Consiglio
dell'Unione europea

Bruxelles, 25 giugno 2021
(OR. en)

10212/21

JAI 786	**DROIPEN 115**
COSI 130	**COPEN 295**
ENFOPOL 249	**FREMP 194**
ENFOCUSTOM 101	**JAIEX 82**
IXIM 133	**CFSP/PESC 646**
CT 89	**COPS 251**
CRIMORG 65	**HYBRID 37**
FRONT 264	**DISINFO 18**
ASIM 45	**TELECOM 276**
VISA 146	**DIGIT 77**
CYBER 187	**COMPET 513**
DATAPROTECT 178	**RECH 324**
CATS 43	

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	23 giugno 2021
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2021) 440 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO sulla seconda 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(2021) 440 final.

All.: COM(2021) 440 final

COMMISSIONE
EUROPEA

Bruxelles, 23.6.2021
COM(2021) 440 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

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

I. INTRODUZIONE

Lo scorso luglio la Commissione ha adottato una strategia dell'UE per l'Unione della sicurezza 2020-2025[1], per concentrare l'azione sui settori prioritari in cui l'UE può apportare un valore aggiunto agli interventi nazionali. Pur basandosi sull'agenda europea sulla sicurezza 2015-2020, la strategia ha fornito un nuovo orientamento e un approccio coordinato ai diversi filoni della politica di sicurezza, per garantire che l'UE sia in grado di rispondere alle minacce in rapida evoluzione. La strategia mira a far sì che l'UE svolga appieno il proprio ruolo nel garantire la sicurezza dei cittadini e i loro diritti fondamentali, facendo fronte ai rischi attuali e adattandosi alle nuove sfide, tenendo fede ai valori che definiscono lo stile di vita europeo.

A tale contesto già di per sé mutevole e dinamico si è aggiunta la pandemia di COVID-19 che creato nuove opportunità per la criminalità online, stimolando la cibercriminalità e aprendo la strada a un aumento della contraffazione e della distribuzione di merci non a norma, a reati organizzati contro il patrimonio e a vari tipi di frodi[2], che in alcuni casi hanno compromesso direttamente i sistemi sanitari e la prestazione di servizi sanitari. Alcune attività criminali ritorneranno alla situazione pre-pandemia, mentre altre risulteranno radicalmente modificate dalla pandemia[3].

La strategia stabiliva le azioni da intraprendere nell'arco di un periodo di cinque anni. Dopo un anno è già stato varato un numero significativo di iniziative[4]. La Commissione ha adottato un programma di lotta al terrorismo dell'UE e iniziative per contrastare la criminalità organizzata, la tratta di esseri umani, le droghe, gli abusi sessuali sui minori e il traffico di armi da fuoco, oltre a una nuova strategia dell'UE per la cibersicurezza. La Commissione ha proposto nuovi atti legislativi importanti per il rafforzamento di Europol, la protezione dell'infrastruttura fisica e digitale e il trattamento di materiale pedopornografico. Il Parlamento europeo e il Consiglio hanno portato avanti questo programma e l'hanno completato per quanto riguarda fascicoli fondamentali quali, in particolare, i contenuti terroristici online e la lotta agli abusi sessuali su minori online. Il lavoro sulla legislazione delineato nella strategia dovrebbe procedere rapidamente, pur mantenendo un livello elevato di ambizione.

A giugno la Commissione ha adottato una nuova "Strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente"[5] con misure efficaci in materia di sicurezza, cooperazione di polizia e giudiziaria per il funzionamento dello spazio di libertà, sicurezza e giustizia, affinché l'UE rimanga forte nei confronti delle minacce alla sicurezza, anche senza i controlli alle frontiere interne. Durante il periodo di riferimento, i colegislatori sono giunti a un accordo sui fondi che sostengono molte delle azioni a titolo dell'Unione della sicurezza, in particolare il Fondo sicurezza interna rafforzato (ISF) e lo strumento per la gestione delle frontiere e i visti (BMVI) nel quadro del Fondo per la gestione integrata delle frontiere (IBMF).

---

1 Comunicazione della Commissione sulla strategia dell'UE per l'Unione della sicurezza (COM(2020) 605).

2 Anche concernenti farmaci salvavita, dispositivi medici e vaccini.

3 Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità nell'UE (SOCTA), relazione 2021, Europol.

4 Cfr. l'allegato II - Tabella di marcia per l'attuazione.

5 COM(2021) 277.

Il successo della strategia dell'UE per l'Unione della sicurezza dipenderà dalla qualità della sua attuazione[6], che richiede il pieno impegno delle autorità nazionali e la costante cooperazione tra tutti gli attori interessati alla sicurezza interna ed esterna dell'Europa, comprese le agenzie dell'UE. L'approccio perseguito è inclusivo ed esteso a tutta la società, grazie alla cooperazione rafforzata tra i portatori di interessi in materia di sicurezza.

Questa seconda relazione sui progressi compiuti nell'Unione della sicurezza, concernente il periodo a partire dalla pubblicazione della prima relazione[7], il 9 dicembre 2020, illustra i progressi compiuti in relazione a tutti e quattro i pilastri della strategia: creare un ambiente della sicurezza adeguato alle esigenze del futuro, affrontare le minacce in evoluzione, proteggere l'Europa dal terrorismo e dalla criminalità organizzata e garantire un ecosistema europeo forte in materia di sicurezza. Il documento indica le modalità di svolgimento del lavoro, compreso il contributo specifico delle agenzie dell'UE.

II. Un ambiente della sicurezza adeguato alle esigenze del futuro

1. Protezione e resilienza delle infrastrutture critiche

La protezione e la resilienza delle infrastrutture critiche, sia fisiche che digitali, sono particolarmente importanti per il funzionamento delle società moderne e lo stile di vita europeo e questo è più vero che mai in un momento di emergenza sanitaria pubblica. Le minacce, gli incidenti e gli attacchi e infrastrutture critiche possono avere conseguenze devastanti.

In tempi di pandemia la resilienza è più essenziale che mai

In un momento in cui l'infrastruttura sanitaria è già sotto pressione, gli incidenti informatici mirati a ospedali, organismi medici e servizi sanitari generali possono avere conseguenze particolarmente drammatiche.

L'Irlanda è stata colpita recentemente da una serie di gravi attacchi informatici diretti al suo sistema sanitario, nei quali gli hacker hanno preso di mira il ministero della Salute e l'Health Service Executive.

Le banche dati nazionali del sistema di allarme rapido e di reazione (SARR)[8] che sostengono la risposta del settore sanitario sono state oggetto di tentativi di intrusione e attacchi ransomware[9].

L'attacco informatico all'Agenzia europea per i medicinali ha evidenziato che i documenti acquisiti illegalmente relativi a farmaci e vaccini contro la COVID-19 possono avere effetti drammatici una volta divulgati su Internet.

Al di fuori del settore sanitario, ma in un altro ambito che comunque tocca direttamente le

[6] L'allegato I fornisce una panoramica dello stato di attuazione della legislazione in materia di sicurezza.

[7] Prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza (COM(2020) 797).

[8] Il SARR è un sistema di allarme rapido per la notifica di allarmi, a livello dell'UE, concernenti gravi minacce per la salute a carattere transfrontaliero, istituito con la decisione 1082/2013/UE, https://ec.europa.eu/health/security/surveillance_early-warning_it.

[9] Il sistema di sicurezza dei dati del SARR gestito dal Centro europeo per la prevenzione e il controllo delle malattie (ECDC) non è stato colpito, ma sarà rafforzato.

vite quotidiane dei cittadini, la prova di quanto sia cruciale proteggere le infrastrutture fisiche critiche e il loro collegamento con la cibersicurezza è rappresentata dall'attacco ransomware al Colonial Pipeline negli USA[10].

La portata dei potenziali rischi dimostra l'urgente necessità di accelerare la preparazione a livello nazionale e dell'UE, sviluppando solide capacità per prevenire, individuare e attenuare simili minacce e gestire le crisi offline e online.
La legislazione dell'UE in questo ambito, e in particolare la direttiva sulla sicurezza delle reti e dei sistemi informativi[11] (direttiva NIS) e la direttiva sulle infrastrutture critiche europee (direttiva ECI)[12], ha fornito una valida base per reagire ai recenti incidenti. Nel caso dell'attacco ransomware al servizio sanitario irlandese, gli esperti nazionali di cibersicurezza si sono avvalsi dei forum esistenti[13] istituiti a norma della direttiva NIS per scambiare informazioni a livello sia tecnico che politico, permettendo alle autorità irlandesi di ricevere sostegno e agli altri Stati membri di intensificare la preparazione nei confronti di tali attacchi.

Nel contempo, la maggiore incidenza e intensità delle minacce dimostra che l'attuale quadro legislativo non è adeguato allo scopo. Dalla valutazione[14] dell'attuazione della direttiva NIS è emerso che il suo ambito di applicazione non rispecchia il livello attuale di digitalizzazione e interconnessione, né l'interdipendenza di settori economici e sociali fondamentali. Alcune entità pubbliche e private appartenenti a settori essenziali inoltre non sono subordinate alla direttiva o non sono tenute a rispettare obblighi in fatto di cibersicurezza non armonizzata e di segnalazione di incidenti. Dalla valutazione[15] dell'attuazione della direttiva ECI è emerso che l'attenzione viene concentrata sulla protezione dei beni solo in un numero molto limitato di settori, al contrario di quanto accade per la resilienza degli operatori. Entrambe le valutazioni hanno evidenziato approcci divergenti e carenze a livello nazionale.

Nel dicembre 2020 la Commissione ha pertanto proposto due importanti atti legislativi: una direttiva sulla **resilienza dei soggetti critici** (CER)[16] e una direttiva rivista relativa a misure per un **livello comune elevato di cibersicurezza nell'Unione** (direttiva NIS rivista)[17]. Entrambe le direttive hanno un ambito di applicazione ampio, che copre gli stessi dieci settori essenziali: trasporti, energia, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. In questi settori la direttiva CER propone misure per istituire un quadro di resilienza fisica con norme minime che consentano la flessibilità necessaria per rispecchiare le specificità nazionali. La proposta di direttiva NIS rivista è intesa a istituire una normativa orizzontale per i requisiti

[10] Il Colonial Pipeline, un sistema di oleodotti di importanza cruciale che trasporta il 45 % del petrolio consumato sulla costa orientale degli USA, nel maggio 2021 è stato vittima di un attacco informatico ransomware che ha bloccato per giorni le forniture di petrolio.
[11] Direttiva 2016/1148, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[12] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.
[13] Rete CSIRT e gruppo di cooperazione.
[14] SWD(2020) 345, parte II.
[15] SWD(2019) 310.
[16] Proposta di direttiva sulla resilienza dei soggetti critici (COM(2020) 829).
[17] Proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020) 823).

di cibersicurezza nel mercato interno, rafforzando la concentrazione sulla sicurezza della catena di approvvigionamento. La direttiva introdurrebbe nuovi strumenti per la gestione e la divulgazione coordinata delle vulnerabilità, nonché per una maggiore efficacia nella risposta agli incidenti e nella gestione delle crisi, razionalizzando anche gli obblighi di segnalazione degli incidenti con disposizioni più precise in merito alla procedura, al contenuto e alla tempistica della segnalazione.

Alla luce della costante evoluzione delle minacce alle nostre infrastrutture critiche, la Commissione invita i colegislatori a dimostrare un livello elevato di ambizione e garantire l'agevole adozione di queste due proposte, preservandone la coerenza e la complementarità. I progressi verso l'adozione di queste proposte devono garantire anche la coerenza con la proposta presentata dalla Commissione nel 2020 sulla resilienza operativa digitale per il settore finanziario[18], intesa a rafforzare la capacità dell'Europa di consolidare la propria autonomia strategica nei servizi finanziari e, di conseguenza, la sua capacità di disciplinare il sistema finanziario e vigilare su di esso nell'interesse della stabilità finanziaria.

Iniziative nel settore dell'energia

Per concentrarsi su vulnerabilità più specifiche sono necessarie iniziative settoriali. A questo proposito occorre evidenziare importanti sviluppi nel settore dell'energia. Nell'ambito del monitoraggio dell'impatto della crisi della COVID-19 nel settore dell'energia, nel maggio 2021 è stato completato uno studio che individua le catene di approvvigionamento tecnologico che sono critiche per la sicurezza energetica e la transizione energetica pulita e propone misure per migliorare la resilienza in scenari di pandemia o caratterizzati da altre minacce. Alle sue conclusioni attingeranno altri filoni di lavoro pertinenti, compreso il lavoro del gruppo di cooperazione NIS sul settore dell'energia. La rete tematica per la protezione delle infrastrutture energetiche critiche ha continuato il suo lavoro sulle sfide per la protezione delle infrastrutture energetiche critiche, affrontando argomenti quali la valutazione del rischio, lo scambio di informazioni e il finanziamento di misure di sicurezza[19].

Nel gennaio 2021 la Commissione ha varato la procedura formale per istituire un codice di rete dedicato sulla **cibersicurezza per i flussi transfrontalieri di energia elettrica,** con l'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (ACER). Questo codice di rete conterrà requisiti minimi comuni in materia di pianificazione, monitoraggio, segnalazione e gestione delle crisi, in linea con il quadro orizzontale stabilito a norma della direttiva NIS. Per quanto riguarda la **preparazione ai rischi nel settore dell'energia elettrica**, nell'aprile 2021 gli Stati membri hanno avviato una consultazione sulla coerenza in merito ai rispettivi progetti di piani di preparazione ai rischi. Questi piani comprendono misure volte a prevenire e attenuare crisi dell'energia elettrica e si basano sugli scenari nazionali di crisi dell'energia elettrica individuati da ciascuno Stato membro, nonché sugli scenari regionali di crisi dell'energia elettrica individuati dalla rete europea dei gestori dei sistemi di trasmissione dell'energia elettrica nel settembre 2020, che comprendono gli attacchi informatici, nonché le pandemie e gli eventi meteorologici estremi.

[18] Proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 (COM(2020) 595).

