di criminali di riciclare proventi illeciti o di finanziare attività terroristiche mediante il sistema finanziario. A maggio 2023[44] è stata adottata dai colegislatori una delle quattro iniziative del pacchetto, per garantire la tracciabilità dei trasferimenti di cripto-attività. Il regolamento si applicherà a decorrere dal 30 dicembre 2024, data entro la quale tutti i prestatori di servizi di cripto-attività dovranno raccogliere e conservare informazioni sul cedente e sul cessionario di trasferimenti di cripto-attività. Le altre tre proposte mirano a: i) istituire una nuova autorità antiriciclaggio dell'UE per assicurare una supervisione coerente e di alta qualità nel mercato interno, compresi i soggetti che operano su base transfrontaliera più a rischio, sostenendo e coordinando il lavoro delle unità di informazione finanziaria; ii) fissare norme armonizzate per il settore privato, compresa l'introduzione a livello dell'UE di un limite di 10 000 EUR nei pagamenti in contanti di importo elevato per l'acquisto di beni e servizi, e iii) rafforzare i poteri e gli strumenti di cooperazione delle autorità competenti. Tale pacchetto dovrebbe migliorare significativamente la capacità dell'UE di combattere il riciclaggio di denaro e proteggere i cittadini dall'UE contro il terrorismo e la criminalità organizzata. Le tre proposte in sospeso sono attualmente oggetto di negoziazione da parte dei colegislatori con l'obiettivo di giungere a un accordo prima della fine della legislatura.

La Commissione invita il Parlamento europeo e il Consiglio a concludere con urgenza, e in ogni caso prima della fine dell'attuale legislatura, i negoziati interistituzionali relativi ai fascicoli in sospeso seguenti:

[40] COM(2021) 429 final.
[41] COM(2022) 245 final.
[42] "Enterprising criminals – Europe's fight against the global networks of financial and economic crime", Europol, 2020.
[43] COM(2021) 420 final.
[44] Regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio, del 31 maggio 2023, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la direttiva (UE) 2015/849.

- proposta di direttiva riguardante il recupero e la confisca dei beni;
- proposta di direttiva per armonizzare le definizioni penali della violazione delle misure restrittive dell'Unione e le relative sanzioni;
- proposta di direttiva anti-tratta;
- proposta di direttiva che migliora la tutela penale dell'ambiente;
- proposta di un pacchetto antiriciclaggio;
- proposta per aggiornare la legislazione vigente in materia di importazione, esportazione e transito di armi da fuoco ad uso civile.

La Commissione invita gli Stati membri, gli organi e gli organismi dell'UE a:

- collaborare per attuare nel 2023 e nel 2024 le 17 azioni della tabella di marcia dell'UE per contrastare il traffico di droga e la criminalità organizzata.

V. Un ecosistema europeo forte in materia di sicurezza

In questi ultimi anni la natura transfrontaliera delle minacce alla sicurezza si è accentuata sempre più e ciò richiede ulteriori sinergie e una cooperazione più serrata a tutti i livelli. Dall'adozione della strategia per l'Unione della sicurezza sono state intraprese importanti iniziative per massimizzare la cooperazione transfrontaliera, razionalizzando e migliorando gli strumenti e le procedure disponibili sia alle frontiere esterne sia all'interno dello spazio Schengen, come pure aumentando lo scambio di informazioni tra le autorità di contrasto e quelle giudiziarie al fine di combattere meglio la criminalità organizzata. In tale contesto l'efficace attuazione del quadro di interoperabilità per lo scambio di dati è un pilastro importante per rafforzare la sicurezza e rendere ancor più efficace la risposta europea alle minacce transfrontaliere, garantendo nel contempo la libera circolazione interna.

