Consiglio dell'Unione europea

Bruxelles, 14 giugno 2024
(OR. en)

11270/24

JAI 1057	**COPEN 321**
COSI 119	**FREMP 305**
ENFOPOL 306	**JAIEX 47**
ENFOCUSTOM 86	**CFSP/PESC 964**
IXIM 166	**COPS 366**
CT 72	**HYBRID 104**
CRIMORG 97	**DISINFO 94**
FRONT 199	**TELECOM 212**
ASIM 60	**DIGIT 160**
VISA 101	**COMPET 677**
CYBER 198	**RECH 313**
DATAPROTECT 242	**CULT 57**
CATS 61	**COTER 134**
DROIPEN 180	**CORDROGUE 83**

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	16 maggio 2024
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2024) 198 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Settima 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(2024) 198 final.

All.: COM(2024) 198 final

COMMISSIONE
EUROPEA

Bruxelles, 15.5.2024
COM(2024) 198 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

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

I INTRODUZIONE

Nel luglio 2020 l'UE ha adottato la sua strategia per l'Unione della sicurezza per il periodo 2020-2025[1]. La strategia è stata elaborata al culmine della pandemia di COVID-19, in un contesto della sicurezza sempre più complesso, caratterizzato da minacce ibride e terroristiche volte a minare la sicurezza dei cittadini e delle imprese europei sia nello spazio fisico sia nel ciberspazio. La risposta dell'UE a tali sfide si è basata su un approccio olistico alla sicurezza, esteso a tutta la società, teso a superare la compartimentazione tra le varie politiche della sicurezza e a mettere in relazione tutti gli aspetti dell'ecosistema europeo della sicurezza.

A quattro anni di distanza il contesto geopolitico, economico e della sicurezza all'interno dell'UE e nei paesi del vicinato è cambiato in maniera profonda e duratura. I rischi che affrontiamo oggi sono assai diversi da quelli prevalenti all'epoca in cui era stata definita la strategia per l'Unione della sicurezza. La pandemia di COVID-19 ha messo in luce che le nostre società ed economie si basano sulle reti di informazione e comunicazione e sui prodotti connessi, evidenziando la necessità di garantire la loro cibersicurezza di fronte a una criminalità informatica in piena espansione e dotata di una grande capacità di adattamento.

La minaccia terroristica sul territorio europeo non si è attenuata e alcuni Stati membri hanno recentemente elevato al massimo il livello nazionale di allerta. La criminalità organizzata pone una minaccia per la stabilità che ha continuato a intensificarsi, in un contesto nel quale il trasferimento online di gran parte delle transazioni commerciali e delle interazioni umane ha aperto nuovi canali per le attività criminose. Poiché milioni di persone sono diventati più vulnerabili a causa dell'instabilità nel vicinato dell'UE, il traffico di migranti e la tratta di esseri umani sono diventate attività prioritarie per coloro che realizzano profitti illeciti attraverso lo sfruttamento di altri individui. La strumentalizzazione dei migranti alle frontiere esterne dell'UE ha messo in luce nuove forme ibride di minacce che, abbinate alle campagne di disinformazione, mirano ad alimentare le divisioni e la diffidenza nelle società europee. Infine il potenziale sfruttamento delle nuove tecnologie, come ad esempio l'intelligenza artificiale, da parte di soggetti malintenzionati per commettere reati di criminalità informatica o manipolare informazioni solleva nuove sfide in materia di sicurezza per le nostre democrazie, soprattutto in un anno caratterizzato da importanti processi elettorali in tutta Europa.

La sicurezza interna e quella esterna sono interconnesse. La guerra di aggressione russa contro l'Ucraina ha determinato un aumento degli attacchi informatici[2] e ha evidenziato la potenziale vulnerabilità di alcune infrastrutture critiche dell'UE. La situazione attuale in Medio Oriente e la portata senza precedenti della violenza nella regione hanno acuito le sfide connesse al mantenimento della sicurezza interna dell'UE, in un contesto in cui si è intensificato il rischio di attacchi terroristici da parte di soggetti che agiscono da soli o di gruppi organizzati, rischio alimentato dai tentativi di diffondere contenuti terroristici attraverso piattaforme e reti online.

In un simile contesto caratterizzato da minacce in costante evoluzione, la prospettiva delineata nella strategia per l'Unione della sicurezza si è rivelata particolarmente pertinente. Sebbene non sia possibile eliminare tutti i rischi, le vulnerabilità possono essere affrontate e la strategia per l'Unione della sicurezza ha fornito un quadro solido per rafforzare la capacità dell'UE di

[1] COM(2020) 605.
[2] Relazione dell'ENISA sul panorama delle minacce 2023, pagg. 10 e 11.

contrastare le minacce attuali e quelle emergenti con unità di intenti e attraverso meccanismi d'azione collettivi migliorati. La presente settima relazione sui progressi dell'Unione della sicurezza mira a fornire una panoramica dell'attuazione della strategia sin dalla sua adozione nel 2020. Sebbene la Commissione abbia affrontato tutti i punti inizialmente evidenziati nella strategia per l'Unione della sicurezza, sono state integrate nuove iniziative a fronte dell'evoluzione delle sfide in materia di sicurezza. Il completamento dei fascicoli in sospeso che sono ancora in attesa di approvazione da parte del Parlamento e del Consiglio nonché l'applicazione e l'attuazione della legislazione adottata da parte degli Stati membri sono ora fondamentali per proteggere efficacemente i cittadini dell'UE dalle minacce alla sicurezza.

II INFRASTRUTTURE FISICHE E DIGITALI PROTETTE MEGLIO E PIÙ RESILIENTI

II.1. Infrastrutture critiche

I cittadini, le imprese e le autorità dell'UE fanno affidamento su infrastrutture critiche, che sono alla base di servizi essenziali quali la fornitura di energia, l'approvvigionamento di risorse idriche e alimentari, i trasporti e le telecomunicazioni. La vita quotidiana dei cittadini e la salute a lungo termine dell'economia dipendono dalla fornitura di tali servizi. Tuttavia il contesto geopolitico in cui operano le infrastrutture critiche nell'UE è estremamente instabile. Tale instabilità è stata acuita dalla guerra di aggressione della Russia nei confronti dell'Ucraina, come dimostrato dall'aumento degli attacchi ibridi e dal sabotaggio del gasdotto Nord Stream nonché dai danni ai gasdotti del Balticconnector.

Dall'inizio del mandato di questa Commissione l'UE ha adottato una serie di misure per rafforzare la protezione delle infrastrutture critiche e la resilienza dei soggetti che le gestiscono, al fine di evitare o di attenuare l'impatto delle perturbazioni dei servizi essenziali. L'UE ha rafforzato il quadro giuridico per affrontare i rischi attuali e futuri online e offline, che vanno dagli attacchi informatici alle catastrofi naturali, con l'adozione della **direttiva sulla resilienza dei soggetti critici** ("direttiva CER")[3] e della **direttiva riveduta sulla sicurezza delle reti e dell'informazione** ("direttiva NIS 2")[4]. Una volta recepite dagli Stati membri, le direttive garantiranno che i rischi e le vulnerabilità che interessano i soggetti operanti in una serie di settori chiave[5] siano presi maggiormente in considerazione. Al fine di accelerare l'attuazione delle due direttive, una raccomandazione del Consiglio[6] ha fornito la base per l'esecuzione di prove di stress con i soggetti che gestiscono infrastrutture critiche, a partire dal settore dell'energia; l'analisi dei risultati da parte della Commissione è in corso.

I recenti avvenimenti hanno inoltre evidenziato la necessità di un'azione urgente a livello dell'UE in caso di incidente. La Commissione ha proposto[7] una **raccomandazione del Consiglio relativa a un programma** che definisce il coordinamento della risposta a livello dell'UE ai tentativi di perturbare il funzionamento delle infrastrutture critiche con significativa

---

3 Direttiva (UE) 2022/2557, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici.

4 Direttiva (UE) 2022/2555, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.

5 La direttiva NIS 2 e la direttiva CER riguardano i seguenti settori: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, infrastrutture digitali, sanità, acque potabili, acque reflue, pubblica amministrazione, spazio nonché produzione, trasformazione e distribuzione di alimenti.

6 La proposta della Commissione COM(2022) 551 è stata seguita dalla raccomandazione del Consiglio 2023/C 20/01.

7 COM(2023) 526.

rilevanza transfrontaliera. Il **regolamento relativo alle emergenze e alla resilienza nel mercato interno** fornirà gli strumenti per garantire la continuità del funzionamento del mercato interno durante una crisi.

La Commissione è inoltre intervenuta per rafforzare la resilienza delle infrastrutture critiche **a livello settoriale**, sulla base del quadro di riferimento stabilito dalla normativa orizzontale. Nel **settore dell'energia** i lavori per l'istituzione di un codice di rete sulle norme settoriali per gli aspetti relativi alla cibersicurezza dei flussi transfrontalieri di energia elettrica contribuiranno a rendere il sistema elettrico dell'UE più resiliente e sicuro. La Commissione ha inoltre annunciato il **piano d'azione per l'energia eolica**, volto a rafforzare la ciberresilienza degli impianti eolici. Nel **settore dei trasporti** la Commissione ha proseguito l'attività concernente il sistema di ispezioni per la sicurezza aerea e marittima, con oltre 100 ispezioni aeree e 60 ispezioni marittime. Per quanto riguarda la **sicurezza marittima**, nell'ottobre 2023 è stata approvata la strategia riveduta per la sicurezza marittima dell'UE[8] con il relativo piano d'azione, nell'intento di proteggere meglio le navi e le infrastrutture marittime critiche dalle minacce fisiche e informatiche. La Commissione sta inoltre sviluppando un **ambiente comune per la condivisione delle informazioni**, al fine di agevolare lo scambio di informazioni tra le autorità marittime a livello transfrontaliero e intersettoriale. Il riesame del regolamento relativo alla **rete transeuropea dei trasporti**[9] prevede per gli Stati membri nuovi obblighi di immunizzazione dai rischi, al fine di garantire l'efficace protezione delle principali infrastrutture di trasporto dell'Unione. A seguito di una valutazione approfondita dei rischi nel **settore delle infrastrutture di interconnettività**, effettuata con gli Stati membri e l'ENISA, la Commissione ha formulato una serie di raccomandazioni per aumentare la cibersicurezza e la resilienza, ad esempio definendo a febbraio del 2024[10] azioni volte a migliorare la sicurezza delle infrastrutture di cavi sottomarini essenziali per le reti di comunicazione dell'UE. La comunicazione sulla gestione dei **rischi climatici** ha individuato le principali categorie di azioni, tra cui un migliore utilizzo dei dati e dei servizi satellitari disponibili per rafforzare la resilienza delle infrastrutture critiche[11].

Nel **settore dello spazio** la **strategia spaziale dell'UE per la sicurezza e la difesa**[12], adottata a marzo del 2023, contempla azioni volte a rafforzare la resilienza dei sistemi e dei servizi spaziali e a sviluppare ulteriori servizi spaziali a duplice uso dell'UE. Per quanto riguarda i **sistemi idrici**, il **manuale per l'attuazione del piano di sicurezza idrica** prevede misure di sicurezza atte a contrastare azioni ostili contro l'integrità fisica e informatica dei sistemi di approvvigionamento idrico nonché la contaminazione intenzionale delle acque[13]. Nel **settore finanziario** l'adozione del **regolamento sulla resilienza operativa digitale (DORA)**[14] rafforza la resilienza digitale delle entità del settore finanziario dell'UE attraverso la razionalizzazione e l'aggiornamento delle norme vigenti. Infine nel **settore sanitario**, nell'ambito dell'Unione europea della salute[15], l'**autorità per la preparazione e la risposta**

---

8 JOIN (2023) 8.

9 Accordo provvisorio del 24 aprile 2024 sul regolamento del Parlamento europeo e del Consiglio sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti.