[19] La discussione con gli operatori è stata allargata agli Stati membri, con un ciclo tecnico di discussioni bilaterali che si è svolto tra marzo e giugno 2021.

2. *Cibersicurezza*

La trasformazione digitale della società, intensificata dalla crisi dovuta alla COVID-19, sta creando nuovi problemi che richiedono risposte innovative. Durante questi ultimi mesi, il numero di attacchi informatici ha continuato ad aumentare, con attacchi sempre più sofisticati da un'ampia gamma di fonti, all'interno e all'esterno dell'UE. Gravi violazioni di dati e recenti attacchi informatici come la massiccia operazione cibernetica contro SolarWinds[20] dimostrano la portata dei rischi per la società in assenza di un cambio di passo nella cibersicurezza. L'UE deve lavorare per proteggere i governi, i cittadini e le imprese dalle minacce informatiche, garantendo nel contempo una rete Internet aperta e globale. Sono stati fatti passi importanti per tenere fede alla visione secondo cui ogni cittadino dell'UE dovrebbe essere in grado di vivere la propria vita digitale in sicurezza, utilizzando la rete Internet aperta e globale.

Nel dicembre 2020 la Commissione e l'Alto rappresentante hanno presentato una nuova strategia dell'UE per la cibersicurezza[21]. In quanto componente essenziale della strategia "Plasmare il futuro digitale dell'Europa" e del piano per la ripresa dell'Europa, nonché della strategia per la sicurezza, la proposta mira a rafforzare la resilienza collettiva dell'Europa nei confronti delle minacce informatiche e contribuirà a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. Il ciberspazio dovrebbe restare globale, aperto, stabile e sicuro. La strategia si fonda su tre pilastri principali: 1) resilienza, sovranità tecnologica e leadership; 2) sviluppo delle capacità operative di prevenzione, dissuasione e risposta; 3) promozione di un ciberspazio globale e aperto grazie a una maggiore cooperazione. La strategia affronta per la prima volta la cibersicurezza delle istituzioni, delle agenzie e degli organismi dell'UE. Il Consiglio ha adottato conclusioni sulla strategia[22], appoggiando le sue principali iniziative strategiche per l'attuazione. La strategia è in corso di attuazione e una panoramica dettagliata della situazione attuale è fornita in una specifica relazione di attuazione[23].

Un'iniziativa fondamentale annunciata negli orientamenti politici della Commissione e a cui ha dato seguito la strategia per la cibersicurezza è l'istituzione di una **unità congiunta per il ciberspazio**. Dopo aver consultato gli Stati membri, la Commissione ha adottato, unitamente alla presente relazione, una raccomandazione per definire meglio la procedura, le tappe e un calendario per la sua istituzione[24]. L'unità congiunta per il ciberspazio riunirà tutte le comunità della cibersicurezza, ossia la comunità civile, le autorità di contrasto, la diplomazia e la difesa. L'unità congiunta per il ciberspazio utilizzerà, fornendo un valore aggiunto, le strutture, risorse e capacità esistenti, come piattaforma per assicurare una rapida cooperazione operativa e tecnica tra soggetti dell'UE e autorità degli Stati membri e riunirà tutte le comunità della cibersicurezza, ossia la comunità civile, le autorità di contrasto, la diplomazia e la difesa. L'unità congiunta per il ciberspazio sarà istituita mediante un processo in quattro fasi, che comprenderà l'individuazione delle capacità operative disponibili nell'UE, la

[20] SolarWinds, un'importante azienda informatica statunitense, è stata oggetto di un attacco informatico allargato ai suoi clienti, che è passato inosservato per mesi, consentendo agli hacker di accedere a migliaia di società e uffici governativi che utilizzavano i suoi prodotti.

[21] Comunicazione congiunta al Parlamento europeo e al Consiglio - "La strategia dell'UE in materia di cibersicurezza per il decennio digitale" (JOIN(2020) 18).

[22] Cibersicurezza: il Consiglio adotta conclusioni sulla strategia dell'UE in materia di cibersicurezza - Consilium (europa.eu).

[23] JOIN(2021) 14.

[24] C(2021) 4520.

preparazione dei piani di risposta a incidenti e crisi a livello nazionale e dell'UE e l'espansione delle attività per instaurare una collaborazione con soggetti privati. L'unità congiunta per il ciberspazio dovrebbe diventare completamente operativa entro il 30 giugno 2023.

Con l'obiettivo di migliorare ulteriormente le **capacità di rilevamento** e sfruttare strumenti basati sull'intelligenza artificiale per proteggere l'UE da attacchi informatici, gli Stati membri stanno aumentando gli investimenti in **centri operativi di sicurezza** (SOC), grazie ai fondi a titolo del dispositivo per la ripresa e la resilienza. La Commissione integrerà gli sforzi degli Stati membri assegnando fondi dal programma Europa digitale.

Cibersicurezza delle reti 5G
Nell'ambito della strategia per la cibersicurezza, la Commissione ha individuato tre obiettivi principali per il lavoro futuro sulla cibersicurezza delle reti 5G, in considerazione del loro ruolo centrale per conseguire la trasformazione digitale dell'economia e della società dell'UE: i) garantire un'ulteriore convergenza negli approcci di attenuazione dei rischi in tutta l'UE, ii) sostenere lo scambio continuo di conoscenze e lo sviluppo di capacità e iii) promuovere la resilienza della catena di approvvigionamento e altri obiettivi strategici di sicurezza dell'UE. Questi obiettivi sono basati su una relazione in materia di cibersicurezza del 5G[25] che ha esaminato l'intenso lavoro congiunto degli Stati membri e della Commissione, con il sostegno dell'Agenzia europea per la cibersicurezza (ENISA), confermando che sono stati compiuti notevoli progressi da quando è stato concordato il pacchetto di strumenti dell'UE contenente misure di attenuazione dei rischi[26]. Maggiori dettagli sulla situazione attuale dell'attuazione del pacchetto di strumenti dell'UE sono forniti nella relazione di attuazione della strategia per la cibersicurezza[27].

Un ecosistema della cibersicurezza
Al fine di contribuire a creare un ecosistema industriale e di ricerca sulla cibersicurezza interconnesso a livello europeo, nel maggio 2021 è stato adottato il regolamento che istituisce il **Centro di competenza per la cibersicurezza** e la **rete dei centri nazionali di coordinamento**[28]. Il Centro punta a rafforzare le capacità europee in materia di cibersicurezza, promuovere l'eccellenza nella ricerca e consolidare la competitività dell'industria dell'Unione in questo ambito[29]. La Commissione sta già lavorando con le autorità della Romania per preparare l'insediamento del Centro a Bucarest. Nell'ambito del piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio[30], la Commissione cercherà di rafforzare il reciproco arricchimento tra le attività del Centro, del Fondo europeo per la difesa e del programma spaziale dell'UE in materia di cibersicurezza e ciberdifesa.

---

25 SWD(2020) 357.
26 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
27 JOIN(2021) 14.
28 Regolamento (UE) 2021/887.
29 In particolare decidendo e gestendo i fondi per la cibersicurezza provenienti dai programmi Europa digitale e Orizzonte Europa, nonché dagli Stati membri.
30 COM(2021) 70 del 22.2.2021.

Il regolamento sulla cibersicurezza[31] ha introdotto un **quadro di certificazione della cibersicurezza per i prodotti, i servizi e i processi TIC**. Le società operanti nell'UE beneficeranno della possibilità di certificare i propri prodotti, processi e servizi TIC solo una volta per ottenere certificati riconosciuti in tutta l'Unione europea. La Commissione ha già chiesto all'ENISA di preparare tre sistemi di certificazione della cibersicurezza: il sistema di criteri comuni europei, il sistema europeo per i servizi informatici in cloud e il sistema europeo per le reti 5G[32].

Dimensione internazionale
La strategia per la cibersicurezza conteneva ulteriori proposte per prevenire, scoraggiare e contrastare attività informatiche dolose, promuovendo un comportamento responsabile degli Stati da parte dei partner internazionali dell'UE nel ciberspazio[33]; rafforzando il quadro relativo a una risposta diplomatica comune dell'UE alle attività informatiche dolose (il pacchetto di strumenti della diplomazia informatica)[34]; intensificando il coordinamento e la cooperazione dell'UE in materia di ciberdifesa; e potenziando le capacità di ciberdifesa mediante il quadro strategico dell'UE in materia di ciberdifesa[35]. L'Alto rappresentante sta preparando un riesame di questi quadri in consultazione con la Commissione e in linea con le ambizioni della bussola strategica. A maggio il Servizio europeo per l'azione esterna (SEAE) ha organizzato un dibattito basato su scenari con gli Stati membri e partner internazionali, al fine di migliorare la comprensione reciproca delle opzioni diplomatiche disponibili per prevenire, scoraggiare e contrastare attività informatiche dolose e farvi fronte, nonché di individuare opportunità per l'ulteriore rafforzamento della cooperazione internazionale.

Oltre che in Europa, interventi di sostegno per la cibersicurezza sono previsti nel vicinato orientale e in Africa, Asia, America Latina e nei Caraibi attraverso progetti di cooperazione definiti, intesi a mobilitare la competenza europea per sviluppare le capacità informatiche e aumentare la sicurezza e la resilienza di infrastrutture critiche e reti[36]. Attraverso il patto sulla dimensione civile della PSDC[37], anche la cibersicurezza è stata aggiunta agli ambiti prioritari per le missioni civili della PSDC.

Al fine di impedire che la tecnologia di sorveglianza informatica sia utilizzata in violazione dei diritti umani al di fuori dell'UE, il nuovo regolamento sulle esportazioni[38] sostiene una modernizzazione generale delle norme dell'UE sull'esportazione di prodotti a duplice uso[39]. Il nuovo regolamento fornisce una base che consente all'UE di effettuare controlli efficaci

[31] Regolamento (UE) 2019/881, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.
[32] Lo stato dei sistemi sarà descritto nel programma di lavoro progressivo dell'Unione.
[33] Segnatamente portando avanti la proposta di un programma d'azione per istituire un'infrastruttura permanente per l'azione concreta intesa a promuovere un comportamento responsabile degli Stati nel ciberspazio.
[34] Decisioni (PESC) 2020/1127, 2020/1537 e 2020/651 del Consiglio, nell'ambito del documento 9916/17.
[35] Decisione 14413/18 del Consiglio.
[36] Tra gli esempi figurano i progetti "Cyber4Dev", "EU4Digital" e "EU CyberNet".
[37] Doc. Rif. 14305/18 del 19 novembre 2018.
[38] Regolamento che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione), del 19 maggio 2021.
[39] Si tratta di beni, software e tecnologie che possono essere impiegati per applicazioni sia civili che militari.

sulle esportazioni di tecnologie di sorveglianza informatica e affrontare i rischi per la sicurezza associati al commercio mondiale di tecnologie emergenti.

3. Protezione degli spazi pubblici

Negli ultimi anni gli spazi pubblici nell'UE sono stati lo scenario di attacchi terroristici senza precedenti nei confronti del pubblico. Tra i rischi emergenti per gli spazi pubblici figura la crescente diffusione di **droni**. I sistemi aerei senza equipaggio possono essere utilizzati da malintenzionati per svolgere attività di sorveglianza, disturbare il funzionamento di infrastrutture critiche o attaccare obiettivi di alto valore. In aprile la Commissione ha adottato un **quadro europeo per la gestione del traffico senza equipaggio** (U-Space)[40], per consentire alle autorità di distinguere più agevolmente tra droni cooperativi e non cooperativi, potenzialmente malintenzionati. La Commissione sostiene inoltre la preparazione di materiali di orientamento dell'Agenzia dell'Unione europea per la sicurezza aerea, sta finanziando progetti e studi innovativi per il contrasto all'uso dei droni e creando collegamenti tra diversi settori interessati (attività di contrasto, aviazione, infrastrutture critiche, carceri, dogane/frontiere, protezione personale, organizzatori di eventi di massa) e altri portatori di interessi. È stato varato un programma europeo inteso ad agevolare un approccio più coordinato alla sperimentazione di diverse tecnologie di contrasto ai droni.

È in corso il lavoro di preparazione di orientamenti per individuare e attenuare le vulnerabilità degli spazi pubblici e garantire la sicurezza fin dalla progettazione. È in corso un programma da 20 milioni di EUR a titolo del Fondo sicurezza interna-Polizia per migliorare la **protezione nei confronti di minacce terroristiche nei luoghi di culto e altri spazi pubblici**, con un'attenzione particolare per i grandi eventi sportivi. A marzo la Commissione ha tenuto una conferenza sui nuovi progetti varati nel 2021. La Commissione inoltre sostiene le autorità nazionali, regionali e urbane e gli operatori di spazi pubblici per la condivisione di buone pratiche, la creazione di reti e la cooperazione a livello dell'UE[41], mediante l'agenda urbana per l'UE e attività nell'ambito del Fondo europeo di sviluppo regionale[42].

Il piano d'azione sulla **sicurezza ferroviaria**, adottato nel 2018[43] e recante una serie azioni concrete per migliorare la sicurezza del trasporto ferroviario di passeggeri, è ormai completamente attuato. La piattaforma di sicurezza per i passeggeri del trasporto ferroviario dell'UE[44] ha adottato una serie di documenti di migliori pratiche in materia di valutazione del rischio, minacce interne e tecnologie di rilevamento, promuovendo una maggiore cooperazione tra Stati membri e risultati migliori nel settore della sicurezza ferroviaria.

---

[40] Regolamenti di esecuzione C(2021) 2671, C(2021) 2672 e C(2021) 2673 della Commissione.

[41] Nell'ambito dell'agenda urbana per l'UE, ad esempio, la Commissione ha fornito indicazioni e sostegno in termini di competenze tecniche e tematiche al partenariato per la sicurezza negli spazi pubblici al fine di contribuire all'attuazione del suo piano d'azione. I programmi di cooperazione transfrontaliera Interreg cofinanziati dal Fondo europeo di sviluppo regionale aiutano gli operatori della sicurezza in regioni frontaliere limitrofe a cooperare con maggiore efficacia.

[42] https://ec.europa.eu/jrc/en/protection-public-spaces-from-terrorist-attacks/newsletter-protection-public-spaces.