Maggiore scambio di informazioni nello spazio Schengen: informazioni anticipate sui passeggeri (dati API), codici di prenotazione (PNR) e Prüm II

Le due proposte API adottate dalla Commissione a dicembre 2022[45] rafforzeranno la sicurezza interna dell'Unione fornendo alle autorità di contrasto degli Stati membri strumenti supplementari per combattere i reati gravi e il terrorismo. In particolare le informazioni anticipate sui passeggeri dei voli intra-UE, utilizzate insieme ai PNR dei viaggiatori aerei, consentirebbero alle autorità di contrasto degli Stati membri di aumentare significativamente l'efficienza delle indagini con interventi più mirati. È importante che le norme proposte siano adottate al più presto: in tal modo non solo si sosterrebbe la lotta contro la criminalità organizzata e il terrorismo, ma si ridurrebbe anche in modo significativo la necessità di controlli sistematici su tutti i viaggiatori in caso di ripristino temporaneo dei controlli alle frontiere interne, facilitando i viaggi aerei e la libera circolazione. Il 6 settembre 2023 la Commissione europea ha raccomandato dal Consiglio di autorizzare l'avvio di negoziati con la Svizzera, l'Islanda e la Norvegia per la conclusione di accordi sul trasferimento dei dati PNR. L'adozione di queste tre raccomandazioni sosterrebbe una politica esterna dell'UE in materia di dati PNR coerente ed efficace.

Il sistema di scambio di informazioni nel quadro di Prüm è utilizzato quotidianamente dalla polizia per combattere la criminalità organizzata, il traffico di stupefacenti, il terrorismo, lo sfruttamento sessuale e la tratta di esseri umani. La proposta di regolamento sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II")[46] rivede l'attuale quadro di

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784 final.

Prüm al fine di colmare le lacune informative e aumentare la prevenzione, l'indagine e l'accertamento dei reati nell'UE. Le norme rivedute in materia di scambio automatizzato di dati per la cooperazione di polizia completano le proposte sulla cooperazione di polizia presentate durante l'attuale legislatura, insieme alla raccomandazione del Consiglio già adottata, che rafforza la cooperazione operativa transfrontaliera, e alla direttiva sullo scambio di informazioni tra le autorità di contrasto. La rapida adozione e attuazione di questi strumenti collegati migliorerebbe, faciliterebbe e accelererebbe lo scambio di dati tra le autorità di contrasto e contribuirebbe all'individuazione dei criminali.

Sistema di gestione delle frontiere pienamente interoperabile per uno spazio Schengen sicuro, forte, digitale e unito

Uno spazio Schengen senza frontiere interne funzionante s'impernia sulla fiducia reciproca tra gli Stati membri, la quale, a sua volta, si basa su controlli efficienti sia alle frontiere esterne dell'Unione sia come misure alternative sul territorio degli Stati membri. La modifica del codice frontiere Schengen proposta dalla Commissione[47] stabilisce in quale modo gli Stati membri possono utilizzare meglio le alternative ai controlli alle frontiere interne, che offrono la possibilità di un elevato livello di sicurezza. È importante che la modifica del codice sia adottata e attuata pienamente per garantire un livello di sicurezza elevato e proporzionato all'interno dello spazio Schengen. Prosegue anche lo sviluppo della nuova architettura dei sistemi di informazione dell'UE per sostenere meglio il lavoro delle autorità nazionali volto a garantire la sicurezza e la gestione delle frontiere. Gli elementi di tale architettura sono il sistema d'informazione Schengen rinnovato, il sistema europeo d'informazione e autorizzazione ai viaggi, il sistema di ingressi/uscite, l'aggiornamento del sistema d'informazione visti e il quadro di interoperabilità per collegare tra loro i sistemi in piena sicurezza. Una volta completata, questa nuova architettura fornirebbe alle autorità nazionali informazioni di sicurezza più esaurienti e attendibili. Tutti gli elementi del quadro di interoperabilità sono essenziali, pertanto un ritardo nell'ambito di un aspetto o da parte di uno Stato membro comporta un ritardo nell'introduzione per tutti. Dovrebbero essere ridotti al minimo i ritardi nello sviluppo tecnico del sistema di ingressi/uscite, in modo che possa essere operativo il prima possibile e che possano essere messi in atto tutti gli elementi fondamentali del quadro di interoperabilità.