10 C(2024) 1181.

11 COM (2024) 91.

12 JOIN(2023) 9 final.

13 Archivio delle pubblicazioni del JRC - *Water Security Plan Implementation Manual for Drinking Water Systems*.

14 Regolamento (UE) 2022/2554, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario.

15 Comunicazione sull'Unione europea della salute.

alle emergenze sanitarie (HERA) sostiene la ricerca e lo sviluppo, la produzione e la fornitura di contromisure mediche. Inoltre è attualmente in corso il potenziamento del modulo di gestione delle crisi del sistema di allarme rapido e di reazione dell'UE, con l'obiettivo di sostenere il coordinamento delle gravi minacce per la salute e i sistemi sanitari e di garantire il coordinamento costante in materia di minacce sanitarie all'interno dell'UE e a livello mondiale. I primi sei laboratori di riferimento europei per la salute pubblica sono stati designati a marzo del 2024 e il piano di prevenzione, preparazione e risposta dell'Unione è in fase di elaborazione e sarà ultimato e collaudato entro la fine del 2024.

II.2. Cibersicurezza

Il panorama delle minacce informatiche è notevolmente peggiorato negli ultimi anni, come dimostrano il drastico aumento degli attacchi alle catene di approvvigionamento e lo sfruttamento delle vulnerabilità presenti nei software, nei sistemi operativi per dispositivi mobili o personal computer e nelle reti private virtuali. Gli attacchi informatici sono in aumento[16] e prendono di mira l'industria pesante, i servizi di informazione, la pubblica amministrazione e la sanità. Il ransomware continua a rappresentare un problema, non soltanto in termini di numero di attacchi ma anche per via della crescente collusione tra gruppi criminali e soggetti statali mossi da interessi che vanno oltre la realizzazione di profitti[17]. Di fronte all'aumento e all'evoluzione di queste minacce informatiche, l'UE ha adottato misure incisive per migliorare la cibersicurezza negli Stati membri, potenziare la sicurezza delle catene di approvvigionamento e dei prodotti, rafforzare la solidarietà a livello dell'UE e migliorare le capacità di rilevamento delle minacce e degli incidenti di cibersicurezza e di preparazione e risposta agli stessi.

Nel corso dell'attuale mandato sono state gettate solide basi per sostenere l'UE nel suo costante impegno volto a salvaguardare la propria infrastruttura digitale. La **revisione della direttiva NIS** ne ha esteso notevolmente l'ambito di applicazione a tutti i soggetti di medie e grandi dimensioni che operano in 18 settori critici, introducendo disposizioni riguardanti obblighi più rigorosi in materia di cibersicurezza, la segnalazione obbligatoria degli incidenti e l'istituzione di una struttura europea di coordinamento per le crisi informatiche. Inoltre è stato raggiunto un accordo in merito alla **legge sulla ciberresilienza**[18] ed è stato adottato il **regolamento sull'identità digitale europea**[19], che potenzierà in misura significativa la cibersicurezza complessiva nell'UE. La legge sulla ciberresilienza introdurrà requisiti obbligatori di cibersicurezza "fin dalla progettazione" e "per impostazione predefinita" per l'hardware e il software durante l'intero ciclo di vita del prodotto, garantendo che i prodotti siano immessi sul mercato senza vulnerabilità note. Il regolamento sull'identità digitale europea faciliterà lo sviluppo del mercato unico digitale sulla base di servizi affidabili e costituirà una componente cruciale degli sforzi volti a contrastare gli attacchi di phishing e a migliorare l'autenticazione e la gestione dell'accesso. Nel frattempo il 1º agosto 2025 entreranno in vigore nuove norme nell'ambito della **direttiva sulle apparecchiature radio**, che impongono ai fabbricanti di dispositivi senza fili l'obbligo di migliorare il livello di cibersicurezza, di tutela della vita privata e di protezione dalle frodi.

---

16 Relazione dell'ENISA sul panorama delle minacce 2023, pagg. 10 e 11.

17 Cfr. ad esempio: https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime.

18 L'accordo provvisorio è stato raggiunto il 30 novembre 2023. L'entrata in vigore è prevista nel 2024.

19 L'accordo provvisorio è stato raggiunto l'8 novembre 2023.

Il **regolamento sulla cibersolidarietà**[20] segnerà una svolta in termini di rilevamento delle minacce informatiche, di preparazione e di risposta agli incidenti a livello dell'UE. Il regolamento prevede un sistema europeo di allarme di cibersicurezza, costituito da una rete paneuropea di poli per la cibersicurezza destinata a sviluppare capacità di rilevamento coordinate a livello dell'UE e a migliorare la conoscenza situazionale comune. Un meccanismo per le emergenze di cibersicurezza rafforzerà la preparazione e migliorerà le capacità di risposta e ripresa degli Stati membri. Sarà istituita la riserva dell'UE per la cibersicurezza, che sosterrà la risposta e la ripresa iniziale in caso di incidenti di cibersicurezza significativi e su vasta scala; potranno usufruirne gli Stati membri, le istituzioni dell'UE e i paesi terzi associati al programma Europa digitale.

Il **Centro europeo di competenza per la cibersicurezza**, che dovrebbe diventare pienamente autonomo nel corso di quest'anno, aumenterà le capacità di cibersicurezza e la competitività dell'Europa, proteggendo l'economia e la società europee dagli attacchi informatici e rafforzando la sovranità tecnologica dell'Europa attraverso investimenti congiunti in progetti strategici in materia di cibersicurezza.

L'adozione del primo **sistema europeo di certificazione della cibersicurezza**[21], basato su criteri comuni dell'UE, rappresenta un ulteriore passo importante verso la creazione di un ambiente nel mercato interno che le imprese e i consumatori possano considerare affidabile. Il programma di lavoro dell'Unione per la certificazione europea della cibersicurezza[22], adottato a febbraio del 2024, individua alcune priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza. Il regolamento sulla cibersicurezza è stato modificato in modo da contemplare i sistemi di certificazione della cibersicurezza per i servizi di sicurezza gestiti che la Commissione richiederà all'ENISA una volta che il regolamento stesso sarà entrato in vigore. Sono in fase di definizione altri sistemi, come ad esempio il sistema europeo di certificazione della cibersicurezza per i servizi cloud, che aiuterà gli utenti a prendere decisioni consapevoli in merito ai servizi acquistati. Tali sistemi dovrebbero prevedere requisiti più rigorosi in funzione della sensibilità dei dati e del livello di garanzia richiesto.

Nel frattempo l'UE ha adottato misure per rafforzare la **cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione europea**, introducendo un quadro di gestione, di governance e di controllo dei rischi per la cibersicurezza, rafforzando il ruolo del CERT-UE e istituendo un nuovo comitato interistituzionale per la cibersicurezza che avrà il compito di monitorare e sostenere l'attuazione di detto quadro. Tuttavia la mancanza di progressi nei negoziati sulla proposta parallela relativa alla sicurezza delle informazioni, che è essenziale per completare un solido quadro legislativo per le istituzioni, gli organi e gli organismi dell'UE e contribuire pertanto a un'amministrazione europea sicura, dovrebbe essere affrontata in via prioritaria.

A complemento dell'intenso lavoro legislativo degli ultimi anni, la Commissione si è adoperata per intensificare la **cooperazione operativa con gli Stati membri**. L'istituzione delle prime reti transfrontaliere di centri operativi di sicurezza nonché l'assistenza fornita agli Stati membri negli ultimi due anni attraverso l'azione di sostegno dell'ENISA con una dotazione di 35 milioni di EUR nell'ambito del programma Europa digitale hanno dimostrato che l'UE può rafforzare la sicurezza per i propri cittadini grazie alla messa in comune di risorse per rafforzare le capacità in materia di cibersicurezza.

[20] COM(2023) 209.
[21] C(2024) 560, adottato il 31 gennaio 2024.
[22] SWD(2024) 38.

Al fine di garantire la sicurezza economica e l'autonomia strategica aperta, l'UE ha inoltre adottato un approccio proattivo per **affrontare i rischi di cibersicurezza nel settore delle tecnologie emergenti**. Nell'ambito della strategia per la sicurezza economica sono in corso valutazioni comuni dei rischi in relazione a tecnologie quali l'IA, i semiconduttori avanzati, le biotecnologie e le tecnologie quantistiche[23]. Al fine di tutelare i dati e rendere sicure le comunicazioni sensibili, la Commissione ha pubblicato una raccomandazione[24] che invita gli Stati membri a elaborare e attuare una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica in tutta l'UE. La raccomandazione incoraggia gli Stati membri a sostenere l'elaborazione di norme e lo sviluppo di algoritmi di crittografia post-quantistica da attuare in tutta l'Unione.

L'**attuazione del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G**[25] è essenziale per garantire l'affidabilità e la cibersicurezza delle reti 5G e post-5G e delle tecnologie correlate. In linea con il pacchetto di strumenti, la Commissione si adopererà per evitare l'esposizione delle proprie comunicazioni istituzionali su reti mobili che utilizzano fornitori ad alto rischio e provvederà affinché la propria valutazione si rifletta in tutti i programmi e gli strumenti di finanziamento dell'UE pertinenti[26]. L'approccio dell'UE alla cibersicurezza ora riguarda non solo la prevenzione e la protezione delle infrastrutture critiche ma anche la **gestione delle crisi**, anche attraverso la creazione e la formalizzazione della **rete europea dei funzionari di collegamento per le crisi informatiche (EU-CyCLONe)**. Lo sviluppo di un ecosistema di portatori di interessi e di reti per la gestione delle crisi ha rafforzato la preparazione dell'UE alla risposta collettiva in caso di gravi incidenti informatici. Un buon coordinamento tra i vari livelli (tecnico, operativo e politico) e forti sinergie tra le diverse comunità di cibersicurezza richiedono esercitazioni e interazioni periodiche tra i vari settori, nonché valutazioni dei rischi, prove di stress e una documentazione chiara, aggiornata e compresa correttamente da tutti i soggetti coinvolti.

La sicurezza e la competitività dell'UE dipendono dalla presenza di una forza lavoro composta da professionisti qualificati nel campo della cibersicurezza. Tuttavia l'UE si trova di fronte a una significativa carenza di professionisti della cibersicurezza, che aumenta i rischi per l'UE, i suoi Stati membri, i suoi cittadini e le sue imprese derivanti da incidenti di cibersicurezza che potrebbero non essere individuati prontamente o non ricevere una risposta adeguata e tempestiva[27]. L'istituzione dell'**Accademia per le competenze in materia di cibersicurezza** contribuirà ad affrontare tale questione, riunendo le iniziative esistenti in materia di formazione nel campo delle competenze di cibersicurezza e migliorandone il coordinamento. Il crescente numero di impegni assunti nell'ambito dell'Accademia dimostra che l'industria e la comunità accademica intendono contribuire in misura significativa a incoraggiare un maggior numero di professionisti, comprese le giovani donne, ad entrare nel mondo della cibersicurezza.

La nuova **politica di ciberdifesa** dell'UE stabilisce i mezzi per migliorare il coordinamento tra le comunità di cibersicurezza civili e l'ecosistema militare/di difesa; i collegamenti tra questi due settori sono probabilmente destinati ad aumentare in futuro. La politica di ciberdifesa consente inoltre all'UE e ai suoi Stati membri di rafforzare la propria capacità di protezione, rilevamento, difesa e deterrenza, avvalendosi opportunamente dell'intera gamma

[23] C(2023) 6689.
[24] C(2024) 2393.
[25] Gruppo di cooperazione NIS, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, 1/2020.
[26] C(2023) 4049.
[27] ENISA, *Foresight Cybersecurity Threats for 2030 – Aggiornamento 2024*.

di opzioni difensive a disposizione delle comunità civile e militare per la sicurezza e la difesa dell'UE più in generale, conformemente al diritto internazionale. La nuova politica evidenzia la necessità di una più stretta collaborazione tra il settore pubblico e quello privato e propone soluzioni per realizzarla.

L'UE in azione

Sin dalla sua istituzione l'ENISA ha prodotto 70 relazioni sulla conoscenza situazionale, in cui sono stati esaminati oltre 4 000 incidenti. L'agenzia ha gestito 22 segnalazioni di incidenti su larga scala. L'ENISA ha contribuito a organizzare una serie di simulazioni informatiche, la più recente delle quali, organizzata congiuntamente con la Commissione, ha verificato la preparazione della rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), che riunisce le autorità nazionali degli Stati membri preposte alla gestione delle crisi informatiche e la Commissione. Tali simulazioni rafforzano il coordinamento attenuando in tal modo l'impatto di potenziali attacchi futuri nell'UE.