[43] COM(2018) 470.

[44] La piattaforma di sicurezza per i passeggeri del trasporto ferroviario dell'UE è costituita dalle autorità degli Stati membri competenti in materia di sicurezza ferroviaria e da portatori di interessi. Poiché il mandato della piattaforma è scaduto a giugno 2021, l'attuazione dei risultati del piano d'azione sulla sicurezza ferroviaria sarà portata avanti da un gruppo di lavoro dedicato alla sicurezza ferroviaria nell'ambito del gruppo di esperti sulla sicurezza del trasporto terrestre (LANDSEC).

III. Affrontare le minacce in evoluzione

1. Cibercriminalità

L'impatto della pandemia sulla cibercriminalità[45]

I criminali hanno saputo rapidamente sfruttare i cambiamenti comportati dal telelavoro e dall'aumento dell'utilizzo dei servizi online, per adattare le loro attività illegali al contesto di crisi. Il numero di truffe favorite dall'informatica e connesse alla pandemia, mediante software maligni, ransomware e attacchi di phishing è aumentato durante la pandemia, prendendo di mira cittadini, imprese e il settore sanitario in particolare.

Le circostanze della pandemia hanno offerto nuove opportunità di frodi, che hanno sfruttato le carenze nelle forniture pubblicizzando finti negozi online e vendendo beni inesistenti, compresi dispositivi di protezione personale e kit per test autodiagnostici. Con lo spostamento della distribuzione dei prodotti farmaceutici dal mercato fisico a quello online, nel dark web sono state addirittura scoperte offerte fraudolente di vaccini anti-COVID.

L'aumento delle perdite economiche mondiali associate alla cibercriminalità (che dovrebbero raggiungere 5 400 miliardi di EUR all'anno entro il 2021) evidenzia la necessità di mettere a punto applicazioni e infrastrutture sicure che possano anticipare una minaccia in costante crescita e reagirvi prontamente. Il bollettino giudiziario della criminalità informatica (Cybercrime Judicial Monitor) pubblicato da Eurojust a maggio offre una panoramica degli sviluppi legislativi e della giurisprudenza dell'UE in relazione alla cibercriminalità e ai reati favoriti dall'informatica[46].

Poiché una cibersicurezza efficace è essenziale per arginare l'ondata di cibercriminalità, è fondamentale che gli Stati membri garantiscano la piena attuazione della normativa esistente. La Commissione valuta costantemente la conformità del recepimento della **direttiva relativa agli attacchi contro i sistemi di informazione**[47]. In aggiunta alle procedure di infrazione avviate in precedenza[48], la Commissione ha aperto nuove procedure di infrazione (cfr. allegato I della presente relazione) concernenti carenze nel recepimento della direttiva. Se necessario, la Commissione avvierà ulteriori procedimenti. Parallelamente, la Commissione ha sostenuto gli Stati membri nell'attuazione della direttiva con l'organizzazione di un workshop il 23 febbraio 2021 sulle migliori pratiche per la registrazione, la produzione e la pubblicazione di dati statistici per la segnalazione, il perseguimento e la condanna per reati di attacchi informatici come definiti nella direttiva. Il pieno recepimento della direttiva relativa agli attacchi contro i sistemi di informazione è fondamentale per smantellare le reti e le attività criminali come l'attuale aumento degli attacchi ransomware. L'impegno dell'UE in questo campo è stato pubblicamente sottolineato agli incontri della NATO[49] e del G7[50] che si sono tenuti in giugno, ai fini della collaborazione

[45] Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità nell'UE (SOCTA), relazione 2021, Europol.

[46] Eurojust, Cybercrime Judicial Monitor, Issue 6 – maggio 2021, consultato il 7 giugno 2021.

[47] Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.

[48] Nel 2019 sono state avviate procedure di infrazione contro Bulgaria, Italia, Portogallo e Slovenia.

[49] Comunicato del vertice NATO di Bruxelles, 14 giugno 2021.

[50] Comunicato del vertice G7, Our Shared Agenda for Global Action to Build Back Better, 13 giugno 2021.

tra paesi che condividono gli stessi principi per affrontare l'escalation della minaccia condivisa proveniente dalle reti criminali ransomware.

Lotta contro gli abusi sessuali su minori
Gli abusi sessuali sui minori sono un fenomeno che desta crescente preoccupazione con reati online e offline spesso collegati.

La pandemia di COVID-19 e gli abusi sessuali su minori

Molte relazioni forniscono prove del fatto che la pandemia abbia aggravato gli abusi, in particolare su minori che vivono con i loro aguzzini[51]. La pandemia ha registrato anche un notevole aumento di materiale visivo "autoprodotto", derivante in parte da abusi online commessi da un criminale che esercita pressioni sul minore per indurlo a produrre tale materiale[52].

In linea con la **strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori**[53] **e la strategia dell'UE sui diritti dei minori**[54]**,** la Commissione sta lavorando sulle iniziative specifiche individuate per promuovere un'azione proattiva e multipartecipativa in tutti i settori pertinenti, quali prevenzione, sostegno all'attività di contrasto e assistenza alle vittime.

In aprile il Parlamento europeo e il Consiglio hanno trovato un accordo politico provvisorio sulla proposta della Commissione per una **legislazione temporanea** intesa a garantire che i fornitori di servizi online possano continuare a svolgere le loro attività volontarie al fine di individuare e segnalare abusi sessuali su minori online, ed eliminare il materiale pedopornografico dai rispettivi sistemi, purché le loro pratiche siano legittime. Queste norme provvisorie saranno sostituite a tempo debito da una legislazione a più lungo termine, con tutele dettagliate per una lotta più efficace contro gli abusi sessuali su minori. L'iniziativa è stata oggetto di una consultazione pubblica aperta e di una valutazione d'impatto.

La Commissione sta monitorando l'attuazione della **direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile**[55]. Dopo le procedure di infrazione avviate nel 2019 contro 23 Stati membri, la Commissione sta proseguendo la sua valutazione e potrà avviare ulteriori azioni nel secondo semestre del 2021. La Commissione prevede inoltre di chiudere una serie di procedure nei prossimi mesi, poiché numerosi Stati membri hanno reso pienamente conforme alla direttiva la propria legislazione nazionale.

---

[51] Cfr. relazione Europol del 19 giugno 2020, e NetClean (14 aprile 2021). Secondo le informazioni fornite dall'US National Centre for Missing and Exploited Children, il numero di segnalazioni di abusi sessuali su minori a livello mondiale nell'aprile 2020 è quadruplicato rispetto all'aprile 2019. Cfr. anche WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, OMS, ITU, End Violence Against Children e UNESCO, aprile 2020.

[52] Cfr. le relazioni di Internet Watch Foundation, del 12 gennaio 2021; e la valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA) di Europol del 12 aprile 2021.

[53] Comunicazione della Commissione, Strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori (COM(2020) 607).

[54] COM(2021) 142.

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

Per sostenere le autorità di contrasto e promuovere il coordinamento multipartecipativo, la Commissione ha avviato i lavori per istituire una **rete per la prevenzione** costituita da operatori e ricercatori, per aumentare la cooperazione e lo scambio di migliori pratiche tra tutti gli attori pertinenti. Questo contribuisce a innalzare gli standard mondiali per la protezione dei minori contro gli abusi sessuali, promuovendo la cooperazione attraverso WePROTECT Global Alliance to End Child Sexual Exploitation Online e mediante finanziamenti dedicati.

Indagini online e dati elettronici

Affinché i cibercriminali siano assicurati alla giustizia è fondamentale garantire l'accesso a prove digitali che possono fornire indizi investigativi. Alcuni Stati membri hanno definito quadri per la **conservazione dei dati**, concernenti la conservazione e l'uso di metadati delle comunicazioni elettroniche ai fini di contrasto, ma queste misure sollevano importanti interrogativi in relazione alle potenziali interferenze con diritti fondamentali, tra cui il diritto alla riservatezza e la protezione dei dati personali. La Corte di giustizia dell'Unione europea ha fornito importanti chiarimenti e indicazioni[56]. A marzo la Corte ha emesso un'altra sentenza[57] riguardante la legislazione nazionale dell'Estonia e ha confermato la precedente giurisprudenza. Sempre a marzo il Consiglio europeo[58] ha sollecitato misure affinché sia "sfruttato meglio il potenziale dei dati e delle tecnologie digitali a vantaggio della società, dell'ambiente e dell'economia, nel rispetto dei pertinenti diritti in materia di protezione dei dati e di riservatezza nonché di altri diritti fondamentali e garantendo la conservazione dei dati necessaria affinché le autorità di contrasto e giudiziarie siano in grado di esercitare i loro legittimi poteri per combattere le forme gravi di criminalità". In risposta a questi recenti sviluppi, nella strategia dell'UE per la lotta alla criminalità organizzata[59] la Commissione ha annunciato la sua intenzione di analizzare e delineare "possibili approcci e soluzioni, in linea con le sentenze della Corte, che rispondano alle esigenze delle autorità di contrasto e giudiziarie in un modo che sia operativamente utile, tecnicamente possibile e giuridicamente valido, anche nel pieno rispetto dei diritti fondamentali". È in corso la consultazione con gli Stati membri per definire il modo di procedere.

Un altro elemento fondamentale per contrastare più efficacemente la cibercriminalità e perseguire i reati in modo più efficiente è la legislazione in materia di **accesso transfrontaliero alle prove elettroniche**. Dalla prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza, i negoziati con i colegislatori sulla proposta della Commissione[60] hanno acquisito nuovo slancio, dopo che il Parlamento europeo ha adottato la sua posizione nel dicembre 2020. Su questa base il Parlamento europeo e il Consiglio hanno avviato discussioni di trilogo. La rapida adozione di misure efficienti in linea con l'obiettivo delle proposte consentirà alle autorità di contrasto e giudiziarie di ottenere un rapido accesso alle prove elettroniche necessarie per le indagini penali.

---

[56] Nelle sentenze nella causa C-623/17, *Privacy International*, e nelle cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, del 6 ottobre 2020, la CGUE ha confermato la sua precedente giurisprudenza, secondo cui le comunicazioni elettroniche di dati sono riservate e, in linea di principio, i dati relativi al traffico e all'ubicazione non possono essere conservati in maniera generalizzata e indifferenziata. Nel contempo, ha individuato talune situazioni nelle quali la conservazione è ammissibile, sulla base di obblighi chiari e proporzionati stabiliti per legge e soggetti a rigorose garanzie sostanziali e procedurali.

[57] Sentenza nella causa C-746/18 *Prokuratuur*.

[58] Dichiarazione dei membri del Consiglio europeo, SN 18/21 del 25.3.2021.

[59] Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025 (COM(2021) 170 del 14.4.2021).

[60] COM(2018) 226 e COM(/2018) 225.

I servizi fiduciari e l'identificazione elettronica svolgono un ruolo fondamentale per contribuire a prevenire l'aumento della cibercriminalità e consentire transazioni transfrontaliere sicure in Internet. La proposta di un **quadro europeo per l'identità digitale** adottata il 3 giugno mira a fornire identità digitali affidabili per tutti i cittadini, i residenti e le imprese dell'UE. Il quadro fornirà i massimi standard di sicurezza disponibili per contrastare le minacce di frode e i furti di identità e garantire ai cittadini e ad altri titolari di tali identità il controllo completo e agevole della quantità di dati fornita per una determinata transazione. Il quadro sarà sostenuto da un'architettura tecnica comune, basata sugli standard più avanzati.

La scadenza per l'applicazione del regolamento sul rafforzamento **della sicurezza delle carte d'identità e dei titoli di soggiorno** è il 2 agosto 2021. La maggior parte degli Stati membri sta rispettando i tempi e rilascerà le carte d'identità e i titoli di soggiorno nel nuovo formato[61].

Dimensione internazionale
Considerato il carattere globale della cibercriminalità, le iniziative a livello internazionale sono essenziali per individuare approcci più efficaci.

I negoziati per il secondo protocollo aggiuntivo alla **convenzione di Budapest sulla criminalità informatica** del Consiglio d'Europa mirano a rafforzare le norme esistenti per l'accesso transfrontaliero alle prove elettroniche per le indagini penali. Nel maggio 2021 le parti della convenzione hanno completato le discussioni e ora il progetto di protocollo sarà esaminato dai comitati pertinenti in seno al Consiglio d'Europa. Sempre quest'anno è prevista la conclusione formale che consentirà la successiva firma e ratifica del protocollo. La Commissione lavorerà con il Parlamento europeo e il Consiglio per consentire agli Stati membri di sottoscrivere e ratificare il protocollo al più presto.

Il protocollo comprende anche disposizioni che agevoleranno l'accesso delle autorità ai dati di registrazione dei nomi di dominio (noti anche come "**informazioni WHOIS**") per le indagini penali. A questo proposito la Commissione partecipa anche alla definizione e all'attuazione di politiche multipartecipative per la raccolta di dati di registrazione dei nomi di dominio e l'accesso agli stessi al livello dell'ICANN (Internet Cooperation for Assigning Names and Numbers). È opportuno che questi processi siano coerenti con le pertinenti disposizioni nella proposta di direttiva NIS rivista, che comprende disposizioni intese a garantire la raccolta e la divulgazione di dati accurati di registrazione dei nomi di dominio per i legittimi richiedenti accesso, comprese le autorità di contrasto.

Un'azione importante in termini di cooperazione internazionale è il progetto Global Action on Cybercrime Extended (GLACY+), inteso a rafforzare la capacità dei paesi in tutto il mondo di applicare la legislazione in materia di cibercriminalità e prove elettroniche, sulla base della convenzione di Budapest, nonché la loro capacità di cooperare in modo efficace, nel rispetto delle norme internazionali sui diritti umani e dello Stato di diritto. Il progetto sostiene 16 paesi prioritari[62] e si occuperà anche di mettere in contatto gli operatori della giustizia

[61] Un numero limitato di Stati membri ha segnalato ritardi, legati principalmente alla pandemia, ma esistono anche motivi di ritardo sostanziali, come procedure di gara oggetto di contestazione in tribunale.