La proposta sugli accertamenti[48] rafforzerebbe la sicurezza all'interno dello spazio Schengen introducendo norme uniformi per l'identificazione dei cittadini di paesi terzi che non soddisfano le condizioni di ingresso previste dal codice frontiere Schengen, e sottoponendoli a controlli sanitari e di sicurezza alle frontiere esterne. Il sistema Eurodac proposto sosterrebbe questi obiettivi indicando i casi in cui, in seguito agli accertamenti, una persona potrebbe rappresentare una minaccia per la sicurezza interna e, a sua volta, faciliterebbe l'attuazione della proposta di regolamento sulla gestione dell'asilo e della migrazione. La Commissione incoraggia i colegislatori a concludere rapidamente i negoziati su questi fascicoli prima della fine dell'attuale legislatura.

Lotta contro la corruzione

La corruzione è un fenomeno che reca gravi danni alle democrazie, all'economia e alla sicurezza, in quanto agisce da catalizzatore per la criminalità organizzata e le ingerenze straniere ostili. Prevenire e combattere efficacemente la corruzione è fondamentale sia per

[47] COM(2021) 891 final.
[48] COM(2020) 612 final.

salvaguardare i valori dell'Unione e l'efficacia delle sue politiche sia per difendere lo Stato di diritto e la fiducia nei confronti di governanti e istituzioni pubbliche. Come annunciato dalla presidente von der Leyen nel discorso sullo stato dell'Unione del 2022, il 3 maggio 2023 la Commissione ha adottato un pacchetto di misure anticorruzione[49]. La proposta di direttiva della Commissione sulla lotta contro la corruzione comprende norme rafforzate relative alla configurazione della corruzione come reato e all'armonizzazione delle sanzioni in tutta l'UE. Consente indagini e azioni penali efficaci e pone un forte accento sulla prevenzione e sull'instaurazione di una cultura dell'integrità in cui la corruzione non è tollerata. Le discussioni su tale proposta sono state avviate in sede di Parlamento europeo e di Consiglio. Gli Stati membri sono invitati inoltre ad attuare le raccomandazioni risultanti dal pilastro anticorruzione della relazione sullo Stato di diritto 2023, adottata il 5 luglio 2023. Anche la proposta dell'alto rappresentante, sostenuta dalla Commissione, stabilisce nell'ambito della politica estera e di sicurezza comune (PESC) un apposito regime di sanzioni per colpire i gravi atti di corruzione in tutto il mondo.

Rafforzare i diritti delle vittime

Il 12 luglio 2023 la Commissione ha proposto la modifica della direttiva sui diritti delle vittime, per rafforzare l'accesso delle vittime alle informazioni, al sostegno e alla protezione, la loro partecipazione ai procedimenti penali e l'accesso al risarcimento. Uno degli obiettivi generali della revisione è quello di contribuire a un elevato livello di sicurezza, creando ambienti più sicuri per la denuncia dei reati da parte delle vittime, riducendo il timore di subire ritorsioni.

La Commissione invita il Parlamento europeo e il Consiglio a concludere con urgenza, e in ogni caso prima della fine dell'attuale legislatura, i negoziati interistituzionali relativi ai fascicoli in sospeso seguenti:

- proposta relativa al regolamento Prüm II;
- proposte in materia di informazioni anticipate sui passeggeri (API);
- proposte in materia di lotta contro la corruzione, in particolare per quanto riguarda l'apposito regime di sanzioni nell'ambito della politica estera e di sicurezza comune (PESC);
- proposta di modifica del regolamento che istituisce il codice frontiere Schengen;
- proposta di direttiva sui diritti delle vittime;
- proposta sugli accertamenti.

La Commissione invita gli Stati membri a:

- garantire l'entrata in vigore del sistema di ingressi/uscite nel più breve tempo possibile affinché si completi l'attuazione dell'architettura dei sistemi di informazione dell'UE.