Nell'ambito del programma Europa digitale, la Commissione sta mobilitando 84 milioni di EUR per azioni a sostegno della cibersicurezza previste dalle nuove norme dell'UE, tra cui l'applicazione dell'IA e di altre tecnologie abilitanti per i centri operativi di sicurezza, nonché la transizione dell'Europa verso la crittografia post-quantistica. Il Centro europeo di competenza per la cibersicurezza contribuirà a garantire che tali progetti vadano a beneficio delle imprese, delle PMI e delle amministrazioni pubbliche degli Stati membri e dei paesi associati.

III LOTTA AL TERRORISMO E ALLA RADICALIZZAZIONE

III.1. Misure di lotta al terrorismo

La minaccia del terrorismo rimane elevata e rischia di essere influenzata dai conflitti al di fuori dell'UE. Secondo Europol[28] nel 2022 gli Stati membri hanno segnalato 28 attacchi realizzati, falliti o sventati; si tratta di un numero in aumento rispetto al 2021 (18 attacchi) ma ben al di sotto dei 56 attacchi segnalati nel 2020. Dopo l'attacco di Hamas del 7 ottobre 2023 sono aumentate le tensioni in alcune comunità negli Stati membri, che sono sfociate in tre attentati terroristici (ad Arras in Francia il 13 ottobre, a Bruxelles il 16 ottobre e a Parigi il 2 dicembre 2023). In parallelo alcuni Stati membri affrontano la minaccia significativa rappresentata dall'estremismo violento di destra. L'esaltazione del terrorismo nonché l'incitamento all'odio, in particolare sotto forma di antisemitismo e di odio anti-islamico, risultano essere in aumento nell'UE dal 7 ottobre 2023[29].

Nell'ambito della strategia per l'Unione della sicurezza è stata adottata una serie di misure e strumenti per sostenere gli Stati membri nella lotta al terrorismo. Sin dalla sua adozione nel dicembre 2020 il **programma di lotta al terrorismo dell'UE**[30] ha dotato l'Unione di strumenti per prevedere e prevenire le minacce terroristiche, proteggere e reagire alle stesse. Nella direttiva sulla lotta contro il terrorismo[31], adottata nel 2017 e oggi attuata da tutti gli Stati membri, sono qualificati come reati l'addestramento e i viaggi a fini terroristici, nonché il

[28] Europol 2023, *European Union Terrorism Situation and Trend report 2023*.
[29] Cfr.: isdglobal.org, 31 ottobre 2023; isdglobal.org, 2 novembre 2023.
[30] COM(2020) 795.
[31] Direttiva (UE) 2017/541, del 15 marzo 2017, sulla lotta contro il terrorismo.

finanziamento del terrorismo. Le carenze nel recepimento della direttiva in una serie di Stati membri sono attualmente oggetto di procedure di infrazione; inoltre sono stati organizzati diversi seminari per garantire che la legislazione raggiunga la piena efficacia attraverso l'attuazione.

Alcuni **combattenti terroristi stranieri** sono rientrati nell'UE ma un notevole numero di essi è ancora detenuto nei campi e nelle carceri del nord-est della Siria. Sebbene la responsabilità primaria spetti agli Stati membri, la cooperazione a livello dell'UE li ha aiutati ad affrontare sfide quali il perseguimento degli autori di reati di terrorismo, la prevenzione dell'ingresso clandestino nello spazio Schengen, con controlli sistematici nel sistema d'informazione Schengen effettuati utilizzando appieno le sue funzionalità, nonché il reinserimento e la riabilitazione dei combattenti terroristi stranieri rimpatriati. Tanto Europol quanto Eurojust hanno svolto un ruolo cruciale nel coordinamento di tali indagini e azioni penali.

Privare i terroristi dei mezzi per compiere un attentato è fondamentale nella lotta contro il terrorismo. La nuova **legislazione sulle armi da fuoco** inciderà sulla capacità dei terroristi di accedere alle armi nell'UE. A febbraio del 2021 sono entrate in vigore nuove norme destinate a limitare l'accessibilità dei **precursori di esplosivi** che i terroristi potrebbero utilizzare per la fabbricazione di bombe[32]. Sulla base dell'approccio utilizzato per regolamentare l'accesso ai precursori di esplosivi, la Commissione ha condotto una valutazione d'impatto sulla regolamentazione dell'accesso alle **sostanze chimiche ad alto rischio**. Inoltre i rapidi progressi nel campo dell'IA e della biotecnologia riducono gli ostacoli all'accesso a sostanze chimiche e agenti patogeni pericolosi, aumentando il rischio di incidenti chimici e biologici.

Al fine di **migliorare la preparazione**, la Commissione sta creando riserve strategiche di capacità a livello europeo attraverso rescEU e l'HERA per reagire di fronte alle minacce chimiche, biologiche, radiologiche e nucleari. Tali riserve strategiche garantiscono la disponibilità di contromisure, comprese attrezzature, per assicurare la protezione contro le conseguenze degli incidenti. L'UE ha continuato a rafforzare il quadro dell'Unione per **prevenire e combattere il riciclaggio di denaro e il finanziamento del terrorismo** e monitora attentamente l'attuazione per garantire che la normativa contribuisca a una più efficace individuazione dei fondi destinati al finanziamento delle organizzazioni terroristiche. Al fine di sostenere le indagini relative al finanziamento del terrorismo, nel 2021 la Commissione ha inoltre istituito una **rete di investigatori finanziari antiterrorismo**. La rete, presieduta dalla Commissione, sostiene gli scambi tra gli investigatori degli Stati membri sulle tecniche e sulle esperienze nella lotta al finanziamento del terrorismo.

La **protezione della popolazione e degli spazi pubblici** è una priorità del programma di lotta al terrorismo. Attraverso il programma dei consulenti UE sulla sicurezza protettiva, oltre 100 esperti nazionali e della Commissione appositamente formati sono a disposizione per condurre, su richiesta di un'autorità di uno Stato membro, missioni di valutazione delle vulnerabilità, finanziate dalla Commissione, con l'obiettivo di contribuire a mantenere gli spazi pubblici, gli eventi ad alto rischio e le infrastrutture critiche nell'UE al riparo dalle minacce terroristiche. Come evidenziato nella comunicazione congiunta della Commissione e dell'alto rappresentante del 6 dicembre 2023[33] dal titolo "Nessuno spazio per l'odio in un'Europa che, unita, lo ripudia", sono stati aumentati i finanziamenti per la protezione degli

[32] Regolamento (UE) 2019/1148, del 20 giugno 2019, relativo all'immissione sul mercato e all'uso di precursori di esplosivi.

[33] JOIN(2023) 51.

spazi pubblici e dei luoghi di culto di tutte le fedi. Dal 2020 è stata assegnata, attraverso il **Fondo Sicurezza interna**, una dotazione di 30 milioni di EUR al programma PROTECT, che tra l'altro rivolge particolare attenzione alla protezione dei luoghi di culto, comprese le sinagoghe e le moschee: un ulteriore importo di 5 milioni di EUR sta contribuendo ad affrontare specifiche minacce poste dal crescente antisemitismo. La Commissione sta collaborando con la società civile per combattere l'incitamento all'odio, ad esempio attraverso il panel europeo di cittadini sulla lotta contro l'odio nella società.

I **droni** sono uno strumento sempre più diffuso e accessibile che può essere utilizzato per scopi legittimi ma anche per scopi malevoli, tra cui attacchi contro spazi pubblici, individui e infrastrutture critiche. A ottobre del 2023 la Commissione ha adottato una comunicazione sul contrasto alle minacce poste dai droni non cooperativi progettati per usi civili[34]. Tra le azioni fondamentali già attuate figurano l'istituzione di un gruppo di esperti anti-droni che fornirà consulenza a livello politico e operativo, nonché una specifica valutazione dei rischi che i velivoli senza equipaggio non cooperativi pongono per l'aviazione civile e le strutture aeroportuali. La Commissione ha inoltre effettuato una **mappatura completa dei rischi per la sicurezza aerea** per fare il punto sulle minacce e sulle vulnerabilità esistenti e in evoluzione al fine di aggiornare il sistema di sicurezza aerea di base dell'UE negli aeroporti dell'Unione[35].

III.2. Prevenzione e contrasto della radicalizzazione

Prevenire la radicalizzazione è il primo passo per la prevenzione degli attentati terroristici. La Commissione ha rafforzato il suo sostegno agli Stati membri per contribuire a impedire che i cittadini siano esposti a contenuti estremisti e terroristici dannosi online e offline, anche nelle carceri. Attraverso la rete di sensibilizzazione al problema della radicalizzazione, la Commissione riunisce 6 500 operatori (responsabili politici, autorità di contrasto, ricercatori) di tutta Europa al fine elaborare le migliori pratiche per affrontare l'estremismo violento. Dal mese di giugno del 2024 la rete di sensibilizzazione al problema della radicalizzazione sarà integrata nel polo di conoscenze dell'UE sulla prevenzione della radicalizzazione. Con il **polo di conoscenze dell'UE** l'Unione mira a superare la compartimentazione tra i responsabili politici, i ricercatori e gli operatori del settore pertinenti, fornendo studi approfonditi, scenari previsionali, sostegno per la risposta agli sviluppi geopolitici, formazione in materia di comunicazione strategica, nonché strumenti per l'elaborazione di politiche e pratiche di contrasto della radicalizzazione. La Commissione ha inoltre adottato una raccomandazione sui diritti procedurali di indagati e imputati sottoposti a custodia cautelare e sulle condizioni materiali di detenzione[36], che contempla misure volte ad affrontare la questione della radicalizzazione nelle carceri.

L'UE si sta inoltre adoperando per prevenire influenze e finanziamenti stranieri che promuovono opinioni radicali/estremiste negli Stati membri. La Commissione vigila per impedire che i fondi dell'UE siano utilizzati a sostegno di progetti che sono incompatibili con i valori europei o che perseguono un programma illegale. Il regolamento finanziario riveduto[37] include ora la condanna per "incitamento all'odio" tra i motivi di esclusione dai finanziamenti dell'UE. Nel gennaio 2024 la Commissione ha pubblicato nuovi orientamenti

[34] COM(2023) 659.
[35] SWD(2023) 37 final.
[36] Raccomandazione (UE) 2023/681 dell'8 dicembre 2022.
[37] Il 7 dicembre 2023 è stato raggiunto un accordo politico provvisorio.

sulle conseguenze delle violazioni dei valori dell'UE, destinati alle autorità di gestione dei programmi finanziari.

La disinformazione con finalità di incitamento all'odio e i contenuti terroristici circolano online, anche sotto forma di immagini generate dall'IA, e possono ispirare atti di estremismo violento. Uno strumento fondamentale per impedire la circolazione di contenuti terroristici online è il **regolamento relativo al contrasto della diffusione di contenuti terroristici online**[38], che obbliga i prestatori di servizi di hosting a rimuovere tali contenuti o a bloccare l'accesso ad essi entro un'ora dal ricevimento dell'ordine di rimozione emesso dalle autorità degli Stati membri. Nella sua relazione di valutazione adottata a febbraio del 2024 la Commissione ha riferito che il regolamento è stato efficace nel prevenire la propagazione di contenuti terroristici online. Finora 23 Stati membri hanno designato autorità competenti incaricate di emettere gli ordini di rimozione; tra giugno del 2022 e aprile del 2024 sono stati emessi circa 500 ordini di rimozione. In parallelo le carenze nel recepimento del regolamento riscontrate in diversi Stati membri sono attualmente oggetto di procedure di infrazione.

La Commissione ha inoltre pubblicato una serie di orientamenti per gli insegnanti e gli educatori volti a contrastare la disinformazione e promuovere l'alfabetizzazione digitale attraverso l'istruzione e la formazione.