[62] A titolo di esempio, il Consiglio d'Europa è sostenuto dallo strumento europeo di vicinato per l'attuazione del progetto CyberSouth, inteso a rafforzare la legislazione e le capacità istituzionali in materia di cibercriminalità e prove elettroniche nel vicinato meridionale, nel rispetto dei diritti umani e dello Stato di diritto. Un progetto analogo - CyberEast - è attuato dal Consiglio d'Europa nella regione del partenariato orientale. Un altro progetto del Consiglio d'Europa finanziato a titolo dello strumento di assistenza preadesione opera nei Balcani occidentali e in Turchia per rafforzare ulteriormente la capacità delle autorità

penale con politici e legislatori, onde garantire un maggiore sostegno politico alla convenzione di Budapest.

2. Moderne attività di contrasto

Le nuove tecnologie offrono notevoli opportunità in materia di sicurezza. Al fine di aumentare la sicurezza e la protezione, è essenziale integrare nella politica di sicurezza l'intelligenza artificiale (IA), i megadati e il calcolo ad alte prestazioni (HPC), senza indebolire l'effettiva protezione dei diritti fondamentali.

L'**intelligenza artificiale** può offrire strumenti a sostegno delle autorità di contrasto nella lotta alla criminalità e al terrorismo, tenendo il passo con le tecnologie in rapida evoluzione usate dai criminali nelle loro attività transfrontaliere. La recente comunicazione della Commissione sulla promozione di un approccio europeo all'intelligenza artificiale (IA)[63] spiega come l'IA possa fornire un importante contributo alla strategia per l'Unione della sicurezza, in quanto strumento strategico per contrastare le attuali minacce e prevedere futuri rischi e opportunità. In aprile la Commissione ha presentato una proposta di regole armonizzate (la "legge sull'intelligenza artificiale")[64] che mira a fare dell'Europa il polo mondiale per un'IA affidabile. Una parte importante delle proposte è incentrata sui sistemi di IA ad alto rischio, che pongono rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone. A norma della legge sull'IA in linea di principio sarebbe vietato il ricorso a sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, con eccezioni rigorosamente definite. Questi tipi di sistemi ad alto rischio devono rispettare una serie di requisiti obbligatori orizzontali per un'IA affidabile, tra cui tracciabilità, trasparenza, sorveglianza umana e precisione. La legge sull'IA avrebbe un impatto significativo nell'ambito delle attività di contrasto e dei controlli alle frontiere. Il suo intento è creare un quadro equilibrato di sorveglianza durante tutto il ciclo di vita dei sistemi ad alto rischio utilizzati dalle autorità di contrasto e istituire una serie di tutele per la protezione dei diritti fondamentali.

Lo spazio europeo dei dati in materia di sicurezza per l'innovazione nell'ambito del **programma Europa digitale** mira ad aumentare la fiducia nell'uso dell'IA da parte delle autorità di contrasto, creando, rendendo accessibili e condividendo serie di dati di alta qualità per esercitare, testare e convalidare algoritmi, un presupposto essenziale per creare ecosistemi di IA di eccellenza e fiducia. L'importanza di creare spazi di dati comuni è stata riconosciuta dal Consiglio europeo in marzo.

Il **calcolo ad alte prestazioni** (HPC) è una capacità di fondamentale importanza per consentire a tecnologie chiave come l'IA e l'analisi di dati di sfruttare l'enorme potenziale dei big data. Le simulazioni di supercalcolo sono cruciali per migliorare la sicurezza di prodotti e servizi (in particolare tramite la modellazione) e per la sicurezza nazionale, la difesa e l'autonomia tecnologica. I supercomputer sono essenziali per usi che vanno dalla cibersicurezza alla simulazione nucleare e la combinazione di HPC e IA cambierà le regole del gioco nella difesa e nella sicurezza. L'inaugurazione della sede centrale dell'impresa

---

nei Balcani occidentali e in Turchia di cercare, sequestrare e confiscare proventi della cibercriminalità, impedire il riciclaggio di denaro in Internet e ottenere prove elettroniche.

[63] Comunicazione "Promuovere un approccio europeo all'intelligenza artificiale" (COM(2021) 205).

[64] COM(2021) 206.

comune per il calcolo ad alte prestazioni europeo (EuroHPC)[65] a maggio è stata un passo importante per fornire un rapido accesso alle risorse di supercalcolo di EuroHPC, laddove siano essenziali per la sicurezza e la difesa.

Il ruolo della crittografia

La **crittografia** è una tecnologia cruciale nell'ambito della sicurezza, essenziale per garantire sistemi e transazioni digitali sicuri e per tutelare diritti fondamentali quali la libertà di espressione, la privacy e la protezione dei dati. Come dimostrato dalle recenti operazioni EncroChat[66] e Sky ECC[67], i criminali sfruttano le comunicazioni crittografate ed è necessario che le autorità di contrasto dell'UE sviluppino costantemente la loro capacità di gestire informazioni crittografate nel contesto delle indagini penali, nel rispetto delle leggi applicabili. Nel dicembre 2020 è stato varato il nuovo strumento di decrittografia di Europol. Istituita per garantire il rispetto dei diritti fondamentali ed evitare di limitare o indebolire la crittografia, questa iniziativa è a disposizione delle autorità di contrasto di tutti gli Stati membri per contribuire a mantenere la sicurezza di società e cittadini.

Nel dicembre 2020 il Consiglio ha sollecitato un dibattito attivo con l'industria del settore tecnologico e l'elaborazione di un quadro normativo in tutta l'UE, che consenta alle autorità competenti di svolgere efficacemente i loro compiti operativi, tutelando nel contempo la riservatezza, i diritti fondamentali e la sicurezza delle comunicazioni[68]. Nella strategia dell'UE per la lotta alla criminalità organizzata[69], la Commissione ha indicato la sua intenzione di suggerire, nel 2022, un percorso da seguire per affrontare la questione dell'accesso legittimo e mirato alle informazioni cifrate nell'ambito delle indagini e delle azioni penali, senza causare un indebolimento generale della crittografia o comportare una sorveglianza indiscriminata. Un primo passo è la mappatura approfondita delle modalità di utilizzo della cifratura da parte degli Stati membri, unitamente a un processo di consultazione dei portatori di interessi per esaminare e valutare le opzioni giuridiche, etiche e tecniche.

Cooperazione giudiziaria

Una risposta adeguata alle sfide per la sicurezza richiede anche la **modernizzazione della cooperazione giudiziaria** tra i paesi dell'UE grazie all'uso della tecnologia digitale. È in corso di preparazione una proposta legislativa sulla digitalizzazione della cooperazione giudiziaria transfrontaliera nell'UE, che istituirà un canale di comunicazione digitale tra le autorità competenti degli Stati membri e, ove opportuno, le agenzie dell'UE, allo scopo di abbandonare le comunicazioni cartacee tra le autorità e di garantire che gli scambi di dati

---

[65] L'impresa comune EuroHPC è stata istituita nel 2018 per consentire all'UE di diventare un leader mondiale nel supercalcolo. Un nuovo regolamento è attualmente in discussione a livello dell'UE e dovrebbe entrare in vigore nei prossimi mesi.

[66] Nel 2020 un'indagine a livello europeo ha portato allo smantellamento di una rete telefonica cifrata utilizzata da gruppi criminali organizzati.

[67] Il 10 marzo 2021 Eurojust ha sostenuto le operazioni congiunte delle autorità giudiziarie e di contrasto di Belgio, Francia e Paesi Bassi per bloccare l'utilizzo di comunicazioni cifrate da parte di gruppi della criminalità organizzata operanti su vasta scala. Gli investigatori sono riusciti a monitorare l'uso criminale dello strumento di comunicazione Sky ECC, ottenendo indicazioni preziose da centinaia di milioni di messaggi scambiati tra criminali, che hanno consentito di accedere a informazioni cruciali su più di cento operazioni criminali pianificate su vasta scala e di prevenire situazioni potenzialmente letali e possibili vittime.

[68] Risoluzione del Consiglio sulla crittografia - La sicurezza attraverso la crittografia e nonostante la crittografia (13084/1/20 REV 1).

[69] Comunicazione della Commissione - Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025 (COM(2021) 170).

avvengano in modo rapido, sicuro ed efficiente. Una consultazione pubblica[70] ha indicato che questo approccio è sostenuto dal pubblico e dai portatori di interessi.

3. Lotta ai contenuti illegali online

La strategia per l'Unione della sicurezza ha evidenziato che la sicurezza degli ambienti sia fisici che digitali richiede uno sforzo costante per contrastare i contenuti illegali online e nel periodo di riferimento sono stati fatti passi avanti decisivi. Il regolamento atteso da tempo relativo al contrasto della **diffusione di contenuti terroristici online** è stato adottato dal Parlamento europeo e dal Consiglio[71] e sarà pienamente applicabile a partire da giugno 2022. Il regolamento consentirà agli Stati membri di inviare ordini di rimozione a determinati prestatori di servizi di hosting operanti nell'UE e di rimuovere entro un'ora materiali che istigano o incitano a compiere reati di terrorismo, promuovono le attività di un gruppo terroristico o impartiscono istruzioni o forniscono tecniche allo scopo di commettere reati di terrorismo. Esso prevede anche salvaguardie per rafforzare la responsabilità e la trasparenza per quanto concerne le misure intraprese per la rimozione di contenuti terroristici e la tutela contro l'erronea rimozione di contenuti legittimi online.

La **legge sui servizi digitali** proposta dalla Commissione nel dicembre 2020 comprende misure per contrastare la distribuzione online di beni, servizi e contenuti illegali, conferendo agli utenti il potere di segnalare contenuti illegali online e creando un canale privilegiato che dia la priorità ai segnalatori attendibili per la segnalazione di contenuti illegali. Alle piattaforme online inoltre sarebbe richiesto di notificare alle autorità di contrasto competenti i sospetti di taluni gravi reati e sono previste disposizioni che obbligano le piattaforme online molto grandi a effettuare ogni anno valutazioni dei rischi e a prendere misure di attenuazione in relazione a rischi sistematici significativi di diffusione di contenuti illegali. La proposta di una legge sui servizi digitali si basa su iniziative volontarie come il **codice di condotta contro l'incitamento dell'odio online** quali strumenti preziosi per combattere forme specifiche di contenuti illegali.

Le sfide poste dai contenuti illegali online, compresi i materiali pedopornografici, sono state al centro del dibattito in occasione della riunione ministeriale del gennaio 2021 del Forum dell'UE su Internet, che riunisce gli Stati membri dell'UE e le imprese tecnologiche. Nel quadro del Forum dell'UE su Internet, la Commissione ha istituito un processo di consultazione di esperti che coinvolge industria, mondo accademico, autorità pubbliche e organizzazioni della società civile, per individuare soluzioni tecniche che consentirebbero alle società di accertare abusi sessuali su minori online nelle comunicazioni elettroniche con cifratura end-to-end, comunque nel rispetto di diritti fondamentali quali la privacy e la riservatezza delle comunicazioni. È in corso di preparazione anche un elenco dell'UE di gruppi e simboli di estremisti di destra violenti per sostenere le imprese tecnologiche nelle decisioni sulla moderazione dei contenuti, in considerazione dei problemi sollevati in queste discussioni in merito all'individuazione di materiale estremista.

---

[70] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12547-Digitalisation-of-justice-in-the-European-Union-_it.

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

4. Minacce ibride

Le tensioni geopolitiche, anche relative alle nuove tecnologie, stanno determinando un aumento delle minacce alla sicurezza mondiale, la frammentazione e uno scontro permanente tra diverse narrazioni. Sono in aumento gli attori statali e non statali che utilizzano impropriamente le tecnologie per perseguire i propri obiettivi, minacciando le nostre società, l'economia e la sicurezza e danneggiando i diritti umani e le libertà fondamentali. La pandemia ha reso l'UE e i suoi Stati membri più vulnerabili di fronte alle minacce ibride, anche a causa dell'intensificazione della disinformazione e di interferenze manipolative.

Salute e resilienza nei confronti delle minacce ibride

La pandemia ha messo in evidenza la debolezza della preparazione alle emergenze e dei meccanismi di risposta a livello dell'UE. Rispetto ad altri attori mondiali (come gli USA e la Cina) le capacità del settore pubblico e privato in materia di preparazione e gestione delle crisi, in particolare per quanto concerne le contromisure mediche, sono frammentate, disperse e inferiori ai livelli ottimali. Questa frammentazione rappresenta un terreno fertile per le minacce ibride perpetrate da attori statali e non statali. Come indicato nelle comunicazioni "Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero"[72] e "Primi insegnamenti della pandemia di COVID-19"[73], la futura autorità europea per la preparazione e la risposta alle emergenze sanitarie (HERA) svolgerà un ruolo fondamentale per il rafforzamento della resilienza garantendo un solido quadro per la preparazione, la sorveglianza, la valutazione del rischio, l'allarme rapido e la risposta a tutte le gravi minacce per la salute a carattere transfrontaliero.

È in corso un riesame dei meccanismi di gestione delle crisi dell'UE, in stretto collegamento con il **protocollo operativo dell'UE per contrastare le minacce ibride (EU Playbook)**. Un primo passo di questo processo è stato compiuto con il rafforzamento e l'espansione della rete di punti di contatto dei servizi della Commissione, del Servizio europeo per l'azione esterna (SEAE) e dell'Agenzia europea per la difesa. Un altro elemento per integrare considerazioni di natura ibrida nell'elaborazione delle politiche è l'inserimento della valutazione delle minacce ibride per le iniziative politiche nell'ambito di "Legiferare meglio".

Prosegue l'attuazione del quadro congiunto per contrastare le minacce ibride del 2016 e della comunicazione congiunta del 2018 "Rafforzamento della resilienza e potenziamento delle capacità per affrontare le minacce ibride" e il relativo stato di avanzamento è contenuto nella quinta relazione annuale[74] sulla lotta alle minacce ibride. La relazione descrive i progressi nella creazione di una piattaforma online ristretta che servirà da agevole riferimento per gli Stati membri e le istituzioni dell'UE riguardo agli strumenti e alle misure per la lotta alle minacce ibride a livello dell'UE, le misure per migliorare la conoscenza situazionale, in particolare attraverso la cellula dell'UE per l'analisi delle minacce ibride (HFC), e l'individuazione di parametri di riferimento settoriali per la resilienza dell'UE.