VI. Attuazione

Garantire la sicurezza dell'Europa nel suo insieme è una responsabilità condivisa, per la quale ogni soggetto deve assumersi le proprie responsabilità, dall'adozione di nuove norme solide, esaustive e pratiche da parte della Commissione e dei colegislatori, fino al recepimento e

[49] COM(2023) 234 final.

all'applicazione di tali norme da parte degli Stati membri o all'impegno concreto diretto assolto da varie autorità, organizzazioni e portatori di interessi. Anche le agenzie dell'UE nel settore della giustizia, degli affari interni e della cibersicurezza svolgono un ruolo centrale, che recentemente si è ulteriormente rafforzato con l'ampliamento delle loro competenze.

Migliorare il vaglio dei beneficiari dei finanziamenti UE

Nel dare esecuzione al bilancio dell'UE, la Commissione è tenuta ad accertare che i beneficiari dei finanziamenti dell'UE rispettino i valori dell'Unione. I meccanismi e i sistemi di controllo che determinano chi può beneficiare dei finanziamenti dell'UE sono già solidi; anche i negoziati in corso relativi alla rifusione del regolamento finanziario mirano a fornire alla Commissione strumenti giuridici più efficaci per agire se necessario. La Commissione è attualmente impegnata nell'elaborazione di modalità per perfezionare il vaglio dei beneficiari dei finanziamenti dell'UE attuali e futuri, migliorando gli orientamenti sugli obblighi relativi al rispetto dei valori dell'UE e sulle conseguenze in caso di una loro violazione. Saranno in tal modo precisate le responsabilità sia dei beneficiari sia di coloro che effettuano i controlli a livello dell'UE e tali precisazioni potranno fungere da modello anche a livello nazionale. In caso di violazione delle condizioni di finanziamento, la Commissione non esita e non esiterà a interrompere la cooperazione con i beneficiari del progetto e a recuperare i fondi se necessario. È importante che gli Stati membri che vengono a conoscenza di possibili rischi riguardanti le organizzazioni che richiedono i finanziamenti dell'UE condividano tali informazioni con la Commissione in modo proattivo.

Infrazioni

Nella settore della sicurezza la Commissione ha avviato e portato avanti numerosi procedimenti di infrazione. Ad esempio, nel 2023 la Commissione ha avviato numerosi procedimenti di infrazione per inadempimento degli obblighi derivanti dal regolamento del 2021 relativo alla diffusione di contenuti terroristici online[50] (16 Stati membri) e, nel corso degli anni 2022 e 2023, ha inviato altre lettere di messa in mora a 20 Stati membri per applicazione non corretta della direttiva del 2011 sulla lotta contro l'abuso sessuale su minori[51]. È ancora aperto un numero importante di procedure d'infrazione per mancata conformità della normativa nazionale alla direttiva del 2017 sulla lotta contro il terrorismo[52] e per mancato recepimento delle norme che facilitano l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati[53]. Tra le procedure di infrazione in corso figurano anche quelle riguardanti la normativa sulle armi da fuoco, le norme sulle sostanze psicoattive utilizzate come stupefacenti, la lotta alla frode e alla contraffazione dei mezzi di pagamento diversi dai contanti, la lotta al riciclaggio, lo scambio delle informazioni estratte dai casellari giudiziali tra gli Stati membri dell'UE e la direttiva sui diritti delle vittime. Un sostegno (tecnico e finanziario) è stato messo a

[50] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online.

[51] Direttiva (UE) 2011/93 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.

[52] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/G AI del Consiglio e che modifica la decisione 2005/671/G AI del Consiglio.

[53] 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, e che abroga la decisione 2000/642/GAI del Consiglio.

disposizione degli Stati membri che attuano iniziative e azioni concordate e la Commissione è sempre disponibile a collaborare con gli Stati membri per ottimizzarne l'attuazione.