Ciò che è illecito offline deve essere vietato anche online. L'applicazione del **regolamento sui servizi digitali**[39], che si applica dal 17 febbraio 2024, è un passo decisivo in questa direzione, giacché esso impone a tutte le piattaforme online una serie di obblighi in materia di contrasto dei contenuti illegali. Un altro elemento del pacchetto di strumenti dell'UE per il contrasto del terrorismo è costituito dall'**unità UE addetta alle segnalazioni su Internet di Europol**, che segnala contenuti terroristici ad oltre 300 piattaforme, sensibilizzando al problema della propaganda terroristica e intensificando gli interventi per contrastarla. Anche il **Forum dell'UE su Internet** sostiene l'industria tecnologica nel contenere la diffusione di contenuti estremisti e attualmente sta affrontando il rischio di sfruttamento dell'IA generativa a fini terroristici, integrando gli sviluppi normativi, in particolare la legge sull'intelligenza artificiale[40]. A seguito degli attentati di Christchurch del marzo 2019, il Forum dell'UE su Internet ha approvato il protocollo di crisi dell'UE per garantire la cooperazione tra le autorità di contrasto e l'industria a seguito di una crisi.

III.3. Protezione delle vittime del terrorismo

A gennaio del 2020 la Commissione ha istituito il centro di competenza dell'UE per le **vittime del terrorismo**, per offrire competenze, orientamenti e sostegno alle autorità nazionali e alle organizzazioni di sostegno alle vittime. Il centro di competenza dell'UE sta contribuendo a garantire la corretta applicazione delle norme dell'UE relative alle vittime del terrorismo, promuovendo lo scambio di migliori pratiche e la condivisione di competenze.

L'UE in azione

Nel 2022 gli attentati terroristici compiuti, falliti o sventati sono stati 28. Nello stesso anno negli Stati membri sono state arrestate 380 persone per reati connessi al terrorismo. 14 di

[38] Regolamento (UE) 2021/784, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online.

[39] Regolamento (UE) 2022/2065, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali (regolamento sui servizi digitali).

[40] L'8 dicembre 2023 è stato raggiunto un accordo politico provvisorio.

questi casi riguardavano il finanziamento del terrorismo ed erano tutti legati al terrorismo jihadista. **Eurojust** ha sostenuto azioni in 203 casi, compreso il lavoro di otto squadre investigative comuni. A norma del regolamento relativo alla prevenzione della diffusione di contenuti terroristici online, dal mese di giugno 2022 sono stati eseguiti 350 ordini di rimozione.

Con il sostegno della Commissione, gli Stati membri hanno messo in atto strumenti di valutazione dei rischi, regimi speciali di detenzione, programmi di riabilitazione e reintegrazione, attività di formazione per il personale penitenziario e di sorveglianza, nonché strutture per lo scambio di informazioni e la cooperazione multidisciplinare per la gestione degli autori di reati dopo la scarcerazione.

Il regolamento relativo al contrasto della diffusione di contenuti terroristici online ha dimostrato la sua validità, ad esempio nel consentire la rapida rimozione dei contenuti terroristici dopo l'attacco perpetrato da Hamas contro Israele il 7 ottobre 2023.

IV LOTTA ALLA CRIMINALITÀ ORGANIZZATA

La criminalità organizzata è una minaccia per i cittadini, le imprese e le istituzioni statali europee, nonché per l'economia nel suo complesso. Le reti criminali sono coinvolte in un'ampia gamma di attività criminali, tra cui traffico di stupefacenti, reati organizzati contro il patrimonio, reati ambientali, frode, traffico di migranti e tratta di esseri umani. La cibercriminalità e la violenza di genere online sono state ulteriormente stimolate dal maggiore utilizzo di internet e dei servizi online. Inoltre la perturbazione causata dalla guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina ha creato nuove opportunità, prontamente sfruttate dai gruppi della criminalità organizzata. I criminali operano agevolmente online e a livello transfrontaliero, il che rende necessaria un'azione coerente a livello europeo e transnazionale. **La strategia dell'UE per la lotta alla criminalità organizzata 2021-2025**[41], adottata dalla Commissione ad aprile del 2021, evidenzia l'importanza di smantellare le strutture della criminalità organizzata, concentrandosi sugli individui ai vertici delle organizzazioni criminali, in particolare sui gruppi che rappresentano il rischio maggiore per la sicurezza dell'Europa.

IV.1. Cibercriminalità

Se da un lato gli sviluppi tecnologici apportano miglioramenti rapidi e importanti nella società, dall'altro lato essi consentono ai criminali informatici di sfruttare la caratteristica precipua del mondo digitale, ossia l'assenza di confini. Tra maggio del 2021 e giugno del 2022 sono stati segnalati 3 640 attacchi ransomware ai danni di imprese e istituzioni dell'UE e nel 2023 i pagamenti collegati a questo tipo di attacchi hanno complessivamente superato per la prima volta 1 miliardo di EUR[42]. I vari tipi di reati, che spaziano dagli attacchi informatici su larga scala alle attività che utilizzano malware, spyware, phishing e spam, interferiscono con il funzionamento delle infrastrutture digitali e fisiche e si ripercuotono gravemente sulla vita delle persone. Per contrastarli l'UE ha adottato una serie di misure legislative e non legislative volte a promuovere la cooperazione transfrontaliera a livello internazionale e dell'UE.

[41] COM(2021) 170.
[42] ENISA, *Threat Landscape for Ransomware Attacks*.

Nel 2021 l'UE ha aderito all'**iniziativa internazionale "Counter Ransomware"**, in cui convergono gli sforzi di oltre 50 partner dell'UE e di paesi terzi con l'obiettivo di far sì che gli autori dei reati **ransomware** rispondano delle loro azioni senza poter contare su alcuna protezione. L'iniziativa contribuisce a impedire che gli autori di reati ransomware beneficino di proventi illeciti, in modo da contrastarne le attività e consegnarli alla giustizia.

Gli oltre 100 milioni di immagini e video segnalati nel mondo nel solo 2023 che ritraggono **abusi sessuali sui minori**, a fronte di molti più casi non segnalati, dimostrano quanto questo fenomeno dilaghi a livelli allarmanti. I minori trascorrono più tempo online, il che li rende più vulnerabili all'adescamento determinando di conseguenza un aumento dei materiali di sfruttamento autoprodotti. In linea con la **strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori**[43] e con la **strategia globale dell'UE sui diritti dei minori**[44], la Commissione ha adottato una proposta che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori[45], imponendo nuovi obblighi ai prestatori di servizi online. Laddove la prevenzione non consenta di ridurre un rischio significativo, i prestatori di servizi potrebbero essere tenuti a rilevare, segnalare, rimuovere e bloccare gli abusi sessuali online sui minori. La proposta istituirebbe inoltre un **apposito Centro dell'UE** per agevolare l'attuazione del regolamento. La legislazione temporanea adottata per consentire ai prestatori di servizi online di continuare a individuare e segnalare volontariamente gli abusi sessuali su minori online è stata prorogata fino al 3 aprile 2026, al fine di concedere tempo sufficiente per trovare un accordo sul regolamento a lungo termine. Tale iniziativa è stata integrata da una proposta di aggiornamento della **direttiva del 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e il materiale pedopornografico**[46]. Le norme rivedute ampliano le definizioni dei reati, in particolare per stare al passo con l'aumento dell'attività criminale online, e introducono sanzioni più elevate e prescrizioni più specifiche in materia di prevenzione e di assistenza alle vittime.

È stato calcolato che metà di tutte le giovani donne è vittima di **violenza di genere online**[47]**.** La **direttiva sulla lotta alla violenza contro le donne e alla violenza domestica**, adottata a maggio del 2024, definisce come reati determinate forme di violenza che colpiscono oltremodo le donne, in particolare la condivisione non consensuale di immagini intime (compresi i deepfake), lo stalking online, le molestie online e l'istigazione misogina all'odio. La direttiva rafforzerà inoltre l'accesso delle vittime alla giustizia.

IV.2. Traffico di stupefacenti

Il traffico illecito di **stupefacenti** rappresenta una delle più importanti minacce che l'UE si trova ad affrontare. Si calcola che il mercato dello spaccio al dettaglio nell'UE abbia un valore di almeno 30 miliardi di EUR l'anno[48]. I sequestri di cocaina nell'UE hanno raggiunto livelli record[49]. Cresce la preoccupazione in merito alla produzione e alla proliferazione in Europa di

43 COM(2020) 607, adottata a luglio del 2020.
44 COM(2021) 142, adottata a marzo del 2021.
45 COM(2022) 209, adottata a maggio del 2022.
46 COM(2024) 60, adottata a febbraio del 2024.
47 Servizio Ricerca del Parlamento europeo (EPRS), *Combating gender-based violence: Cyberviolence, European added value assessment*, 2021.
48 Europol, 2024.
49 Nel 2021 sono state sequestrate 303 tonnellate di cocaina. Relazione europea sulla droga 2023, EMCDDA.

droghe sintetiche e al nesso tra traffico di stupefacenti e violenza[50]. L'**agenda e il piano d'azione dell'UE in materia di droga 2021-2025**[51] definiscono interventi concreti per intensificare l'azione a livello dell'UE, tra cui l'attuale rafforzamento della cooperazione internazionale in materia di traffico di stupefacenti e la trasformazione dell'Osservatorio europeo delle droghe e delle tossicodipendenze in **Agenzia dell'Unione europea sulle droghe**[52]. L'Agenzia entrerà in funzione nel luglio 2024.

L'agenda è stata integrata dalla **tabella di marcia dell'UE**, adottata dalla Commissione a ottobre del 2023[53], che definisce misure aggiuntive per contrastare il traffico di droga e la criminalità organizzata, compresa l'istituzione di una nuova **Alleanza europea dei porti** al fine di aumentare la resilienza dei porti alle infiltrazioni criminali attraverso il rafforzamento dell'operato delle autorità doganali, delle autorità di contrasto e degli attori pubblici e privati nei porti di tutta l'UE. L'attuazione della tabella di marcia ha inoltre comportato una valutazione tematica Schengen, nella quale sono state valutate le capacità degli Stati membri per quanto concerne la cooperazione di polizia, la protezione delle frontiere esterne e la gestione dei sistemi informatici ai fini della lotta al traffico di droga. La valutazione ha consentito di individuare 40 migliori pratiche.

IV.3. Traffico illegale di merci

Il traffico illegale di merci è un'attività estremamente redditizia, che ha un costo per la società non soltanto in termini di mancate entrate ma anche a causa dei pericoli per la salute e la sicurezza dei cittadini. È dunque necessaria una risposta coordinata da parte dei governi, delle autorità di contrasto e degli attori privati.

Il **traffico di armi da fuoco** alimenta la criminalità organizzata all'interno dell'UE e nei paesi del vicinato. Si calcola che 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 di nuove tecnologie come la stampa 3D, il traffico di armi da fuoco trova nuove modalità per sfuggire ai controlli. Unitamente al **piano d'azione 2020-2025 dell'UE sul traffico di armi da fuoco**[54], tutti gli Stati membri hanno ormai recepito nei rispettivi ordinamenti la **direttiva sulle armi da fuoco**[55], che migliora notevolmente la sicurezza rendendo più difficile l'acquisizione legale delle armi più pericolose. Il Parlamento europeo e il Consiglio hanno anche raggiunto un accordo sulla revisione delle **norme sulle autorizzazioni all'esportazione e sulle misure di importazione e transito per le armi da fuoco**[56] al fine di migliorare la tracciabilità delle armi da fuoco ad uso civile, ponendo un maggiore accento sulla digitalizzazione.

[50] All'inizio del 2024 due agenti sono stati uccisi a Barbate (Spagna) da presunti trafficanti di droga, mentre a Bruxelles (Belgio) sono avvenute diverse sparatorie legate ad episodi di violenza associata al traffico di droga, che hanno provocato diversi morti e feriti.

[51] COM(2020) 606.

[52] Regolamento (UE) 2023/1322, del 27 giugno 2023, riguardante l'Agenzia dell'Unione europea sulle droghe (EUDA).

[53] COM(2023) 641 final.

[54] COM(2020) 608 final.

[55] Direttiva (UE) 2021/555 relativa al controllo dell'acquisizione e della detenzione di armi.

[56] COM(2022) 480.