[72] COM(2020) 724.
[73] COM(2021) 380.
[74] SWD(2021) 729.

La lotta alle minacce ibride e informatiche sempre più complesse e distruttive resta una componente di importanza fondamentale della **cooperazione UE-NATO**, come evidenziato anche nel comunicato del recente vertice NATO di Bruxelles[75]. Questa cooperazione è proseguita a un ritmo costante, basandosi sui risultati ottenuti e mantenendo lo slancio dei precedenti periodi di riferimento. I principali risultati sono stati presentati nella sesta relazione congiunta UE-NATO sui progressi compiuti[76]. Sono costantemente aumentate le adesioni al Centro europeo di eccellenza per la lotta contro le minacce ibride di Helsinki (Hybrid CoE), che ora conta 30 Stati membri dell'UE e alleati NATO. Durante il periodo di riferimento, Hybrid CoE ha facilitato una serie di discussioni, workshop ed esercitazioni sulla base di scenari.

Nell'ambito del patto sulla dimensione civile della PSDC[77], le minacce ibride sono state aggiunte tra gli ambiti prioritari per le missioni civili della PSDC, con l'elaborazione di un corrispondente miniconcetto su un sostegno della dimensione civile della PSDC alla lotta contro le minacce ibride[78]. Il documento propone di 1) definire le priorità della protezione delle missioni contro gli attacchi ibridi e 2) se del caso, assistere lo Stato ospitante nell'aumentare la resilienza alle minacce ibride.

Una componente importante delle minacce ibride è la **disinformazione**. Il piano d'azione per la democrazia europea[79] ha individuato numerose azioni per rafforzare la risposta alle manipolazioni delle informazioni e alle ingerenze straniere[80]. Il Consiglio europeo ha accolto con favore l'approccio del piano d'azione per la democrazia e ha invitato anche ad approfondire l'azione dell'UE[81]. Il SEAE sta collaborando strettamente con la Commissione per portare avanti il lavoro, facendo riferimento anche al sistema di allarme rapido dell'UE per riunire la comunità di esperti al fine di istituire un quadro solido, robusto, flessibile e generale contro la manipolazione delle informazioni e le ingerenze straniere. Questo obiettivo è sostenuto anche dal codice di buone pratiche sulla disinformazione online, che in maggio è stato rafforzato con la pubblicazione di orientamenti che definiscono il modo in cui i fornitori di servizi online e altre parti interessate dovrebbero rafforzare le loro misure per colmare le lacune e le carenze del codice di buone pratiche e creare un ambiente online più trasparente, sicuro e affidabile[82].

IV. Proteggere gli europei dal terrorismo e dalla criminalità organizzata

1. Terrorismo e radicalizzazione

---

75 Comunicato del vertice NATO di Bruxelles del 14 giugno 2021.

76 Sesta relazione sullo stato dei lavori relativi all'attuazione dell'insieme comune di proposte approvato dai Consigli dell'UE e della NATO il 6 dicembre 2016 e il 5 dicembre 2017, 3 giugno 2021.

77 Doc. Rif. 14305/18 del 19 novembre 2018.

78 Doc. Rif. 8077/20 del 20 maggio 2020.

79 COM(2020) 790.

80 Tre aree fondamentali sono: 1) affinare ulteriormente la terminologia utilizzata per descrivere il problema; 2) sviluppare un quadro e una metodologia comuni per raccogliere prove sistematiche della manipolazione delle informazioni e dell'ingerenza straniere e 3) sviluppare ulteriormente il pacchetto di strumenti dell'UE per contrastare la manipolazione delle informazioni e l'ingerenza straniere al fine di renderlo maggiormente adeguato allo scopo di imporre oneri ai responsabili.

81 Dichiarazione del Consiglio europeo di marzo 2021; conclusioni del Consiglio di dicembre 2020.

82 COM(2021) 262. Gli orientamenti affrontano anche nello specifico l'infodemia relativa alla COVID-19.

Gli attacchi della fine del 2020 hanno dimostrato quanto sia fondamentale affrontare il terrorismo e le sue cause profonde. Adottato nel dicembre 2020, il nuovo **programma di lotta al terrorismo dell'UE**[83] indica come intensificare la lotta contro il terrorismo e l'estremismo violento e promuovere la resilienza dell'UE nei confronti delle minacce terroristiche. La sua attuazione è ben avviata. La Commissione sta inoltre valutando la direttiva (UE) 2017/541 sulla lotta contro il terrorismo, che stabilisce norme minime relative alla definizione dei reati di terrorismo e dei reati ad esso connessi e delle relative sanzioni, nonché le misure di protezione, sostegno e assistenza per le vittime del terrorismo.

Alla fine del 2020 la Commissione ha assegnato un nuovo contratto quadro a un consorzio per il sostegno politico alla **rete di sensibilizzazione al problema della radicalizzazione** (RAN) che integra il lavoro degli operatori della rete e per continuare a sostenere i responsabili politici su questioni di prevenzione generale. L'obiettivo è quello di rafforzare le conoscenze e le capacità degli Stati membri in materia di comunicazione strategica, nonché la base di conoscenze comprovate per l'ulteriore sviluppo di politiche, approcci e interventi concreti.

La Commissione collabora inoltre con gli Stati membri per combattere le ideologie estremiste che possono sfociare in estremismo violento. Nel 2021 il lavoro si concentra sugli intercollegamenti tra tutti i generi di ideologie estremiste violente (tra cui estremismo di sinistra, di destra e islamico) e sulla radicalizzazione che porta all'autosegregazione. Negli ultimi mesi si sono svolte numerose iniziative di sensibilizzazione in questo campo. Le attività della RAN si sono estese ai Balcani occidentali attraverso un apposito contratto in vigore da gennaio 2021.

Un'altra priorità è evitare che i terroristi acquisiscano materiali che possono essere trasformati in armi. Il piano d'azione del 2017 sul materiale **chimico, biologico, radiologico e nucleare (CBRN)** è stato portato avanti con uno studio di fattibilità per la limitazione dell'accesso ad alcune sostanze chimiche ad alto rischio, completato nel giugno 2021. La Commissione ha avviato anche il lavoro preparatorio per esercitazioni e workshop transfrontalieri sulla sicurezza delle fonti radioattive e biologiche in ospedali e laboratori, che si terranno nel 2022. L'attuazione del piano d'azione sul materiale CBRN è sostenuta da progetti cofinanziati dal Fondo sicurezza interna, che ha selezionato iniziative come il progetto Stadio sicuro[84], incentrato sulla protezione e la preparazione in materia di CBRN nelle grandi strutture sportive come gli stadi di calcio. La nuova legislazione relativa all'immissione sul mercato e all'uso di precursori di esplosivi è entrata in vigore il 1° febbraio 2021. L'attuazione è ben avviata e la Commissione continua ad assistere i portatori di interesse nell'adempimento dei rispettivi obblighi.

Una parte del collegamento intrinseco tra la sicurezza esterna e interna dell'Unione riguarda la collaborazione in materia di minacce quali i materiali CBRN. Gli strumenti di finanziamento esterno dell'UE sostengono iniziative per migliorare la governance e la cooperazione globale e regionale in materia di individuazione e attenuazione dei rischi CBRN, sulla base dell'esperienza positiva acquisita ad esempio attraverso l'iniziativa dei centri di eccellenza dell'UE sull'attenuazione dei rischi CBRN e il programma di controllo

[83] Comunicazione della Commissione, Un programma di lotta al terrorismo dell'UE: prevedere, prevenire, proteggere e reagire (COM(2020) 795).

[84] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034226/ISFP.

delle esportazioni di prodotti a duplice uso. Finora 34 paesi hanno preparato un piano d'azione nazionale CBRN e 10 paesi l'hanno adottato ufficialmente.

Salute e terrorismo

Il programma EU4Health[85] sostiene azioni in materia di prevenzione, preparazione e risposta in caso di minacce per la salute a carattere transfrontaliero.

Il terzo programma UE per la salute cofinanzia la **preparazione sanitaria contro gli attacchi terroristici**[86], un'azione comune delle autorità sanitarie dell'UE, varata nel maggio 2021 con l'obiettivo di proteggere i cittadini dell'UE da emergenze sanitarie intenzionali, affrontando le lacune nella preparazione sanitaria e rafforzando il lavoro intersettoriale (nei settori sanitario, della sicurezza e della protezione civile) in risposta a un attacco terroristico biologico e/o chimico.

Il programma per la salute 2017-2021 ha sostenuto la preparazione e le capacità di risposta del settore sanitario nei confronti delle minacce chimiche e biologiche. L'azione comune **Rafforzamento dei regolamenti internazionali in materia di salute e preparazione dei partner nell'UE**[87] ospita una rete di laboratori di riferimento per agenti altamente patogeni, che conta 41 laboratori.

La risposta alla minaccia posta dai **combattenti terroristi stranieri** di ritorno in Siria e Iraq rimane un elemento importante dell'antiterrorismo e una priorità nella prevenzione della radicalizzazione. Come concordato negli orientamenti strategici su un approccio coordinato dell'UE alla prevenzione della radicalizzazione per il 2021, la Commissione ha lavorato su quattro principali priorità: rimpatrio dei minori, rafforzamento e sicurezza del processo di ritorno (rimpatrio, azione giudiziaria e reinserimento), competenze dei professionisti coinvolti nel reinserimento delle donne e dei minori rimpatriati. In relazione alle carceri e ai campi di sfollati interni nel nord-est della Siria, e in accordo con gli Stati membri, il SEAE e la Commissione stanno esplorando nuove modalità di assistenza più efficaci nella regione, per contribuire a migliorare le condizioni di vita e cercare di fermare la radicalizzazione.

La Commissione ha recentemente concluso l'aggiornamento dell'analisi dei dati in materia di lotta al terrorismo e prevenzione/contrasto dell'estremismo violento. Dalla mappatura è emerso che la portata e la rapidità dei finanziamenti da strumenti esterni dell'UE a favore di tali attività è stata impressionante[88]. Al 1° gennaio 2021 erano in corso nel complesso 99 azioni intese a prevedere, prevenire, proteggere e reagire nella lotta contro il terrorismo in paesi al di fuori dell'UE, per un totale di 501 milioni di EUR (un aumento dell'8 % rispetto all'anno precedente) per conseguire le priorità del programma di lotta al terrorismo dell'UE e delle conclusioni del Consiglio in materia di lotta al terrorismo.

---

[85] Istituito dal regolamento (UE) 2021/522.

[86] Health preparedness against terror attack Joint Action, https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-2019-presentation-03_en.pdf.

[87] Azione comune SHARP - Rafforzamento dei regolamenti internazionali in materia di salute e preparazione dei partner nell'UE https://sharpja.eu/wp7/.

[88] L'UE fornisce un sostegno consistente a tutte le iniziative del Forum globale contro il terrorismo, tra cui l'Istituto per la Giustizia e lo Stato di diritto, nonché al Fondo globale per l'impegno e la capacità di resistenza delle comunità (GCERF) al fine di sostenere le attività di prevenzione/contrasto degli estremismi violenti in una serie di paesi di importanza strategica per l'UE.

Sono state intraprese ulteriori misure per sviluppare e rafforzare partenariati e cooperazione in materia di lotta al terrorismo con i paesi del vicinato e oltre, attingendo alle competenze della rete per la lotta al terrorismo e agli esperti di sicurezza dell'UE. Negli ultimi mesi, l'attuazione del piano d'azione congiunto sulla lotta al terrorismo con i partner dei Balcani occidentali è progredita, con alcuni ritardi dovuti alla pandemia e a dinamiche di politica interna dei partner.

L'UE ha continuato ad applicare il suo quadro di sanzioni antiterrorismo durante il periodo di riferimento. Nel febbraio 2021, il Consiglio ha portato a termine il riesame dell'elenco di terroristi dell'UE[89] e nell'aprile 2021 è stata adottata una nuova designazione nel quadro del regime autonomo di sanzioni antiterrorismo dell'UE nei confronti dell'ISIL (Da'esh)/Al-Qaeda[90].

Infine nel maggio 2021 Eurojust e la rete europea hanno organizzato congiuntamente la sesta giornata UE contro l'impunità, incentrata in particolare sui crimini internazionali commessi in Siria da organizzazioni terroristiche e dal regime siriano. L'iniziativa si è basata sul lavoro intrapreso dall'anno scorso per sostenere azioni penali cumulative nei confronti di combattenti terroristi stranieri per reati connessi al terrorismo e crimini internazionali e ha ulteriormente dimostrato che il rafforzamento della cooperazione giudiziaria tra Stati membri è fondamentale per l'identificazione e il perseguimento dei criminali di guerra presenti nell'UE.

2. Lotta contro la criminalità organizzata

La relazione del 2021 sulla valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA 2021)[91] ha fatto luce sulla costante minaccia della criminalità organizzata e sulla sua crescente complessità. La criminalità organizzata è transnazionale: il 65 % dei gruppi della criminalità organizzata è composto da membri di molteplici nazionalità e sette su dieci operano in più di tre paesi. Il panorama della criminalità organizzata nell'UE è caratterizzato da un ambiente collegato in rete, in cui diversi gruppi collaborano tra loro e con prestatori di servizi criminali. Il 60 % delle reti criminali prevede l'impiego della violenza nella propria attività criminale, ma praticamente tutte le attività criminali ora presentano qualche componente online. È in aumento anche il rischio di infiltrazioni della criminalità nell'economia legale: secondo le stime, in più dell'80 % dei casi le attività criminali si servono di strutture commerciali legali.

Criminali che sfruttano le vulnerabilità economiche create dalla pandemia

Traendo insegnamento da crisi precedenti, si può prevedere che una situazione economica volatile caratterizzata da crescente povertà e disuguaglianza sociale funga da terreno fertile

[89] Decisione (PESC) 2021/142 del Consiglio del 5 febbraio 2021 che aggiorna l'elenco delle persone, dei gruppi e delle entità a cui si applicano gli articoli 2, 3 e 4 della posizione comune 2001/931/PESC.