Monitoraggio tramite le valutazioni Schengen e il nuovo sistema di governance dello spazio Schengen

Il meccanismo di valutazione e monitoraggio Schengen ha continuato a contribuire all'efficace attuazione delle norme Schengen volte a rafforzare la sicurezza all'interno dello spazio senza controlli interni. Nel 2023 sono state effettuate le prime valutazioni nell'ambito del meccanismo rafforzato di valutazione e monitoraggio Schengen, che hanno permesso di individuare e correggere tempestivamente le vulnerabilità strategiche che hanno ripercussioni a livello transfrontaliero sulla sicurezza all'interno dell'UE. Nel 2023 la Commissione ha inoltre avviato una valutazione Schengen tematica per valutare le pratiche seguite da Stati membri confrontati a sfide simili nella lotta contro il traffico di stupefacenti verso l'UE, concentrandosi in particolare sul traffico di volumi ingenti. Le valutazioni hanno introdotto un'attenzione maggiore e più approfondita nei confronti degli elementi di sicurezza dello spazio Schengen. Sulla base dei risultati delle valutazioni Schengen periodiche, tematiche e senza preavviso, a giugno 2023 il Consiglio ha stabilito le priorità del ciclo Schengen 2023-2024, definendo i settori di interesse che richiedono un ulteriore impulso verso uno spazio Schengen più sicuro e più forte. Un'attuazione efficace e rapida di queste priorità, insieme a un maggiore coordinamento politico del Consiglio Schengen, rafforzerà ulteriormente la lotta contro la criminalità organizzata e massimizzerà la cooperazione operativa transfrontaliera.

Ruolo degli organi e organismi dell'UE

Ai fini dell'attuazione delle iniziative dell'Unione della sicurezza i partenariati sono essenziali, poiché per ottenere risultati concreti è necessario l'impegno di diverse autorità e dii vari organismi nazionali ed europei. Ad esempio, l'EMPACT (la piattaforma multidisciplinare europea di lotta alle minacce della criminalità) permette la cooperazione multidisciplinare strutturata degli Stati membri, con il sostegno di tutte le istituzioni, gli organi e gli organismi dell'UE (ad esempio Europol, Frontex, Eurojust, CEPOL, OLAF, EU-LISA). Le operazioni condotte mediante l'EMPACT, anche ricorrendo a task force operative apposite, coordinano le attività degli Stati membri e dei partner operativi nella lotta alle reti criminali e ai reati gravi. Nel solo 2022 l'EMPACT ha consentito di procedere a un totale di 9 922 arresti, di effettuare sequestri di beni e denaro per oltre 180 milioni di EUR, di avviare 9 263 indagini, di identificare 4 019 vittime, di sequestrare oltre 62 tonnellate di stupefacenti, di identificare 51 obiettivi ad alto valore con 12 arresti e di condurre operazioni nel contesto della guerra di aggressione contro l'Ucraina, in particolare per contrastare la tratta di esseri umani e le minacce connesse alle armi da fuoco.

Frontex, l'Agenzia europea per la sicurezza marittima (EMSA), e l'Agenzia europea di controllo della pesca (EFCA) continuano a rafforzare la cooperazione nell'ambito delle rispettive funzioni di guardia costiera volte a sostenere le autorità nazionali nel garantire maggiore sicurezza in mare. Queste agenzie contribuiranno in modo determinante all'attuazione della strategia per la sicurezza marittima dell'UE.

Molte iniziative dell'Unione della sicurezza hanno comportato nuove responsabilità e nuovi compiti per le agenzie pertinenti, talvolta con implicazioni a livello di risorse umane.