Anche il traffico illecito di beni culturali è un'attività lucrativa per i gruppi della criminalità organizzata e, in alcuni casi, per le parti in conflitto e i terroristi[57]. A dicembre del 2022 la Commissione ha adottato un piano d'azione dell'UE per rafforzare la lotta al **traffico illecito di beni culturali**[58], che prevede un dialogo con i portatori di interessi volto a promuovere un mercato dell'arte equo e riconosciuto che tuteli il patrimonio culturale.

IV.4. Traffico di migranti e tratta di esseri umani

Si calcola che oltre il 90 % dei migranti che arrivano nell'UE senza autorizzazione faccia ricorso ai servizi dei trafficanti. I profitti derivanti dal traffico di migranti sono stimati tra i 4,7 e i 6 miliardi di EUR all'anno a livello mondiale e si calcola che dal 2014 i decessi dovuti a questo commercio criminale siano stati, nel solo Mediterraneo, oltre 28 000.

Per intensificare la lotta al **traffico di migranti**, la Commissione ha proposto di aggiornare l'attuale quadro legislativo[59] con una proposta di direttiva che mira a garantire una maggiore efficacia nelle indagini e nelle azioni penali nei confronti dei trafficanti e con una proposta di regolamento che rafforza il coordinamento dell'UE potenziando il **Centro europeo contro il traffico di migranti** in seno a Europol e migliorando la condivisione delle informazioni tra le autorità competenti. La Commissione invita il Parlamento europeo e il Consiglio a trovare quanto prima un accordo su tali fascicoli. In parallelo il 28 novembre 2023 la Commissione ha varato un'**alleanza mondiale per contrastare il traffico di migranti**, con un **invito ad agire**, di cui è attualmente in corso l'attuazione con i portatori di interessi. Ad aprile del 2024 la Commissione ha organizzato un evento finalizzato alla creazione di una comunità di portatori di interessi e autorità competenti al fine di contrastare l'utilizzo dei servizi digitali nel traffico di migranti. La Commissione sostiene inoltre le autorità di contrasto e le autorità giudiziarie dei principali paesi terzi per rafforzare la loro capacità di indagine e azione penale nei confronti di gruppi organizzati dediti al traffico di migranti e alla tratta di esseri umani.

Molte delle reti criminali dedite al traffico di migranti sono anche implicate nella **tratta di esseri umani**. Europol calcola che a livello mondiale i profitti derivanti dalla tratta di esseri umani superino ogni anno i 29,4 miliardi di EUR[60]. Le vittime sono per la maggior parte donne e ragazze, ma è in aumento anche la tratta di uomini, in particolare a fini di sfruttamento lavorativo. Ad aprile del 2021 la strategia dell'UE per la lotta alla tratta di esseri umani 2021-2025[61] ha fornito un quadro globale d'azione. La direttiva anti-tratta recentemente riveduta contempla nuove forme di sfruttamento (maternità surrogata, matrimonio forzato e adozione illegale), rafforza gli strumenti per le autorità di contrasto e giudiziarie e obbliga gli Stati membri a imporre sanzioni nei confronti di chi ricorre consapevolmente a servizi che dipendono dalle vittime della tratta. Eurojust, in collaborazione con il coordinatore anti-tratta dell'UE, ha istituito un gruppo di riflessione composto da pubblici ministeri specializzati nella tratta di esseri umani.

IV.5. Reati contro l'ambiente

I reati ambientali causano spesso danni irreversibili e a lungo termine alla salute delle persone, nonché agli ecosistemi e all'ambiente. Sono estremamente lucrativi e spesso vedono

---

[57] Cfr. ad esempio le risoluzioni 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) e 2617 (2021) del Consiglio di sicurezza delle Nazioni Unite e la dichiarazione di Roma dei ministri della Cultura del G20 del 30 luglio 2021.

[58] COM(2022) 800.

[59] COM(2023) 754 e COM(2023) 755.

[60] *Study on the economic, social and human costs of trafficking in human beings within the EU* (2020).

[61] COM(2021) 171.

coinvolta la criminalità organizzata, ma sono difficili da individuare e perseguire. La criminalità ambientale è la terza attività criminale più importante al mondo in termini di proventi; i comportamenti e i profitti illeciti aumentano in misura significativa ogni anno[62] e sono attualmente in ascesa.

I profitti illeciti connessi a questo tipo di reati sono stimati in 200 miliardi di EUR all'anno, con notevoli ripercussioni negative sull'economia, ma i danni all'ambiente, alla biodiversità, alla salute umana e alla sicurezza sono incalcolabili. L'azione a livello dell'UE intesa a reprimere la criminalità ambientale è stata rafforzata attraverso **la nuova direttiva sulla tutela penale dell'ambiente**[63], che amplia la gamma di reati da sottoporre a indagine e azione penale e prevede tipi e livelli concreti di sanzioni da irrogare nei confronti delle persone fisiche e giuridiche che hanno commesso reati ambientali. Sono stati intrapresi ulteriori interventi con l'adozione del regolamento sulle spedizioni di rifiuti e una più efficace azione di contrasto al disboscamento illegale mediante l'introduzione di nuove norme sui prodotti a deforestazione zero. Inoltre il **piano d'azione riveduto dell'Unione europea contro il traffico illegale di specie selvatiche** aggiorna le priorità dell'UE per prevenire meglio tale fenomeno e affrontarne le cause alla radice.

IV.6. Criminalità economica e finanziaria

Il riciclaggio di denaro e il finanziamento del terrorismo rappresentano una grave minaccia per l'integrità dell'economia e del sistema finanziario dell'UE e per la sicurezza dei suoi cittadini. Secondo le stime di Europol, circa l'1 % del prodotto interno lordo annuo dell'UE viene utilizzato per attività finanziarie sospette[64].

L'UE ha adottato nuove norme in materia di **prevenzione del riciclaggio e del finanziamento del terrorismo**, al fine di rafforzare la prevenzione e la rilevazione dei tentativi da parte di criminali di riciclare proventi illeciti o di finanziare attività terroristiche mediante il sistema finanziario dell'Unione[65], ponendo a carico degli operatori del settore privato obblighi a livello dell'Unione direttamente applicabili, compreso l'obbligo di effettuare l'adeguata verifica della clientela e di segnalare i casi sospetti. I compiti e i poteri dei supervisori nazionali e delle unità di informazione finanziaria saranno rafforzati e armonizzati per garantire che le autorità competenti svolgano i rispettivi compiti più efficacemente e cooperino in maniera più efficiente. Inoltre norme chiare rafforzano la funzione preventiva della titolarità effettiva e dei registri dei conti bancari. Sarà istituita una nuova **Autorità per la lotta al riciclaggio**, che avrà poteri di supervisione diretta sui soggetti del settore finanziario che operano su base transfrontaliera e sono più a rischio e fornirà sostegno operativo per l'analisi congiunta dei casi transfrontalieri da parte delle unità di informazione finanziaria.

Oltre alle nuove norme antiriciclaggio, la **direttiva riguardante il recupero e la confisca dei beni**, di recente adozione, costituirà uno strumento importante nella lotta contro la criminalità organizzata e le forme gravi di criminalità, stabilendo misure più incisive per confiscare i profitti illeciti derivanti da un'ampia gamma di reati. Gli uffici per il recupero dei beni avranno il compito di reperire, identificare e congelare i beni di origine criminosa. In combinazione con la **direttiva relativa alla qualifica come reato della violazione delle misure restrittive dell'Unione**, di recente adozione, che armonizza la definizione di tali reati

---

62 *Organized crime groups pushing environmental security to tipping point (interpol.int)*.
63 Direttiva 99/2008/CE sulla tutela penale dell'ambiente.
64 Gruppo di informazione finanziaria di Europol, *From suspicion to action* (2017).
65 COM(2021) 420, COM(2021) 421, COM(2021) 422 e COM(2021) 423.

e le relative sanzioni in tutta l'Unione, tali norme consentiranno anche il tracciamento, il congelamento, la gestione e la confisca dei profitti ottenuti dai criminali attraverso la violazione delle sanzioni dell'Unione.

IV.7. Lotta contro la corruzione

La **corruzione** arreca gravi danni alla società, indebolendo le istituzioni pubbliche, compromettendo la realizzazione delle politiche pubbliche e l'erogazione dei servizi pubblici e minando la fiducia dei cittadini nelle istituzioni democratiche. La corruzione nel settore privato indebolisce il mercato unico e offre nuove opportunità alla criminalità organizzata.

Al fine di affrontare i rischi e le sfide legati alla corruzione, la Commissione ha proposto[66] una **direttiva sulla lotta contro la corruzione** per rafforzare le norme che configurano come reato la corruzione e armonizzano le sanzioni in tutta l'UE. Il Parlamento europeo ha adottato la sua posizione a febbraio del 2024. Affinché la corruzione nell'UE non resti impunita, la Commissione invita il Consiglio a proseguire le discussioni e a sostenere gli obiettivi della proposta della Commissione.

La **direttiva PIF**[67] stabilisce norme specifiche per proteggere il bilancio dell'UE da attività criminali, compresa la corruzione. Una solida attuazione di tale misura, unitamente alla proposta di direttiva anticorruzione, è indispensabile per mantenere le finanze dell'UE al riparo da frodi e attività di corruzione. La Commissione fornisce il suo contributo avviando, ove necessario, procedure di infrazione. L'OLAF e la **Procura europea** svolgono un ruolo fondamentale a tale riguardo, conducendo indagini sulle irregolarità e perseguendo i reati che ledono gli interessi finanziari dell'Unione[68]. La nuova **rete dell'UE contro la corruzione**[69], che rappresenta un consesso in cui tutti i portatori di interessi nell'UE possono scambiare buone prassi, opportunità, idee e piani per ulteriori attività, si è riunita per la prima volta a settembre del 2023.

IV.8. Protezione delle vittime di reato

Le **vittime** di ogni tipo di reato meritano sostegno e attenzione. La Commissione ha già realizzato la maggior parte delle azioni contemplate nella prima **strategia dell'UE sui diritti delle vittime (2020-2025)**[70]. Il 12 luglio 2023 la Commissione ha proposto una direttiva che modifica la **direttiva sui diritti delle vittime** del 2012[71] per rafforzare ulteriormente i diritti di tutte le vittime di reato nell'UE, in particolare i diritti delle vittime più vulnerabili.

L'UE in azione

Il 5 aprile 2024 Europol ha pubblicato una relazione contenente una prima mappatura delle reti criminali più temibili, che costituisce una delle azioni fondamentali previste dalla tabella di marcia dell'UE per contrastare il traffico di droga e la criminalità organizzata. I risultati indicano che 821 reti criminali ad alto rischio, costituite nel loro complesso da 25 000 membri, rappresentano la minaccia principale. Il 34 % delle reti criminali ad alto rischio è

66 COM(2023) 234.

67 Direttiva (UE) 2017/1371, del 5 luglio 2017, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale. Dal mese di dicembre 2021 la Commissione ha avviato 19 procedure di infrazione per inosservanza della direttiva PIF.

68 La Polonia ha aderito formalmente alla Procura europea a febbraio del 2024.

69 JOIN(2023) 12.

70 COM(2020) 258.

71 COM(2023) 424.

attivo nell'UE da oltre 10 anni, il 76 % è presente o attivo in un massimo di 7 paesi e i membri di tali reti rappresentano 112 nazionalità.

Nell'ambito di un'operazione di repressione della criminalità transfrontaliera ("Operazione Mobile 6"), 400 funzionari delle autorità di contrasto di 25 paesi hanno recuperato 505 automobili rubate, 2 000 parti di automobili, 16 imbarcazioni, 32 motori fuoribordo e 248 documenti contraffatti. Sono stati fermati 209 presunti trafficanti di esseri umani. Nel 2022 e nel 2023 l'EPPO ha svolto un'indagine importante, estesa a oltre 30 paesi, su gruppi della criminalità organizzata sospettati di essere responsabili di frodi transfrontaliere in materia di IVA per un valore stimato in 2,2 miliardi di EUR ("Operazione Admiral").