[90] Decisione (PESC) 2021/613 del Consiglio e regolamento di esecuzione (UE) 2021/612, del 15 aprile 2021, concernenti misure restrittive nei confronti dell'ISIL (Dàesh) e di Al Qaeda e di persone, gruppi, imprese ed entità a essi associati.

[91] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

per la criminalità organizzata e gravi forme di criminalità.

Le imprese operanti in settori che risentono di pressioni economiche particolarmente negative, come i settori dell'ospitalità, della ristorazione e del turismo, sono sempre più soggette a infiltrazioni criminali[92].

Nel 2020 il Centro Europol per la criminalità organizzata e le forme gravi di criminalità (ESOCC) ha ricevuto e trattato più di 35 183 contributi operativi nei sette ambiti di interesse del Centro[93], che rappresentano oltre la metà (57 %) dei contributi operativi di Europol. L'ESOCC ha sostenuto gli Stati membri in 837 operazioni, con un aumento del 41 % in termini comparabili rispetto al 2019. Queste cifre riflettono la maggiore attività dei gruppi della criminalità organizzata e la crescente richiesta del sostegno di Europol in questo campo da parte degli Stati membri. L'ESOCC ha organizzato e coordinato 11 task force operative per il coordinamento delle attività di intelligence e investigative contro 60 cosiddetti "obiettivi di alto valore", cioè persone sospettate di essere membri di organizzazioni criminali particolarmente pericolose, di cui 21 sono stati arrestate.

Per contribuire alla risposta alle sfide crescenti, in aprile la Commissione ha adottato la **strategia dell'UE per la lotta alla criminalità organizzata** (2021-2025)[94]. Il documento definisce le azioni prioritarie intese a promuovere la cooperazione giudiziaria e l'attività di contrasto, garantire indagini efficaci per smantellare le strutture della criminalità organizzata e combattere i crimini altamente prioritari, puntando ai profitti generati dalla criminalità organizzata e adeguando le attività di contrasto e giudiziarie all'era digitale. La Commissione ha pubblicato anche un documento sulla "piattaforma multidisciplinare europea contro le minacce criminali" (EMPACT)[95], che spiega come sfruttare appieno il potenziale di EMPACT e trasformarla in uno strumento di primo piano per la cooperazione operativa multisciplinare e multiagenzia per la lotta alla criminalità organizzata. La Commissione è strettamente coinvolta nella preparazione del prossimo ciclo EMPACT, che coprirà il periodo dal 2022 al 2025.

Lotta contro la tratta degli esseri umani

La tratta degli esseri umani è un crimine altamente redditizio, che produce enormi profitti per i criminali a spese delle vittime e della società nel suo complesso. In aprile la Commissione ha adottato la strategia dell'UE per la lotta alla tratta degli esseri umani (2021-2025)[96]. Poiché la tratta degli esseri umani è spesso condotta da gruppi organizzati, questa strategia è strettamente correlata alla strategia dell'UE per la lotta alla criminalità organizzata. La strategia anti-tratta propone iniziative legislative, politiche e operative per la lotta alla

[92] Sulla base del contributo della prima riunione del gruppo di lavoro sulle minacce criminali legate alla COVID-19 e le risposte delle autorità di contrasto; Europol 2020, Enterprising criminals: Europe's fight against the global networks of financial and economic crime.

[93] Traffico di migranti, gruppi della criminalità organizzata ad alto rischio, crimini ambientali, reati organizzati contro il patrimonio, traffico di stupefacenti, tratta di essere umani e traffico di armi ed esplosivi.

[94] COM(2021) 170.

[95] EMPACT è lo strumento di cooperazione di polizia dell'UE utilizzato per affrontare le principali minacce alla sicurezza dell'UE rafforzando la cooperazione tra i servizi competenti degli Stati membri, le istituzioni dell'UE e le agenzie dell'UE nonché i paesi terzi e le organizzazioni. EMPACT riunisce diversi portatori di interessi per migliorare e rafforzare la cooperazione tra gli Stati membri, le istituzioni dell'UE e le agenzie dell'UE, nonché i paesi terzi e le organizzazioni, compreso il settore privato, se del caso (SWD(2021) 74).

[96] Comunicazione della Commissione - Strategia dell'UE per la lotta alla tratta degli esseri umani 2021-2025 (COM(2021) 171).

tratta degli esseri umani, dalla prevenzione alla condanna dei criminali, facendo della protezione delle vittime una priorità in tutte le fasi e tenendo conto in particolare delle vittime donne e minori, nonché della tratta a fini di sfruttamento sessuale. L'obiettivo è ridurre la domanda che alimenta la tratta; smantellare il modello criminale per porre fine allo sfruttamento delle vittime; proteggere, sostenere e responsabilizzare le vittime e affrontare la dimensione internazionale di questa forma di criminalità. La strategia ha fatto seguito a una relazione di Eurojust che formula 18 raccomandazioni per sostenere gli Stati membri nelle indagini, nelle azioni penali e nella cooperazione giudiziaria nei casi di tratta, ma anche nell'identificazione, nel salvataggio e nella protezione delle vittime[97].

Lotta contro le droghe illegali

A seguito dell'adozione della strategia dell'UE in materia di droga 2021-2025, prosegue il dibattito sul relativo piano d'azione, in vista dell'adozione in seno al Consiglio entro la fine della Presidenza portoghese. Alla legislazione sulle nuove **sostanze psicoattive** (NPS), entrata pienamente in vigore nel novembre 2018, ha fatto seguito un atto delegato che include due nuove sostanze psicoattive nella definizione di stupefacenti[98].

La relazione di Eurojust sul traffico di stupefacenti dell'aprile 2021[99] sottolinea l'aumento della produzione di droghe sintetiche e dell'uso della darknet per la vendita, con conseguenti difficoltà legali per i procuratori dell'UE. La relazione formula raccomandazioni per aumentare le indagini finanziarie, il recupero dei beni e la cooperazione giudiziaria, anche con paesi terzi. Nel marzo 2021, in occasione del dialogo annuale UE-USA in materia di droghe, Eurojust ha presentato casi cruciali ed esempi di successo nella cooperazione giudiziaria tra gli Stati membri e gli USA in casi relativi al traffico di stupefacenti. La prima riunione del dialogo UE-Cina in materia di droghe si è tenuta il 22 gennaio 2021 e ha riguardato anche la cooperazione nella lotta contro le droghe. L'UE ha partecipato alla 64ª Commissione stupefacenti delle Nazioni Unite e ha ripetuto i suoi appelli per accelerare l'attuazione degli impegni generali assunti dalla comunità internazionale per affrontare la situazione delle droghe a livello mondiale.

Lotta contro il traffico illecito di armi da fuoco

La direttiva sulle armi da fuoco codificata[100] è entrata in vigore nell'aprile 2021 e la Commissione vi ha dato seguito mediante la normativa sullo scambio sistematico, con mezzi elettronici, di informazioni relative al rifiuto di concedere l'autorizzazione ad acquisire o detenere talune armi da fuoco[101]. Queste norme dovrebbero applicarsi con effetto dal 31 gennaio 2022 e consentiranno alle autorità nazionali competenti di sapere se al richiedente di una licenza sia stata negata un'analoga autorizzazione in un altro Stato membro, impedendo quindi la scelta opportunistica del foro per eludere il divieto di detenere un'arma da fuoco.

---

97 La relazione è consultabile al seguente indirizzo: https://www.eurojust.europa.eu/eurojust-report-trafficking-human-beings.

98 C(2021) 1570; il periodo di esame del Parlamento europeo e del Consiglio termina alla metà di maggio.

99 La relazione è consultabile al seguente indirizzo: https://www.eurojust.europa.eu/eurojust-report-drug-trafficking.

100 Direttiva (UE) 2017/853 relativa al controllo dell'acquisizione e della detenzione di armi.

101 Direttiva delegata C(2021)3400, del 21 maggio 2021, che stabilisce le modalità dettagliate per lo scambio sistematico con mezzi elettronici di informazioni relative al rifiuto di concedere autorizzazioni all'acquisizione o alla detenzione di talune armi da fuoco.

La Commissione sostiene anche un progetto pilota per istituire la tracciatura in tempo reale degli incidenti connessi ad armi da fuoco nel territorio dell'UE al fine di mantenere un quadro permanentemente aggiornato. Per sostenere il lavoro delle autorità di contrasto, la Commissione sta guidando l'azione relativa all'istituzione e allo sviluppo di punti focali sulle armi da fuoco a livello nazionale.

Per quanto riguarda la cooperazione internazionale, la Commissione ha sostenuto attivamente il coinvolgimento costruttivo della Turchia nelle attività operative dell'EMPACT relative alla minaccia delle armi d'allarme e da segnalazione trasformabili; inoltre, ha contribuito a riportare la questione del traffico di armi da fuoco nell'agenda della cooperazione con i paesi del Medio Oriente e del Nord Africa. La Commissione è stata molto attiva anche nella cooperazione operativa con l'Europa sudorientale, tra l'altro con la preparazione di un'operazione congiunta tra Stati membri e partner dei Balcani occidentali e di incontri regionali delle commissioni per le armi leggere e di piccolo calibro.

Il programma dell'UE in materia di flussi illeciti globali[102] ha continuato a rappresentare un meccanismo efficace per il coordinamento dell'azione transregionale contro la criminalità organizzata e per lo sviluppo delle capacità di oltre 80 paesi partner in tutto il mondo per fermare il traffico di merci illegali, in particolare stupefacenti e armi da fuoco. La Commissione ha sostenuto anche le agenzie e gli Stati membri dell'UE nell'ampliare il raggio d'azione dell'attività di contrasto.

Lotta contro la criminalità finanziaria

Nell'ambito della lotta contro il rischio di infiltrazioni della criminalità organizzata nell'economia legale, gli Stati membri sono tenuti a recepire entro agosto 2021 la direttiva del 2019 che agevola l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati[103]. La Commissione intende monitorare da vicino il recepimento e l'effettiva applicazione della direttiva.

A maggio e giugno 2021 si sono tenuti due incontri di consultazione con gli Stati membri sulla revisione della decisione del Consiglio sugli uffici per il recupero dei beni[104] e sulla direttiva in materia di confisca[105]. Le discussioni hanno sottolineato il valore aggiunto di questi strumenti ai fini del rafforzamento del recupero dei beni nell'Unione e l'importanza di una gestione efficace dei beni confiscati, nel pieno rispetto dei diritti fondamentali, nonché la necessità di migliorare la cooperazione durante l'intero processo di recupero dei beni.

[102] https://illicitflows.eu/.

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

[104] Decisione 2007/845/GAI del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi.

[105] Direttiva 2014/42/UE, del 3 aprile 2014, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea.

Dal 3 giugno 2021 si applica una nuova legislazione relativa ai controlli sul denaro contante in entrata nell'UE o in uscita dall'UE[106] e da maggio sono in vigore disposizioni di attuazione essenziali che stabiliscono procedure e norme tecniche[107]. Sono in preparazione ulteriori disposizioni di attuazione che stabiliscono i criteri per il quadro comune di gestione del rischio sui movimenti di contante.

La Procura europea (EPPO) ha assunto i propri compiti in materia di indagine e azione penale il 1° giugno 2021 e ha cominciato a indagare e perseguire i reati che ledono gli interessi finanziari dell'Unione. I reati indagati e perseguiti dall'EPPO includono le frodi in materia di IVA concernenti il territorio di due o più Stati membri con un danno totale di almeno 10 milioni di EUR. Ogni anno gli Stati membri perdono miliardi di euro di entrate IVA a causa delle frodi.

Lotta contro la criminalità ambientale

La **direttiva sulla criminalità ambientale** (2008/99/CE) è il principale strumento giuridico dell'UE sulla tutela penale dell'ambiente. Sono in corso ampie consultazioni ai fini della revisione del testo per migliorarne l'attuazione e rafforzare il funzionamento della catena di applicazione della legge (accertamento, indagine, perseguimento, procedimento penale). L'attività contro la criminalità ambientale è portata avanti anche attraverso il Forum sulla conformità e la governance ambientali[108], le cui riunioni di gennaio e giugno 2021 si sono incentrate sulla revisione della direttiva e sulla lotta contro la criminalità ambientale in generale.

Lotta contro il traffico di beni culturali

La legislazione dell'UE sull'importazione di beni culturali è intesa a bloccare le importazioni di beni culturali esportati illecitamente dal loro paese d'origine. È in corso la definizione di disposizioni di attuazione concernenti un sistema elettronico centralizzato per l'importazione di beni culturali, che consentirà l'archiviazione e lo scambio di informazioni tra gli Stati membri e l'adempimento delle formalità di importazione. La norma generale di divieto prevista dal regolamento[109] è entrata in vigore il 28 dicembre 2020, consentendo alle autorità doganali degli Stati membri di controllare e intervenire sulle spedizioni che possono contenere beni culturali esportati illecitamente dal paese di origine.

V. Un forte ecosistema europeo della sicurezza

1. Cooperazione e scambio di informazioni

La strategia per l'Unione della sicurezza ha indicato come l'azione dell'UE possa fornire un contributo sostanziale per affrontare minacce alla sicurezza di carattere transfrontaliero e intersettoriale sempre più complesse, fornendo agli operatori della sicurezza negli Stati membri gli strumenti e le informazioni di cui hanno bisogno.

[106] Regolamento (UE) 2018/1672 relativo ai controlli sul denaro contante in entrata nell'Unione o in uscita dall'Unione.

[107] Regolamento di esecuzione (UE) 2021/776 della Commissione, dell'11 maggio 2021, che stabilisce i modelli per determinati moduli nonché le norme tecniche per l'efficace scambio di informazioni.

[108] Compliance Assurance - Legislation - Environment - European Commission (europa.eu).

[109] Regolamento (UE) 2019/880 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'introduzione e all'importazione di beni culturali.