Agenzia dell'Unione europea per la cibersicurezza (ENISA)

Per quanto riguarda la preparazione e la risposta agli incidenti allo scopo di migliorare la cibersicurezza, la Commissione ha dato avvio a un'azione a breve termine per sostenere gli Stati membri, trasferendo i finanziamenti dal programma Europa digitale all'**Agenzia dell'Unione europea per la cibersicurezza (ENISA)** al fine di rafforzare la preparazione e le capacità di risposta ai grandi incidenti informatici. La proposta di regolamento sulla cibersolidarietà adottata ad aprile 2023 si basa su tale azione e, una volta adottata dai colegislatori, potrebbe affidare all'ENISA compiti supplementari, come la gestione operativa e amministrativa della futura riserva dell'UE per la cibersicurezza o la preparazione delle relazioni di riesame degli incidenti a seguito di incidenti di cibersicurezza su larga scala. La legge sulla ciberresilienza proposta attribuirebbe all'ENISA l'incarico di ricevere dai produttori le notifiche riguardanti le vulnerabilità presenti nei prodotti con elementi digitali e gli incidenti con impatto sulla sicurezza di tali prodotti, che l'ENISA a sua volta dovrebbe inoltrare ai CSIRT competenti o ai pertinenti punti di contatto unici degli Stati membri. L'ENISA dovrebbe inoltre preparare una relazione tecnica biennale sulle tendenze emergenti in materia di rischi di cibersicurezza nei prodotti con elementi digitali e presentarla al gruppo di cooperazione NIS.

Centro europeo di competenza per la cibersicurezza

Il **Centro europeo di competenza per la cibersicurezza (centro di competenza)** costituisce, insieme alla rete dei centri nazionali di coordinamento (rete), il nuovo organismo dell'Unione per il sostegno all'innovazione e alla politica industriale in materia di cibersicurezza. Questo ecosistema potenzierà le capacità della comunità della tecnologia della cibersicurezza, porterà avanti l'eccellenza della ricerca e rafforzerà la competitività dell'industria dell'Unione nel settore. Il centro di competenza e la rete prenderanno decisioni strategiche di investimento e metteranno in comune le risorse dell'Unione, degli Stati membri e, indirettamente, del settore, per migliorare e rafforzare le capacità in materia cibersicurezza a livello tecnologico e industriale. Il centro di competenza riveste quindi un ruolo chiave nel raggiungimento degli ambiziosi obiettivi di cibersicurezza dei programmi Europa digitale e Orizzonte Europa.

Il centro di competenza ha assunto più della metà del personale e presto sceglierà il direttore esecutivo. I lavori già in corso riguardano la parte relativa alla cibersicurezza del programma Europa digitale e una nuova agenda strategica[54] per lo sviluppo e la diffusione della tecnologia, che stabilisce le azioni prioritarie per sostenere le PMI nello sviluppo e nell'uso di tecnologie, servizi e processi strategici per la cibersicurezza, e per rafforzare le competenze in materia di ricerca, sviluppo e innovazione nell'ecosistema europeo della cibersicurezza in senso lato.

Europol

Con il nuovo mandato **Europol** sarà attrezzata meglio per sostenere gli Stati membri nella lotta contro la criminalità organizzata. La lotta contro il traffico di stupefacenti è una priorità centrale, vista la sempre maggiore importanza che riveste e l'impatto sempre più negativo che produce sulla sicurezza dei cittadini dell'UE. Ottenuta l'autorizzazione del Consiglio, il 15 maggio 2023, la Commissione si è adoperata attivamente per concludere accordi internazionali con Bolivia, Brasile, Ecuador, Messico e Perù sullo scambio di dati personali con Europol, allo scopo di prevenire e combattere le forme gravi di criminalità e il terrorismo.

Eurojust

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_it.

Forte di oltre 20 anni di esperienza nel fornire sostegno giudiziale alle autorità nazionali per combattere una molteplicità di reati transfrontalieri gravi e complessi, **Eurojust** ha consolidato la propria posizione nello spazio di libertà, sicurezza e giustizia dell'UE. Per rafforzare trasversalmente la cooperazione, la Commissione è impegnata nella negoziazione di accordi internazionali volti a facilitare la cooperazione tra Eurojust e 13 paesi terzi nello scambio di dati personali ai fini della lotta alla criminalità organizzata e al terrorismo[55] I negoziati si sono già conclusi con l'Armenia e il Libano, mentre sono in corso con l'Algeria e la Colombia e sono iniziati con la Bosnia-Erzegovina. La Commissione incoraggia il Parlamento europeo e il Consiglio a portare a termine la conclusione degli accordi con questi paesi prima della fine della legislatura, in modo da rafforzare la cooperazione giudiziaria transnazionale e ampliare la lotta contro la criminalità transfrontaliera.