V GARANTIRE LA SICUREZZA DELLE FRONTIERE DELL'UE E SOSTENERE LA COOPERAZIONE TRA AUTORITÀ DI CONTRASTO E AUTORITÀ GIUDIZIARIE

In uno spazio senza controlli alle frontiere interne i funzionari di polizia di uno Stato membro dovrebbero avere accesso alle informazioni di cui dispongono i loro colleghi di un altro Stato membro. Di norma essi dovrebbero operare all'insegna di una cooperazione efficace. Per tale motivo è essenziale rafforzare gli strumenti a disposizione delle autorità di contrasto e di quelle giudiziarie in tutta l'UE per lo scambio di informazioni e la cooperazione transfrontaliera.

Come evidenziato nella relazione sullo stato di Schengen 2024[72], il rafforzamento continuo dello **spazio Schengen**, con il superamento delle carenze emerse nelle valutazioni e la concentrazione degli sforzi collettivi grazie a una governance Schengen più concertata, contribuisce non soltanto alla libera circolazione ma anche alla sicurezza dei cittadini di tutta l'Europa. Il buon funzionamento dello spazio Schengen è sorretto da tre pilastri: gestione efficace delle frontiere esterne dell'UE, rafforzamento delle misure interne per compensare l'assenza di controlli alle frontiere interne (in particolare misure in materia di cooperazione di polizia, sicurezza e gestione della migrazione) e una preparazione e una governance solide[73].

La gestione delle frontiere esterne sarà rafforzata grazie a nuove norme in materia di accertamenti[74] sugli arrivi irregolari. La nuova definizione di strumentalizzazione dei migranti[75] contribuirà ad affrontare il problema dello sfruttamento dei migranti negli attacchi ibridi alle frontiere esterne dell'UE, osservato ad esempio al confine con la Bielorussia nel 2021. Un'efficace gestione della migrazione attraverso una procedura fluida alle frontiere[76] rafforzerà lo spazio Schengen garantendo una più stretta cooperazione e una ripartizione delle responsabilità tra gli Stati membri. Il codice frontiere Schengen, una volta adottato, garantirà un maggiore coordinamento a livello dell'UE e doterà gli Stati membri di strumenti più efficaci per affrontare le sfide emergenti alle frontiere esterne comuni dell'UE e all'interno dello spazio Schengen, mentre le agenzie dell'UE continueranno ad aiutare gli Stati membri a mantenere un elevato livello di sicurezza interna nello spazio Schengen.

---

[72] COM(2024) 173.

[73] A marzo del 2024 la Bulgaria e la Romania sono diventate membri dello spazio Schengen che applicano appieno l'*acquis* di Schengen e sono stati aboliti i controlli alle frontiere interne marittime e aeree.

[74] COM(2020) 612.

[75] COM(2020) 613.

[76] Regolamento che stabilisce una procedura comune di protezione internazionale nell'Unione (COM(2016) 467 final e COM(2020) 614 final).

Il **pacchetto sulla cooperazione di polizia**[77] ha proposto un importante aggiornamento degli strumenti disponibili per migliorare le operazioni transfrontaliere, fornire canali e tempistiche chiari per lo scambio di informazioni tra le forze dell'ordine nei vari Stati membri e rafforzare il ruolo di **Europol**. La revisione delle norme sullo **scambio automatizzato** contribuirà a colmare le lacune in materia d'informazione e a rafforzare la prevenzione, l'indagine e l'accertamento dei reati nell'UE. Con la revisione del quadro giuridico per l'utilizzo delle **informazioni anticipate sui passeggeri** sono stati compiuti importanti progressi anche nello sviluppo di efficaci strumenti atti a garantire viaggi aerei agevoli verso l'UE, in provenienza da essa e al suo interno, migliorando al contempo la capacità delle autorità di individuare le minacce per la sicurezza.

Per quanto concerne il terrorismo, la modifica del **regolamento Eurojust** riguardante lo scambio digitale di informazioni nei casi di terrorismo, adottata nel 2023[78], renderà più efficace lo scambio di informazioni tra le autorità nazionali competenti ed Eurojust attraverso il registro giudiziario europeo antiterrorismo.

Per perseguire i criminali informatici sono necessari particolari mezzi di prova; sono stati realizzati progressi indispensabili per rafforzare la cooperazione transfrontaliera nello **scambio di prove elettroniche**. Il secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa[79] dovrebbe intensificare la lotta contro la criminalità informatica offrendo alle autorità giudiziarie maggiori possibilità di raccogliere le prove elettroniche di un reato (ad esempio attraverso l'istituzione di squadre investigative comuni). Le norme interne dell'UE in materia di **prove elettroniche**[80], adottate nel 2023, introdurranno un nuovo sistema per l'acquisizione di prove elettroniche nei procedimenti penali consentendo alle autorità di contrasto e a quelle giudiziarie di rivolgersi direttamente ai prestatori di servizi privati ubicati in un altro Stato membro.

L'**intelligenza artificiale** è diventata una componente versatile e cruciale nelle tecnologie di cui dispongono le autorità di contrasto e altri soggetti impegnati nella sicurezza interna; allo stesso tempo l'utilizzo con queste finalità dovrebbe rispettare i diritti fondamentali. L'IA generativa, però, può anche essere utilizzata dai criminali informatici per organizzare sofisticati attacchi informatici e altre attività illecite. Il **regolamento sull'intelligenza artificiale (legge sull'IA)** è un primo passo verso la regolamentazione dell'uso dell'IA all'interno dell'UE e fissa i confini per l'utilizzo responsabile dei sistemi di IA in tale settore, salvaguardando nel contempo i diritti fondamentali e la sicurezza dei cittadini. L'ufficio per l'IA sosterrà l'attuazione del regolamento, garantendo il rispetto delle tutele e dei requisiti procedurali in esso previsti. La Commissione contribuirà all'elaborazione di orientamenti adeguati per sostenere le autorità di contrasto e altri operatori della sicurezza nell'utilizzo adeguato ed efficace dell'IA nell'ambito delle rispettive attività.

Mentre proseguono i lavori per l'istituzione di un **sistema di comunicazione critica dell'UE,** un nuovo regolamento che istituisce una piattaforma di collaborazione per le squadre

---

77 COM(2021) 780, COM (2021) 782 e COM(2021) 784.

78 Regolamento (UE) 2023/2131 riguardante lo scambio digitale di informazioni nei casi di terrorismo.

79 Adottato dal Comitato dei ministri il 17 novembre 2021.

80 Regolamento (UE) 2023/1543, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, e direttiva (UE) 2023/1544, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali.

investigative comuni[81] fornisce ai soggetti coinvolti strumenti sicuri per lo scambio di prove e informazioni, la comunicazione efficiente e la cooperazione agevole con i paesi terzi.

Con l'aumento dei reati transfrontalieri, l'UE si trova sempre più spesso di fronte a situazioni in cui diversi Stati membri hanno la giurisdizione per esercitare l'azione penale nello stesso caso. Le nuove norme sul **trasferimento dei procedimenti penali** contribuiranno a prevenire una duplicazione inefficiente dei procedimenti e ad evitare casi di impunità qualora sia rifiutata la consegna di una persona in forza di un mandato d'arresto europeo, garantendo al contempo che siano debitamente rispettati i diritti degli indagati e delle vittime. Una cooperazione giudiziaria transfrontaliera efficiente richiede una comunicazione sicura, affidabile ed efficiente in termini di tempo tra gli organi giurisdizionali, che d'ora in poi sarà possibile grazie al **pacchetto sulla giustizia digitale**. Le autorità saranno in grado di comunicare tra loro e di scambiare dati relativi alle cause in materia civile, commerciale e penale attraverso canali digitali sicuri e affidabili. Ciò faciliterà la lotta contro la criminalità e la rapida attuazione da parte degli Stati membri sarà fondamentale.

L'UE in azione
Nel 2022 l'EMPACT ha consentito di:
- procedere a 9 922 arresti
- identificare 4 019 vittime della tratta di esseri umani
- procedere all'arresto di 3 646 trafficanti di migranti
- effettuare sequestri di beni e denaro per oltre 180 milioni di EUR
- sequestrare oltre 62 tonnellate di droga.

VI NESSO TRA SICUREZZA INTERNA ED ESTERNA: LA SICUREZZA NELL'UE, NEI PAESI VICINI E NEI PAESI PARTNER

La crescente interconnessione tra sicurezza interna ed esterna è diventata più evidente negli ultimi anni dato l'attuale contesto geopolitico. L'UE è più sicura quando lo sono anche i suoi partner. Nel solo 2023 sono stati spesi circa 700 milioni di EUR per potenziare le capacità dei paesi terzi e rafforzare la cooperazione dell'UE con tali paesi in materia di lotta al terrorismo e di prevenzione e contrasto dell'estremismo violento; il 72 % di tale importo è stato destinato all'Africa per via della crescente instabilità e della presenza di gruppi terroristici nel Sahel. Si tratta di una spesa cinque volte superiore a quella di 10 anni fa. Nel frattempo la cooperazione nell'attività di contrasto con i paesi terzi è stata integrata in tutti i piani d'azione operativi dell'EMPACT.

La Commissione ha agito prontamente per prevenire le minacce per la sicurezza interna derivanti dalla guerra di aggressione della Russia nei confronti dell'**Ucraina,** garantendo la massima vigilanza per quanto riguarda lo sfruttamento del conflitto e dei flussi di coloro che cercano rifugio in Europa da parte della criminalità organizzata e dei gruppi di trafficanti. I servizi della Commissione e il SEAE, insieme al coordinatore antiterrorismo dell'UE, hanno convenuto con l'Ucraina di istituire un dialogo strutturato sulla sicurezza interna, anche in ambiti quali il traffico di armi da fuoco e la gestione delle frontiere. Il dialogo in materia di cibersicurezza tra l'UE e l'Ucraina, abbinato al sostegno politico, tecnico, finanziario e materiale coordinato da parte dell'UE, hanno aiutato l'Ucraina a rafforzare la sua

[81] Regolamento (UE) 2023/969, del 10 maggio 2023, che istituisce una piattaforma di collaborazione come ausilio al funzionamento delle squadre investigative comuni.

ciberresilienza. L'annunciato ufficio dell'UE per l'innovazione nel settore della difesa a Kiev fungerà da ponte tra le start-up e gli innovatori dell'UE e l'industria e le forze armate ucraine, anche nel settore della ciberdifesa, e contribuirà a trasmettere i progressi tecnologici che possono avere un impatto sul campo di battaglia.

Anche la repubblica di **Moldova** è molto esposta alle implicazioni criminali e di sicurezza dell'invasione dell'Ucraina da parte della Russia e a una serie di minacce ibride e informatiche. A luglio del 2022 i servizi della Commissione, in cooperazione con il SEAE, hanno varato un polo di sostegno dell'UE per la sicurezza interna e la gestione delle frontiere con la Repubblica di Moldova. L'UE sta aiutando la Moldova a migliorare la propria resilienza e la capacità di contrastare le minacce ibride e informatiche, anche attraverso l'attuazione delle raccomandazioni contenute nello studio sui rischi ibridi, che è stato riavviato, e la missione di partenariato dell'UE nella Repubblica di Moldova.

La sicurezza dei partner dei **Balcani occidentali** è strettamente connessa alla sicurezza interna dell'UE, data la loro prossimità geografica, e la cooperazione in materia di contrasto tra l'UE e questi paesi ha continuato a intensificarsi durante l'attuale mandato. Il piano d'azione comune sulla lotta al terrorismo, firmato con tutti i partner dei Balcani occidentali nel 2018, ha registrato buoni progressi e, laddove la maggior parte delle azioni è stata completata, ossia nella Macedonia del Nord, in Albania e nel Montenegro, sono stati firmati accordi aggiornati. L'UE continua inoltre a rafforzare la ciberresilienza collettiva dei partner dei Balcani occidentali attraverso il sostegno operativo e tecnico, la formazione e il coinvolgimento della regione nei meccanismi di cibersicurezza dell'UE.

Anche la situazione attuale **in Medio Oriente** ha un potenziale impatto sulla sicurezza interna dell'UE, compreso un aumento significativo degli incidenti in alcuni Stati membri. La rete di investigatori finanziari antiterrorismo ha consentito agli Stati membri di condividere informazioni su casi correlati alle attività di raccolta di fondi di Hamas nell'UE, consentendo agli investigatori di capire meglio come affrontare tali minacce.