Europol svolge un ruolo centrale a questo proposito. La proposta della Commissione adottata lo scorso dicembre per la modernizzazione e il rafforzamento del **mandato di Europol**[110] riguarda specifiche limitazioni attuali di Europol, come i rapporti con il settore privato. La Commissione propone inoltre di consentire a Europol di inserire nel sistema d'informazione Schengen segnalazioni su terroristi e altri criminali, sulla base di informazioni fornite da paesi terzi, rafforzando così la capacità di Europol di sostenere gli Stati membri nel contrasto alle forme gravi di criminalità e al terrorismo. La Commissione auspica una rapida conclusione del Parlamento europeo e del Consiglio in merito alle rispettive posizioni in vista dell'avvio dei triloghi sotto la Presidenza slovena.

La cooperazione tra l'**UE e Interpol** è profonda e di lunga data. Interpol è un partner fondamentale dell'UE nel settore della sicurezza interna ed esterna, compresa la lotta al terrorismo e alla criminalità organizzata, nonché nella gestione integrata delle frontiere. La Commissione ha proposto negoziati per rafforzare ulteriormente la cooperazione operativa e strategica grazie a un accordo di cooperazione[111].

A livello operativo, sono in corso i preparativi per la piena attuazione della revisione del **sistema d'informazione Schengen** (SIS) con l'intento di completare tutte le necessarie attività di verifica entro la fine del 2021. Europol è connessa alla centrale di posta elettronica (mail relay) SIRENE[112] da marzo 2021. Alla fine del 2020 la maggior parte degli Stati membri aveva attivato la nuova funzionalità di ricerca di impronte digitali del SIS[113].

È cominciato il lavoro di modifica della legislazione per migliorare la capacità di **Eurojust** di individuare i collegamenti tra procedimenti paralleli nei casi di terrorismo transfrontaliero[114]. Parallelamente, Eurojust ha continuato ad assicurare follow-up operativi e coordinamento sulla base delle informazioni trasmesse mediante il registro giudiziario antiterrorismo (CTR), istituito allo scopo di individuare i collegamenti tra i procedimenti giudiziari antiterrorismo negli Stati membri. L'esperienza del CTR finora indica un aumento significativo della quantità di informazioni trasmesse a Eurojust e sono già stati individuati alcuni collegamenti tra procedimenti precedentemente sconosciuti alle autorità nazionali. Il CTR ha anche consentito di migliorare in misura rilevante la condivisione delle informazioni nei procedimenti antiterrorismo.

È cominciato il lavoro preparatorio per l'istituzione della **piattaforma di collaborazione informatica per le squadre investigative comuni (JIT)**. Sono in corso consultazioni con Stati membri, segretariato della rete JIT, Eurojust, Europol e OLAF sulla progettazione della piattaforma di collaborazione. Da aprile 2021 Eurojust fornisce anche assistenza finanziaria alle squadre investigative comuni per azioni urgenti e/o impreviste al di fuori del normale programma di finanziamento[115].

---

[110] COM(2020) 769, COM(2020) 791.
[111] COM(2021) 177.
[112] Informazioni supplementari richieste all'ingresso nazionale. Ogni paese dell'UE che utilizza il SIS ha istituito un ufficio nazionale SIRENE, competente per qualsiasi scambio di informazioni supplementari e per il coordinamento di attività connesse alle segnalazioni SIS.
[113] Sistema di identificazione automatizzato delle impronte digitali.
[114] Decisione 2005/671/GAI del Consiglio e regolamento (UE) 2018/1727.
[115] https://www.eurojust.europa.eu/eurojust-launches-new-scheme-urgent-jit-funding.

I dati del **codice di prenotazione** (PNR) sono una fonte di informazioni importante per individuare i soggetti pericolosi per la sicurezza. Sulla base delle informazioni raccolte per preparare il riesame della legislazione[116], la Commissione sta aiutando gli Stati membri a migliorare l'uso dei dati PNR e a intensificare la cooperazione[117]. La maggioranza delle unità d'informazione sui passeggeri è pienamente operativa e il trattamento dei dati PNR è uno strumento importante per le autorità di contrasto nazionali nella lotta contro il terrorismo e i reati gravi, malgrado il calo del numero di passeggeri aerei durante la pandemia.

L'attività si è intensificata anche sul fronte internazionale. Il 30 dicembre 2020 è stato firmato l'accordo sugli scambi e la cooperazione UE-Regno Unito[118], in vigore da maggio. L'accordo riguarda lo scambio di dati PNR e il loro uso ai fini della lotta al terrorismo e alle forme gravi di criminalità. La Commissione ha adottato relazioni[119] sulle valutazioni congiunte degli accordi internazionali vigenti sui dati del codice di prenotazione (PNR) con gli USA e l'Australia, nonché sulla verifica congiunta dell'accordo UE-Australia. Nel complesso, queste relazioni hanno confermato i vantaggi dell'uso del PNR, la sua efficacia ai fini della realizzazione delle finalità perseguite e l'unicità delle informazioni fornite dal PNR. Nel gennaio 2021 il Consiglio ha adottato la posizione dell'Unione[120] che accoglie con favore l'adozione da parte dell'Organizzazione per l'aviazione civile internazionale (ICAO) di una nuova serie di norme e pratiche raccomandate sul trattamento e sulla protezione dei dati PNR. Il 28 febbraio 2021 la decisione ICAO è divenuta operativa e vincolante per tutti i membri dell'ICAO[121] e ora rappresenta un valido riferimento per il trattamento dei dati PNR a livello mondiale, nel pieno rispetto dei diritti fondamentali.

Sono in corso i negoziati per lo scambio di dati personali tra Europol e taluni paesi terzi per la lotta alle forme gravi di criminalità e al terrorismo. I primi due cicli di negoziati con la Nuova Zelanda si sono svolti in un'atmosfera costruttiva. Si sono registrati progressi anche nei negoziati con la Turchia e si sono svolti dialoghi costruttivi con la Tunisia. Sono in corso colloqui esplorativi a livello tecnico con una serie di altri paesi.

Nel marzo 2021 il Consiglio ha adottato il mandato della Commissione per avviare i negoziati per gli accordi tra l'UE e tredici paesi terzi[122] sulla cooperazione tra Eurojust e le autorità competenti per la cooperazione giudiziaria in materia penale. Questi accordi internazionali diventeranno una pietra angolare della legislazione dell'UE in materia di sicurezza e contribuiranno a migliorare la lotta contro la criminalità organizzata a livello mondiale.

Dal 2012 il **sistema europeo di informazione sui casellari giudiziali (ECRIS)** garantisce uno scambio elettronico efficiente di informazioni sui casellari giudiziali tra gli Stati membri, con oltre 4 milioni di messaggi scambiati ogni anno. La Commissione ha adottato una

[116] COM(2020) 305 sul riesame della direttiva (UE) 2016/681.
[117] La Slovenia è l'ultimo Stato membro le cui misure nazionali di recepimento della direttiva PNR sono oggetto di valutazione da parte della Commissione, mentre tutti gli altri Stati membri hanno recepito completamente la direttiva.
[118] GU L 444 del 31.12.2020, pag. 309.
[119] COM(2021) 17 final; COM(2021) 18 final; COM(2021) 19 final.
[120] GU L 37 del 3.2.2021, pag. 6.
[121] Gli Stati membri hanno introdotto una differenza per quanto riguarda una parte degli standard e delle pratiche raccomandate (SARP) pertinenti.
[122] Algeria, Armenia, Argentina, Bosnia-Erzegovina, Brasile, Colombia, Egitto, Israele, Giordania, Libano, Marocco, Tunisia e Turchia.

relazione sul funzionamento di ECRIS[123] e sta dando seguito alle sue conclusioni presso gli Stati membri. Il lavoro per lo sviluppo e l'attuazione di un sistema centralizzato per l'identificazione degli Stati membri in possesso di informazioni sulla condanna di cittadini di paesi terzi (ECRIS-TCN) è in corso, con l'intento di avviare le operazioni nel 2023. Il nuovo sistema integrerà ECRIS per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi condannati nell'UE.

2. ***Il contributo di frontiere esterne solide***

Una gestione efficiente delle frontiere esterne dell'UE è fondamentale per garantire la sicurezza dei cittadini. La strategia della Commissione per lo spazio Schengen[124] prevede azioni in questo campo intese a proteggere l'integrità dello spazio Schengen e migliorarne ulteriormente il funzionamento. È in fase di sviluppo la nuova architettura dei sistemi d'informazione dell'UE per la gestione della sicurezza, delle frontiere e della migrazione, a sostegno delle autorità nazionali. È essenziale che gli Stati membri prendano senza indugio le misure necessarie per rispettare il calendario di attuazione concordato al fine di realizzare questo ambizioso progetto.

Il lavoro sull'attuazione dei **regolamenti sull'interoperabilità** sta procedendo, in vista della piena attuazione entro la fine del 2023. EU-LISA sta completando l'approvvigionamento delle diverse componenti dell'interoperabilità e la Commissione sta collaborando con esperti su un manuale di orientamento. Sono in corso i preparativi per l'entrata in funzione del **sistema di ingressi/uscite** (EES), con l'intento di completare le verifiche e la formazione all'inizio del 2022, prima dell'entrata in funzione nel maggio 2022. Sono in corso anche i preparativi per il **sistema europeo di informazione e autorizzazione ai viaggi** (ETIAS), la cui entrata in funzione è prevista entro la fine del 2022. Il Parlamento europeo e il Consiglio hanno anche trovato un accordo sulla proposta di garantire la connessione tra ETIAS e le banche dati pertinenti dell'UE.

Nel dicembre 2020 il Parlamento europeo e il Consiglio hanno raggiunto un accordo provvisorio sulla proposta della Commissione di rivedere e aggiornare il **sistema di informazione sui visti** (VIS). I vantaggi principali delle modifiche concordate comprendono controlli più approfonditi dei precedenti personali dei richiedenti il visto grazie al miglioramento dello scambio di informazioni tra gli Stati membri, l'ampliamento del VIS per includere i visti per soggiorni di lunga durata e i permessi di soggiorno e l'abbassamento dell'età dell'identificazione tramite impronte digitali per i minori ai fini della lotta contro la tratta degli esseri umani. Insieme ad altri sistemi di informazione nuovi e aggiornati, il nuovo VIS dovrebbe essere operativo e pienamente interoperabile entro la fine del 2023.

Le prime squadre del corpo permanente della **guardia di frontiera e costiera europea** sono state dispiegate con successo a partire dal 1° gennaio. Il corpo permanente, composto da 10 000 funzionari Frontex e nazionali, rafforzerà in misura significativa la sicurezza delle frontiere, crescendo gradualmente nei prossimi anni fino a raggiungere la sua piena capacità. Il regolamento di esecuzione sul sistema europeo di sorveglianza delle frontiere (EUROSUR) di recente adozione[125] promuoverà l'ulteriore miglioramento della conoscenza situazionale e

[123] COM(2020) 778, SWD(2020) 378 del 21 dicembre 2020.
[124] COM(2021) 277.
[125] Regolamento di esecuzione (UE) 2021/581 della Commissione.

l'aumento della capacità di reazione alle frontiere esterne allo scopo di accertare, prevenire e combattere l'immigrazione clandestina e la criminalità transfrontaliera.

Controlli doganali
La Commissione sta preparando una nuova strategia per la gestione dei rischi doganali intesa a promuovere l'approccio strutturato alla gestione dei rischi doganali, aumentando l'efficacia dei controlli e riducendo i rischi per l'UE e i suoi cittadini, pur garantendo la competitività delle imprese legittime dell'UE.

Nel quadro della strategia e del piano d'azione dell'UE per il rafforzamento della gestione dei rischi doganali, la Commissione sta sviluppando anche il nuovo sistema doganale avanzato per la gestione del rischio del carico, che consente un'analisi collaborativa del rischio per la sicurezza prima che le merci arrivino nell'UE o siano caricate per il trasporto nell'UE[126].

3. Rafforzare la ricerca e l'innovazione in materia di sicurezza

L'innovazione dovrebbe essere considerata uno strumento strategico per l'UE: produce effetti orizzontali su quasi tutti gli aspetti della comunità della sicurezza, offrendo nuovi modi per affrontare i problemi sollevati dalle tecnologie, riducendo la dipendenza strategica e rafforzando le catene di approvvigionamento. Per questo motivo l'UE tiene conto della dimensione della sicurezza, delle sue esigenze e del ruolo del settore privato nel definire i suoi principali progetti di ricerca.

Il **polo europeo dell'innovazione per la sicurezza interna** è in fase di sviluppo. Il programma **Orizzonte Europa** sostiene le risposte dell'UE alle sfide per la sicurezza, fornendo 1,6 miliardi di EUR di finanziamenti per il 2021-2027. Nel marzo 2021 la Commissione ha adottato il primo piano strategico Orizzonte Europa, definendo gli orientamenti strategici per i primi quattro anni: la ricerca in materia di sicurezza servirà come strumento per passare da un approccio reattivo nel campo della sicurezza a un approccio proattivo, basato su previsioni e prevenzione. È stato concordato un nuovo programma di lavoro 2021-2022 che sosterrà l'attuazione della dimensione della sicurezza interna della strategia per l'Unione della sicurezza, nonché la gestione delle frontiere e la dimensione della sicurezza delle politiche in materia di immigrazione e asilo e le politiche dell'UE volte alla riduzione del rischio di catastrofi.

Il finanziamento dell'UE presenta ulteriori opportunità per rafforzare l'innovazione europea nell'interfaccia tra le applicazioni nella difesa e nei settori spaziale e civile. Nel febbraio 2021 la Commissione ha varato il piano d'azione sulle sinergie tra **l'industria civile, della difesa e dello spazio**[127]. Sono stati individuati tre progetti principali (tecnologie dei droni, connettività spaziale sicura e gestione del traffico spaziale). Il piano d'azione sosterrà le industrie della sicurezza dell'UE con soluzioni moderne e innovative derivanti dal reciproco arricchimento e da sinergie efficienti tra l'industria civile, della difesa e dello spazio.

[126] La versione 1, riguardante le spedizioni espresso per via aerea e postali, è disponibile da marzo. La versione 2, riguardante il carico aereo generale, è prevista per marzo 2023. La versione 3, che comprende il trasporto marittimo, stradale e ferroviario, è prevista per il 2024.
[127] COM(2021) 70.