EPPO

Dall'inizio delle attività operative nel giugno 2021, la **Procura europea (EPPO)** si dimostra un potente strumento a disposizione dell'Unione per indagare e perseguire gli illeciti penali che incidono sul bilancio dell'Unione, compresi quelli legati alla partecipazione a un'organizzazione criminale nel caso di reati incentrati sul bilancio dell'Unione. La Commissione incoraggia gli Stati membri che ancora non partecipano alla cooperazione rafforzata dell'EPPO a parteciparvi al più presto, al fine di sfruttarne appieno tutte le potenzialità in termini di protezione del denaro dei contribuenti dell'UE.

EUDA

Grazie al nuovo mandato adottato dai colegislatori a giugno 2023, l'Osservatorio europeo delle droghe e delle tossicodipendenze (OEDT) diverrà un'agenzia a pieno titolo (**Agenzia dell'Unione europea sulle droghe (EUDA)**) con un ruolo rafforzato. L'agenzia sarà in grado di valutare in modo più esaustivo le nuove sfide per la salute e la sicurezza poste dalle sostanze stupefacenti illecite e di contribuire in modo più efficace ai lavori a livello di Stati membri e internazionale. La raccolta, l'analisi e la diffusione dei dati continueranno a essere il compito principale dell'agenzia, ma il mandato rafforzato le consentirà anche di sviluppare capacità generali di valutazione delle minacce alla salute e alla sicurezza per individuare le minacce emergenti, comprese quelle del policonsumo, di rafforzare la cooperazione con i punti focali nazionali e di creare una rete di laboratori che le forniscano informazioni medico-legali e tossicologiche. In tal modo l'agenzia potrà emanare allarmi quando appaiono sul mercato sostanze particolarmente pericolose e accrescere la consapevolezza in merito.

La Commissione invita il Parlamento europeo e il Consiglio a concludere con urgenza, e in ogni caso prima della fine dell'attuale legislatura, i negoziati interistituzionali relativi ai fascicoli in sospeso seguenti:

- proposta di rifusione del regolamento finanziario.

La Commissione invita gli Stati membri a:

- condividere informazioni in modo proattivo con la Commissione quando vengono a conoscenza di possibili rischi riguardanti le organizzazioni che richiedono i finanziamenti dell'UE;
- attuare rapidamente le priorità del ciclo Schengen 2023-2024 per uno spazio Schengen più sicuro e più forte;
- interessarsi delle procedure di infrazione aperte nei loro confronti per garantire il corretto recepimento della normativa in questione.

VII. Conclusioni

Gli ultimi tre anni sono stati caratterizzati da un impegno costante e determinato per realizzare l'obiettivo di creare un'Unione della sicurezza per l'UE. Sono stati compiuti enormi passi avanti in tutto il raggio d'azione della politica di sicurezza. La realtà della costante evoluzione delle minacce richiede ora un impegno con rinnovata motivazione. I lavori relativi al quadro legislativo devono essere conclusi in tempo utile, prima della fine della legislatura nella primavera del 2024. Agli Stati membri incombe costantemente la responsabilità di recepire, attuare e applicare la nuova normativa. L'attuazione richiede sforzi concertati, anche con il sostegno delle agenzie dell'UE, e molto spesso una cooperazione ancora più intensa con i partner internazionali.

Solo con l'impegno collettivo e risoluto di tutte le parti interessate si potranno raggiungere nell'UE i livelli di sicurezza che i cittadini si attendono: nelle circostanze attuali, svolgere il proprio ruolo per rafforzare la sicurezza dell'UE dovrebbe costituire una priorità per ogni soggetto coinvolto.