Alla luce degli sviluppi in **Afghanistan**, in coordinamento con la Commissione, l'alto rappresentante, la presidenza e le principali agenzie dell'UE, il coordinatore antiterrorismo dell'UE ha elaborato un piano d'azione per la lotta al terrorismo sull'Afghanistan, approvato dal Consiglio nell'ottobre 2021. L'UE conferma il proprio impegno in Afghanistan e sta rafforzando il proprio ruolo in tutta la regione attraverso una cooperazione rafforzata con i **paesi dell'Asia centrale** in materia di sicurezza e un dialogo con il **Pakistan** sulla lotta al terrorismo.

L'UE ha rafforzato la cooperazione con i paesi dell'**America latina e dei Caraibi**, in particolare per quanto riguarda la lotta contro la criminalità organizzata, il traffico di stupefacenti e il finanziamento del terrorismo.

La **cooperazione multilaterale** è al centro dell'approccio dell'UE. L'UE collabora strettamente con l'ONU, in particolare con l'Ufficio delle Nazioni Unite per l'antiterrorismo e la direzione esecutiva del comitato antiterrorismo. L'UE collabora anche con gli oltre 40 organismi delle Nazioni Unite che compongono il patto globale delle Nazioni Unite per il coordinamento della lotta al terrorismo. Dal settembre 2022 l'UE presiede, insieme all'Egitto, il Forum globale contro il terrorismo, un forum multilaterale che sostiene gli aspetti civili della lotta contro il terrorismo e l'estremismo violento, con un'attenzione particolare all'Africa. L'UE è inoltre un partner non militare della coalizione internazionale per combattere il Da'esh e dialoga attivamente con la NATO, Interpol e l'OSCE. Nel campo della lotta contro il

riciclaggio e il finanziamento del terrorismo e della proliferazione, la Commissione contribuisce attivamente all'operato del gruppo di azione finanziaria internazionale. L'impegno nella coalizione internazionale per combattere il Da'esh è una componente importante della risposta di politica estera dell'UE al terrorismo/all'estremismo violento e alle minacce correlate.

L'UE ha notevolmente approfondito e ampliato la sua **cooperazione con la NATO**, in particolare in settori quali la resilienza, le infrastrutture critiche, la sicurezza sanitaria, la lotta contro le minacce informatiche e ibride, compresa la disinformazione, la mobilità militare, lo spazio, le tecnologie emergenti e innovative, il clima e la difesa. A gennaio del 2022 è stato avviato un dialogo strutturato sulla resilienza, rafforzato dalla task force UE-NATO sulla resilienza delle infrastrutture critiche. Nel giugno 2023 la task force ha pubblicato una relazione che definisce le attuali sfide di sicurezza per le infrastrutture critiche suddivise in quattro settori chiave (energia, trasporti, infrastrutture digitali e spazio). L'attuazione delle raccomandazioni per un'ulteriore cooperazione UE-NATO, contenute nella relazione, procede a ritmo sostenuto, con particolare attenzione alle esercitazioni, al coordinamento civile-militare e al dialogo con il settore privato.

Gli orientamenti di attuazione rivisti del **pacchetto di strumenti della diplomazia informatica dell'UE** permettono di elaborare strategie durature, mirate, coerenti e coordinate contro gli autori di minacce informatiche persistenti, affrontando meglio le sfide legate alle continue minacce e attività di livello più basso che rientrano nella cosiddetta "zona grigia" e che provengono da tali soggetti. L'UE continua ad adoperarsi per rafforzare la ciberresilienza, sostenere i partner e promuovere il quadro delle Nazioni Unite per il comportamento responsabile nel ciberspazio, nonché infrastrutture digitali sicure attraverso il Global Gateway. L'UE ha intensificato la **cooperazione in materia di sicurezza informatica con la NATO** attraverso uno specifico dialogo strutturato **e con i partner internazionali**. Il dialogo con gli Stati Uniti, che è sfociato nel piano d'azione congiunto UE-USA per i prodotti cibersicuri, frutto del lavoro tecnico congiunto di mappatura e raffronto della legislazione e delle iniziative di normazione, costituisce un valido esempio della cooperazione concreta dell'UE con i partner a sostegno della cibersicurezza globale. Nel 2023 l'UE ha inoltre ripreso i dialoghi sulla cibersicurezza con il Giappone e l'India e ha avviato il primo ciberdialogo con il Regno Unito, offrendo la possibilità di un confronto per quanto riguarda il panorama delle minacce, lo sviluppo delle capacità informatiche e la cooperazione nei consessi multilaterali e regionali.

Negli ultimi anni l'UE ha istituito **dialoghi sulla lotta al terrorismo** con i principali paesi partner e le principali organizzazioni multilaterali, tra cui le Nazioni Unite, l'Australia, l'Arabia Saudita, l'Egitto, l'India, il Pakistan, la Turchia e gli Stati Uniti. L'UE inoltre può contare su una rete di 20 esperti in materia di antiterrorismo/sicurezza nelle delegazioni dell'UE in tutto il mondo; tale rete sostiene gli obiettivi della politica estera e di sicurezza dell'UE in relazione alla lotta contro il terrorismo e l'estremismo violento. La Commissione continua ad adoperarsi per eliminare i contenuti terroristici online da internet, rispettando nel contempo le libertà fondamentali nello spirito dell'"appello di Christchurch"[82]. Nell'ambito dell'attuazione dell'accordo sugli scambi commerciali e la cooperazione, il primo ciclo di dialoghi UE-Regno Unito sul ciberterrorismo e sulla lotta al terrorismo si è tenuto a dicembre del 2023 e a febbraio del 2024.

[82] L'appello di Christchurch è stato lanciato dalla Francia e dalla Nuova Zelanda nel 2019.

In relazione al **traffico di stupefacenti**, l'incontro ad alto livello nell'ambito del meccanismo di coordinamento e cooperazione sulle droghe UE-CELAC, svoltosi a febbraio del 2024, si è concluso con l'adozione di una dichiarazione[83] nella quale sono state individuate le priorità della cooperazione per i prossimi cinque anni. L'UE contribuisce ai lavori della coalizione globale per affrontare le minacce delle droghe sintetiche, varata dagli Stati Uniti. L'Osservatorio europeo delle droghe e delle tossicodipendenze sta intensificando la cooperazione con la Colombia, l'Ecuador e il Cile attraverso la conclusione di accordi di lavoro.

Misure efficaci di recupero e confisca dei beni a livello mondiale sono essenziali nella lotta contro la criminalità organizzata e le forme gravi di criminalità. La Commissione è impegnata a garantire un approccio comune dell'UE nei prossimi negoziati su un protocollo addizionale alla convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo (Convenzione di Varsavia), che necessita di aggiornamento, alla luce degli sviluppi internazionali e della rapida evoluzione del panorama delle attività criminali. Nell'aprile 2024 la Commissione ha adottato una raccomandazione di decisione nella quale chiede al Consiglio di autorizzarla a negoziare il protocollo per conto dell'UE.

In un contesto di **minacce ibride** sempre più complesse e sofisticate, l'attuazione della bussola strategica dell'UE per la sicurezza e la difesa è di fondamentale importanza. I servizi della Commissione e il Servizio europeo per l'azione esterna hanno contribuito alla creazione del pacchetto di strumenti dell'UE contro le minacce ibride, che fornisce un quadro per una risposta coordinata alle campagne ibride, riunendo tutte le misure e tutti gli strumenti interni ed esterni pertinenti. Il protocollo operativo dell'UE per contrastare le minacce ibride, aggiornato nell'aprile 2023, contribuisce a garantire un'applicazione efficace di processi e strumenti in risposta alle minacce ibride durante l'intero ciclo di gestione delle crisi. È in corso la creazione di gruppi di risposta rapida dell'UE alle minacce ibride, che forniranno un'assistenza mirata e a breve termine nella lotta contro le minacce ibride negli Stati membri dell'UE e nei paesi partner.

Il ricorso strategico e coordinato alla **manipolazione delle informazioni e all'ingerenza da parte di soggetti stranieri** rappresenta un'evidente minaccia per la sicurezza dell'UE e dei suoi partner, considerato che metà della popolazione mondiale sarà chiamata alle urne nel 2024. Negli ultimi anni, facendo leva sul piano d'azione per la democrazia europea e attuando la bussola strategica dell'UE per la sicurezza e la difesa, l'UE ha intensificato la lotta contro la manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri e ha istituito una task force della Commissione sulla comunicazione strategica che contribuisce a predisporre risposte adeguate.

Sono emersi **tentativi di ingerenza straniera** in alcuni casi di presunta corruzione di politici dell'UE che avrebbero ricevuto pagamenti da paesi terzi. Il rischio di ingerenze straniere è particolarmente accentuato a ridosso delle elezioni europee. Per razionalizzare la condivisione delle informazioni in vista delle elezioni, nell'aprile 2024 il Consiglio ha attivato i dispositivi integrati per la risposta politica alle crisi (IPCR).

[83] Meccanismo di coordinamento e cooperazione sulle droghe UE-CELAC - Dichiarazione di La Paz, 22 febbraio 2024.

La **bussola strategica dell'UE e l'analisi delle minacce** riconoscono che il cambiamento climatico e il degrado ambientale hanno un crescente impatto nel campo della pace, della sicurezza e della difesa. Tali fattori, sommati alla scarsità di risorse idriche, rappresentano una minaccia per i contesti fragili nei paesi del vicinato dell'UE e possono determinare crisi legate allo sfollamento, turbolenze interne o controversie tra Stati. A giugno del 2023 la Commissione e l'alto rappresentante per gli affari esteri e la politica di sicurezza hanno adottato una comunicazione congiunta sul nesso tra clima e sicurezza[84].

A dicembre del 2023 il pacchetto per la **difesa della democrazia** ha definito le modalità di utilizzo delle norme sulla trasparenza della rappresentanza d'interessi per proteggere le democrazie dell'UE dal rischio di ingerenze occulte[85] e ha illustrato l'attività dell'UE nella lotta contro la disinformazione, ad esempio gli scambi intensivi in tempo reale tra le istituzioni, il ricorso alle reti di verifica dei fatti e l'intenso lavoro svolto con le principali piattaforme attraverso il codice di buone pratiche sulla disinformazione e ora anche mediante il regolamento sui servizi digitali.

L'UE in azione

In un mondo globalizzato, in cui le forme gravi di criminalità e il terrorismo sono sempre più transnazionali, la cooperazione e lo scambio di informazioni tra le autorità di contrasto e le autorità giudiziarie dei paesi terzi sono essenziali.

Europol ed Eurojust hanno firmato accordi di cooperazione con paesi terzi per migliorare lo scambio di informazioni nella loro lotta contro il terrorismo e la criminalità organizzata. A luglio del 2023 è entrato in vigore un accordo tra l'UE e la Nuova Zelanda sullo scambio di dati personali con Europol e sono in corso i negoziati con Europol sugli accordi con Bolivia, Brasile, Messico, Perù e Ecuador.

Eurojust facilita la cooperazione giudiziaria per combattere le forme gravi di criminalità anche con i paesi terzi, mediante 13 accordi di cooperazione, con le reti giudiziarie internazionali, attraverso accordi di lavoro, e nell'ambito di una rete di oltre 70 giurisdizioni in tutto il mondo nonché tramite punti di contatto. 12 magistrati di collegamento di paesi terzi sono distaccati presso Eurojust. Sono in corso i negoziati con Brasile, Argentina e Colombia sugli accordi di cooperazione giudiziaria internazionale con Eurojust.

Anche l'ENISA ha rafforzato la cooperazione e la propria azione a livello internazionale e ha recentemente firmato accordi di lavoro con le agenzie per la sicurezza informatica ucraina e statunitense.

VII ATTUARE L'UNIONE DELLA SICUREZZA

La corretta attuazione dell'Unione della sicurezza è una responsabilità condivisa, per la quale ogni soggetto deve assumersi le proprie responsabilità. La Commissione sostiene le strategie, la politica, la legislazione, l'organizzazione e il rafforzamento delle capacità degli Stati membri per l'attuazione del lavoro svolto nell'ambito dell'Unione della sicurezza, anche attraverso lo strumento di sostegno tecnico.