Le tecnologie, i dati e i servizi spaziali sono diventati indispensabili per la sicurezza degli europei e svolgono un ruolo fondamentale per la tutela di diversi interessi strategici. Il **regolamento sul programma spaziale**[128], adottato ad aprile con un bilancio di 14,6 miliardi di EUR, introduce una nuova componente per le comunicazioni satellitari governative, offrendo la base di partenza per una connettività spaziale sicura dell'UE.

4. Competenze e sensibilizzazione

La consapevolezza delle minacce per la sicurezza e le competenze necessarie per affrontarle sono essenziali per costruire una società più resiliente nella quale le imprese, le amministrazioni e i singoli siano preparati meglio. Il 9 febbraio 2021 si è tenuta la 18ª giornata "Per un internet più sicuro", mediante collegamento online in 170 paesi con i giovani ambasciatori di "Internet migliore per i ragazzi" e rappresentanti dell'alleanza dell'industria. Il piano d'azione dell'UE per l'istruzione digitale (2021-2027) comprende un'azione dedicata ad aiutare insegnanti ed educatori a promuovere l'alfabetizzazione digitale e a contrastare la disinformazione. Saranno messi a punto orientamenti da diffondere in tutta l'UE nel settembre 2022.

Una buona conoscenza dell'ambiente digitale e lo sviluppo delle relative competenze nel settore pubblico e privato è fondamentale per una società resiliente e competitiva. Nell'ambito del programma Europa digitale, un primo bando per i poli europei dell'innovazione (EDIH)[129] è stato pubblicato a maggio, con l'obiettivo di disporre di primi poli operativi dall'inizio del 2022. Gli EDIH assisteranno attori privati e pubblici fornendo l'accesso a competenze e sperimentazioni tecniche, stimolando l'ampia diffusione dell'intelligenza artificiale, del calcolo ad alte prestazioni (HPC) e della cibersicurezza, nonché altre tecnologie digitali da parte dell'industria (in particolare PMI e imprese a media capitalizzazione) e di organizzazioni del settore pubblico in Europa.

In un panorama della sicurezza in costante evoluzione, occorre che le competenze dei funzionari delle autorità di contrasto e dei professionisti della giustizia siano costantemente aggiornate. Una valutazione di **CEPOL** si concluderà nel secondo semestre del 2021. La Commissione ha adottato la strategia europea di formazione giudiziaria per il periodo 2021-2024[130] alla fine del 2020 e ha organizzato una conferenza di portatori di interessi per promuovere la formazione di giudici e pubblici ministeri nel maggio 2021, sotto la Presidenza portoghese.

La sensibilizzazione è anche al centro della strategia dell'UE sui **diritti delle vittime** (2020-2025), adottata nel giugno 2020, intesa a garantire che tutte le vittime di reato, indipendentemente dalla loro ubicazione nell'UE o dalle circostanze del reato, possano contare pienamente sui propri diritti. La prima riunione plenaria della piattaforma per i diritti delle vittime si è tenuta nel febbraio 2021. La Commissione sta lavorando anche sulla valutazione della direttiva sui diritti delle vittime e, se del caso, proporrà modifiche legislative nel 2022.

---

[128] Regolamento (UE) 2021/696, del 28 aprile 2021, che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale.

[129] https://digital-strategy.ec.europa.eu/en/activities/edihs.

[130] COM(2020) 713.

5. Il ruolo delle agenzie dell'UE

La strategia per l'Unione della sicurezza si basa su un approccio esteso all'intera società, coinvolgendo tutte le istituzioni, le organizzazioni e le autorità che svolgono un ruolo nella protezione dei cittadini. Oltre a fornire sostegno e competenze agli Stati membri, le agenzie dell'UE svolgono un ruolo fondamentale nella promozione della cooperazione e dello scambio di informazioni tra le autorità nazionali degli Stati membri a livello operativo. In considerazione della molteplicità di minacce nuove ed emergenti nell'attuale panorama, occorre incoraggiare ulteriormente le sinergie e il coordinamento delle attività delle agenzie dell'UE.

Europol
Le relazioni annuali di Europol in materia di criminalità organizzata (SOCTA), terrorismo (TE-SAT) e criminalità organizzata su Internet (IOCTA) forniscono dati e analisi fondamentali a sostegno delle attività politiche e operative nell'ambito della sicurezza. Anche Europol contribuisce a potenziare l'efficacia operativa generale delle autorità di contrasto, ampliando la cooperazione con i paesi terzi per contrastare la criminalità e il terrorismo, coerentemente con altre politiche e strumenti esterni dell'UE.

Il centro operativo e di analisi è il polo informativo di Europol. Il centro controlla operazioni e sviluppi 24 ore su 24 e 7 giorni su 7, promuove la cooperazione con paesi e organizzazioni non appartenenti all'UE e impiega esperti sul campo, oltre a fornire analisi ad altri centri e organizzazioni di Europol. Il Centro Europol per la criminalità organizzata e le forme gravi di criminalità sostiene i paesi dell'UE nella lotta contro le reti criminali internazionali coinvolte nel traffico di stupefacenti, armi ed esplosivi, reati contro il patrimonio e crimini ambientali. Il Centro ospita anche il Centro europeo contro il traffico di migranti, che mira a smantellare le reti criminali complesse e sofisticate coinvolte nella tratta di migranti. Il Centro europeo per la criminalità economica e finanziaria di Europol invece ha il compito di fornire sostegno nel trattare casi altamente sofisticati di riciclaggio di denaro, truffe e frodi, che colpiscono i cittadini, le imprese e il settore pubblico.

Il contributo di Europol è fondamentale anche per il coordinamento dell'approccio dell'UE in materia di lotta al terrorismo. Europol ha continuato a sostenere gli Stati membri nelle indagini connesse al terrorismo attraverso il Centro europeo antiterrorismo (ECTC). Malgrado le restrizioni causate dalla pandemia, nel 2020 l'ECTC ha fornito sostegno a 776 operazioni antiterrorismo (rispetto a 632 nel 2019). Anche l'unità UE addetta alle segnalazioni su Internet di Europol ha continuato a svolgere un ruolo cruciale nel monitorare l'attività dei gruppi terroristici online e le azioni intraprese dalle piattaforme, nonché nell'ulteriore sviluppo del protocollo di risposta alle crisi dell'UE. Europol resta impegnata a sostenere gli Stati membri nell'ampliamento delle loro capacità nazionali per la prevenzione della diffusione di contenuti terroristici online, con l'organizzazione di giornate di azione dedicate alle segnalazioni mirate (Targeted Referral Action Days).

Eurojust

Nei primi mesi del 2021 Eurojust ha sostenuto numerose indagini e azioni penali transfrontaliere contro gruppi della criminalità organizzata specializzati in frodi e ha provveduto anche al sequestro dei beni di società o alla chiusura amministrativa di imprese utilizzate per il sistema di frode[131].

Eurojust ha sostenuto importanti operazioni congiunte a livello internazionale per lo smantellamento di reti di criminalità informatica, anche nei confronti di gruppi criminali che gestivano un'applicazione mobile interpiattaforma denominata Mobdro che agevolava lo streaming di opere audiovisive ottenute illegalmente, tra cui partite di calcio[132], o uno dei software maligni più pericolosi (EMOTET) utilizzato per accedere ai computer delle vittime e consentire a terzi di infettarli[133]. Eurojust ha anche collaborato con operatori giudiziari per la mappatura delle sfide giuridiche e operative da affrontare per indagare e perseguire reati commessi da estremisti di destra, gruppi terroristici e soggetti che agiscono da soli, oltre a facilitare la condivisione di esperienze[134].

Cooperazione tra agenzie

A livello operativo, il 23 dicembre 2020 Europol ed Eurojust hanno sottoscritto un accordo di contributo[135] per ampliare il loro partenariato a sostegno delle autorità di contrasto e giudiziarie con l'accesso transfrontaliero a prove elettroniche. Eurojust ed Europol hanno anche firmato accordi operativi bilaterali con l'**EPPO** per disciplinare i loro rapporti futuri e garantire una stretta cooperazione intesa a proteggere meglio gli interessi finanziari dell'Unione all'interno e al di là delle frontiere dell'UE. Grazie alla stretta cooperazione tra Europol, Eurojust e la rete giudiziaria europea, il progetto SIRIUS[136] sostiene la comunità giudiziaria e delle autorità di contrasto dell'UE fornendo materiale di formazione e orientamenti per migliorare la cooperazione (principalmente UE-USA) in materia di accesso transfrontaliero alle informazioni elettroniche. A marzo Eurojust e l'Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO) hanno concordato di instaurare una cooperazione più stretta per la lotta alla contraffazione e alla pirateria online[137]. Questo nuovo accordo segna una nuova era di cooperazione tra Eurojust, Europol ed EUIPO, poiché consentirà un sostegno efficace durante l'intero ciclo di vita dei casi, dalla denuncia penale al verdetto giudiziario.

ENISA

ENISA ha attuato il quadro per la **cooperazione strutturata con CERT-UE**[138] al fine di sfruttare le sinergie ed evitare duplicazioni di attività nell'esecuzione dei suoi compiti nell'ambito della cooperazione operativa, sulla base di un protocollo d'intesa firmato a marzo. Il risultato sarà un aumento dell'efficacia ed efficienza del meccanismo di risposta dell'UE e dello sviluppo di capacità a lungo termine, con il sostegno di un ufficio locale dell'agenzia a

---

131 https://www.eurojust.europa.eu/action-counter-italian-fuel-tax-fraud-worth-almost-eur-1-billion.

132 https://www.eurojust.europa.eu/eurojust-supports-spanish-action-against-illegal-streaming-football-matches.

133 https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action.

134 https://www.eurojust.europa.eu/eurojust-expert-workshops-violent-right-wing-extremism-and-terrorism.

135 Europol coopera con Eurojust nel progetto SIRIUS, che include una piattaforma interattiva di condivisione delle conoscenze accessibile alle autorità di contrasto e giudiziarie e mira a produrre e diffondere materiale di formazione e orientamenti per migliorare la cooperazione (principalmente UE-USA) in materia di accesso transfrontaliero alle informazioni elettroniche.

136 https://www.europol.europa.eu/activities-services/sirius-project.

137 https://www.eurojust.europa.eu/stepping-cooperation-tackle-intellectual-property-crime.

138 La squadra di pronto intervento informatico per le istituzioni, gli organismi e le agenzie dell'UE (CERT-UE) è composta da esperti di sicurezza informatica delle principali istituzioni dell'UE.

Bruxelles, studiato per promuovere la cooperazione con altre istituzioni, agenzie e organismi dell'UE[139]. ENISA sta contribuendo alla realizzazione di misure concrete per attuare nuove politiche in materia di cibersicurezza. A maggio ha trasmesso la prima proposta di sistema di certificazione della cibersicurezza basata su criteri comuni[140], mentre a giugno ha avviato il processo per istituire un gruppo di lavoro ad hoc sulla certificazione di cibersicurezza per il 5G[141].

Agenzia europea della guardia di frontiera e costiera (Frontex)
Frontex svolge un ruolo cruciale per sostenere gli Stati membri nella gestione delle frontiere esterne e dei rimpatri, contribuendo alla sicurezza dell'UE. Con il nuovo regolamento[142], Frontex è diventata la maggiore agenzia dell'UE in termini di personale e risorse finanziarie.

Osservatorio europeo delle droghe e delle tossicodipendenze
L'osservatorio europeo delle droghe e delle tossicodipendenze (EMCDDA) svolge un ruolo importante, garantendo il monitoraggio costante della situazione delle droghe nell'UE per fornire alle istituzioni dell'UE e agli Stati membri informazioni il più possibile aggiornate. L'attività recente si è concentrata nello specifico sull'impatto della pandemia per quanto riguarda i mercati, il consumo e i danni delle droghe, nonché i servizi per le tossicodipendenze[143].

VI. Conclusioni

L'UE ha una capacità unica di rispondere alle minacce e alle sfide attuali alla sicurezza e si sta gradualmente attrezzando per rafforzare la sua risposta. La strategia per l'Unione della sicurezza, con il suo approccio globale e dinamico, tende a smantellare i compartimenti stagni, per garantire che ciascun rischio sia compreso nel contesto del panorama generale delle minacce, che la competenza di tutti i portatori di interessi contribuisca alla costruzione di un'UE più sicura e resiliente e che tutti gli strumenti a nostra disposizione siano impiegati in modo efficace in linea con i valori europei e nel rispetto dei diritti fondamentali.

La Commissione intende sostenere il Parlamento europeo e il Consiglio nel completare gli importanti strumenti normativi ancora da adottare in materia di sicurezza, assicurandosi che il livello di ambizione corrisponda alle sfide attuali e future dell'UE.

Nello sforzo di affrontare le sfide per la sicurezza a livello mondiale e di rafforzare i legami con i paesi che condividono gli stessi principi, l'UE intensificherà anche la cooperazione con i partner internazionali in settori quali la lotta al terrorismo e all'estremismo, le attività informatiche dolose, le minacce ibride e altri rischi condivisi per la sicurezza. Questa intenzione si riflette anche nella dichiarazione concordata al recente vertice UE-USA[144].

---

[139] C(2021) 4626.
[140] Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission — ENISA (europa.eu).
[141] Calling on you, 5G Experts! Join us on 5G Cybersecurity Certification — ENISA (europa.eu).
[142] Regolamento (UE) 2019/1896.
[143] Relazione europea sulla droga 2021 dell'EMCDDA del 9 giugno 2021.
[144] Dichiarazione al vertice UE-USA: verso un partenariato transatlantico rinnovato del 15 giugno 2021.

L'aggiornamento e l'adeguamento del quadro legislativo dell'UE per affrontare le varie dimensioni della sicurezza stanno progredendo a un ritmo costante, ma è necessario che le normative siano attuate correttamente. Nell'ambito di questa responsabilità comune, ogni Stato membro ha un ruolo da svolgere per garantire la sicurezza dell'Europa nel suo complesso.