VII.1. Infrazioni

[84] JOIN(2023) 19.
[85] COM(2023) 637.

Il diritto dell'UE ha ormai consolidato nuove norme rigorose per proteggere meglio i cittadini dell'UE ma spetta agli Stati membri recepirle, attuarle e applicarle con tempestività. Il livello di attuazione della legislazione dell'UE nel settore dell'Unione della sicurezza da parte degli Stati membri è per lo più soddisfacente, ma nell'ambito di questo tema sensibile non sono ammessi anelli deboli.

Ogniqualvolta necessario, la Commissione adempie all'obbligo di utilizzare le procedure di infrazione e deferisce gli Stati membri alla Corte di giustizia dell'Unione europea a fronte di violazioni del diritto dell'UE. Grazie alla stretta collaborazione tra la Commissione e gli Stati membri, è stato dato seguito a molte delle procedure di infrazione avviate per motivi legati alla legislazione nell'ambito della strategia per l'Unione della sicurezza.

VII.2. Ruolo degli organi e organismi dell'UE

Gli organi e gli organismi dell'UE nei settori della giustizia, degli affari interni e della cibersicurezza svolgono un ruolo fondamentale nell'attuazione dell'*acquis* dell'UE in materia di sicurezza, che continua ad espandersi via via che le loro competenze vengono estese. Tale cooperazione ha prodotto risultati concreti, come dimostra ad esempio l'**EMPACT**, che facilita la cooperazione multidisciplinare strutturata degli Stati membri, con il sostegno di tutte le istituzioni e di tutti gli organi e organismi dell'UE. Le operazioni condotte mediante l'EMPACT, anche ricorrendo ad apposite task force operative, coordinano le attività degli Stati membri e dei partner operativi nella lotta alle reti criminali e ai reati gravi.

L'**ENISA** è stata fondamentale nel rafforzare la capacità dell'UE di prevenire, individuare e scoraggiare gli attacchi informatici e di rispondere ad essi, promuovendo nel contempo la ciberresilienza, salvaguardando le nostre comunicazioni e i nostri dati e garantendo che l'economia e la società online siano al sicuro. Avvalendosi della consulenza e del sostegno di esperti in materia di cibersicurezza, anche attraverso relazioni sulla conoscenza situazionale e valutazioni dei rischi, l'ENISA facilita la cooperazione e la condivisione di informazioni tra gli Stati membri, le istituzioni dell'UE e altri portatori di interessi. I suoi compiti sono stati rafforzati in linea con le nuove norme in materia di cibersicurezza. Il recente aggiornamento del compendio sulla cibersicurezza e sulla resilienza delle elezioni e la relazione sulle migliori pratiche in materia di gestione delle crisi informatiche sono alcuni esempi del contributo dell'ENISA alla cibersicurezza.

Il **Centro europeo di competenza per la cibersicurezza** costituisce, insieme alla rete dei centri nazionali di coordinamento, il nuovo quadro europeo per il sostegno all'innovazione e alla politica industriale in materia di cibersicurezza. Una volta completata la loro istituzione, il Centro e la rete prenderanno decisioni strategiche di investimento e metteranno in comune le risorse per migliorare e rafforzare le capacità in materia di cibersicurezza a livello tecnologico e industriale. Il Centro rivestirà dunque un ruolo chiave nel raggiungimento degli obiettivi di cibersicurezza dei programmi Europa digitale e Orizzonte Europa.

Dal 2022 **Europol** ha un mandato rafforzato per sostenere meglio gli Stati membri dell'UE nella lotta contro il terrorismo, la criminalità organizzata e le forme gravi di criminalità. Europol è ora in grado di sostenere gli Stati membri nell'utilizzo delle tecnologie emergenti e nello sviluppo di soluzioni tecnologiche comuni. Inoltre può ora ricevere dati direttamente da parti private (contribuendo ad esempio a contrastare la diffusione online di materiale pedopornografico). Inoltre il direttore esecutivo di Europol può ora proporre un'indagine nazionale se un reato in un solo Stato membro incide su un interesse comune oggetto di una politica dell'Unione. Il mandato rafforza inoltre il quadro per la protezione dei dati di Europol

e la supervisione del Garante europeo della protezione dei dati. Il lavoro costante di Europol ha permesso di portare a compimento numerose operazioni, come ad esempio il caso Encrochat, che finora ha portato a oltre 6 500 arresti in tutto il mondo. Il mandato rafforza inoltre il quadro per la protezione dei dati di Europol e la supervisione del Garante europeo della protezione dei dati.

A ottobre del 2023 è entrata in vigore una modifica del regolamento **Eurojust**, che migliora la capacità dell'Agenzia di individuare i collegamenti tra le indagini in materia di terrorismo e le azioni penali, di istituire un sistema di gestione dei fascicoli moderno, di fornire un canale di comunicazione digitale sicuro tra gli Stati membri ed Eurojust e di agevolare la cooperazione con i paesi terzi. La modifica inoltre garantisce che Eurojust disponga di poteri per la preservazione, l'analisi e la conservazione delle prove relative ai crimini internazionali fondamentali.

Sin dall'inizio delle attività operative nel giugno 2021, la **Procura europea** si è dimostrata indispensabile per indagare e perseguire gli illeciti penali che ledono gli interessi finanziari dell'Unione, nel caso di reati ai danni del bilancio dell'Unione. Al 31 dicembre 2023 l'EPPO aveva 1 927 indagini attive, con un danno stimato ad oltre 19,2 miliardi di EUR. L'EPPO ha iniziato a chiamare in causa dinanzi ai giudici nazionali un maggior numero di presunti autori di frodi a danno dell'UE; nel 2023 sono state presentate 139 richieste di rinvio a giudizio.

Anche **Frontex** ha svolto un ruolo attivo in materia di sicurezza nello svolgimento dei propri compiti attinenti alle frontiere, con riferimento in particolare al traffico di migranti, alla sicurezza marittima e alla tratta di esseri umani. A gennaio del 2024 Frontex ed Europol hanno firmato un accordo che delinea la modalità con cui le due agenzie possono migliorare il coordinamento delle rispettive attività per renderle complementari e individuare azioni prioritarie concrete da realizzare nel breve e lungo periodo. In pratica Frontex ha il compito di fornire intelligence sulla base delle proprie attività di sorveglianza e monitoraggio delle frontiere. Viceversa Europol deve garantire un'azione di contrasto della criminalità organizzata transfrontaliera e del terrorismo all'interno dell'UE. Inoltre Frontex, l'**Agenzia europea per la sicurezza marittima** e l'**Agenzia europea di controllo della pesca** hanno rafforzato la loro cooperazione con il rinnovo dell'accordo di lavoro tripartito sulle funzioni di guardia costiera nel 2021, contribuendo a migliorare la sicurezza in mare.

VIII PROSPETTIVE FUTURE

Per affrontare le sfide in materia di sicurezza l'UE è oggi più attrezzata di quanto non fosse all'inizio dell'attuale mandato della Commissione, grazie all'ampia gamma di misure legislative e operative adottate negli ultimi quattro anni. Tuttavia, data la costante evoluzione del panorama delle minacce, è necessario cogliere tutte le opportunità per affrontare le potenziali vulnerabilità. **La strategia attuale è stata adottata con un orizzonte temporale che si estende fino al 2025. Dopo tale data occorrerà proseguire il lavoro iniziato, mantenendo una determinazione e una vigilanza costanti.**

Il concetto di sicurezza, tradizionalmente incentrato sugli affari militari e interni, deve stare al passo con l'evoluzione delle minacce. È necessario tenere conto dei rischi e delle vulnerabilità, ad esempio sul piano della sicurezza economica, delle interruzioni nelle forniture e della preparazione alle crisi, prendendo in considerazione praticamente ogni settore della nostra società, dalla sanità alle questioni ambientali/climatiche fino all'energia e ai trasporti. La dimensione digitale è ora imprescindibile in tutti gli aspetti della sicurezza e la separazione tra minacce online e minacce offline è progressivamente superata dalle nuove

realtà, in un contesto nel quale la maggior parte delle minacce contiene un elemento informatico ed è di carattere ibrido. La situazione attuale ha inoltre dimostrato più che mai i legami intrinseci tra le dimensioni interna ed esterna della sicurezza. **Sono pertanto necessari sforzi costanti per garantire che gli aspetti relativi alla sicurezza siano integrati in tutte le politiche** e in tutti i processi decisionali dell'UE.

La strategia europea per la sicurezza economica del 20 giugno 2023 integra l'"approccio esteso a tutta la società" proposto nella strategia dell'UE per l'Unione della sicurezza, aggiungendo una componente strategica incentrata sulla difesa degli interessi dell'UE, degli Stati membri e dei cittadini dalle minacce alla nostra economia o l'impiego di mezzi economici. Essa definisce un quadro per conseguire la **sicurezza economica** attraverso la promozione della base economica e della competitività dell'UE, la protezione dai rischi e la realizzazione di partenariati con la più ampia gamma possibile di paesi al fine di affrontare preoccupazioni e interessi condivisi; ciò costituirà un **elemento essenziale nelle future considerazioni sulla sicurezza dell'UE**.

La nuova politica di ciberdifesa dell'UE è solo uno dei settori che dimostrano la necessità di **migliorare il coordinamento tra le comunità civili e l'ecosistema militare/di difesa**, e i collegamenti tra questi due ambiti sono probabilmente destinati ad aumentare in futuro.

I criminali adattano e diffondono rapidamente le nuove tecnologie nelle loro attività. Un **gruppo ad alto livello sull'accesso ai dati per un'efficace azione di contrasto**, copresieduto dalla Commissione e dalla presidenza del Consiglio, ha esaminato le sfide che le autorità di contrasto si trovano ad affrontare, in particolare l'accesso ai dati. Nelle future riflessioni sulla sicurezza sarà necessario **valutare come l'attività di contrasto possa avvalersi delle tecnologie digitali**, garantendo nel contempo il pieno rispetto dei diritti fondamentali per quanto riguarda l'accesso ai dati in settori quali l'infrastruttura di comunicazione quantistica, l'intelligenza artificiale e le tecnologie avanzate di sorveglianza.

Le future politiche di sicurezza dovranno continuare a cercare risposte efficaci a fronte dei rischi emergenti. A tal fine sarà necessario ripensare il modo in cui le istituzioni e gli organismi dell'UE nonché gli Stati membri dovrebbero rispondere alle sfide e garantire che all'occorrenza l'UE sia in grado di reagire rapidamente. **Occorre evitare compartimentazioni e meccanismi di risposta che duplichino la valutazione dei rischi o complichino la risposta alle crisi**.

Inoltre poiché l'UE dimostra continuamente di sapersi adattare all'evoluzione dei rischi, è opportuno evitare che emergano nuove vulnerabilità per effetto di un'attuazione non omogenea degli strumenti già adottati. **È indispensabile che la legislazione sia attuata e applicata in maniera efficace a livello nazionale**.

La capacità dell'UE è stata rafforzata dal crescente ruolo svolto dalle agenzie dell'UE nel settore della sicurezza ma **può essere ottimizzata attraverso un ulteriore rafforzamento del coordinamento e della complementarità tra le agenzie**. Si potrebbe prendere in considerazione la possibilità di approfondire la cooperazione non soltanto tra le agenzie che per tradizione si occupano di questioni di sicurezza, quali Europol, Eurojust e l'ENISA, nonché Frontex e la Procura europea, ma anche tra le agenzie settoriali, tra cui la nuova Agenzia dell'Unione europea sulle droghe, l'Autorità per la lotta al riciclaggio, l'Agenzia dell'Unione europea per la sicurezza aerea, l'Agenzia europea per la sicurezza marittima e l'Agenzia europea di controllo della pesca.

La strategia per l'Unione della sicurezza 2020-2025 ha consolidato il pacchetto di strumenti dell'UE sulla sicurezza e offre ora una solida base per la protezione futura dei cittadini europei. In un'ottica futura le azioni intraprese in relazione a tutte le componenti dell'Unione della sicurezza rimarranno essenziali per garantire che l'UE sia in grado di adattarsi, anche di fronte a minacce eccezionali e impreviste.