Consiglio dell'Unione europea

Bruxelles, 3 aprile 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	2 aprile 2025
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2025) 148 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI ProtectEU: strategia europea di sicurezza interna

Si trasmette in allegato, per le delegazioni, il documento COM(2025) 148 final.

All.: COM(2025) 148 final

COMMISSIONE
EUROPEA

Strasburgo, 1.4.2025
COM(2025) 148 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

ProtectEU: strategia europea di sicurezza interna

1. ProtectEU: strategia europea di sicurezza interna

La sicurezza è il fondamento di tutte le nostre libertà. La democrazia, lo Stato di diritto, i diritti fondamentali, il benessere dei cittadini europei, la competitività e la prosperità dipendono tutti dalla nostra capacità di garantire le basi della sicurezza. Oggi più che mai, in questa nuova epoca densa di minacce alla sicurezza in cui ci troviamo a vivere, la capacità degli Stati membri dell'Unione di garantire la sicurezza dei propri cittadini presuppone un **approccio europeo unitario alla difesa della sicurezza interna**. Nell'evoluzione del panorama geopolitico l'Europa deve rimanere fedele alla sua perenne promessa di pace.

I primi passi nella costruzione di un apparato di sicurezza europeo sono già stati compiuti. Negli ultimi dieci anni abbiamo perfezionato i meccanismi d'azione collettivi dell'Unione nei settori della cooperazione delle autorità di contrasto e giudiziarie, della sicurezza delle frontiere, della lotta alla criminalità organizzata e alle forme gravi di criminalità, della lotta al terrorismo e all'estremismo violento e della protezione delle infrastrutture critiche fisiche e digitali dell'UE. La corretta attuazione della legislazione adottata in precedenza e delle politiche già elaborate rimane un elemento fondamentale.

La natura delle minacce odierne e il nesso intrinseco tra la sicurezza interna ed esterna dell'UE ci impongono un ulteriore sforzo.

Il quadro delle minacce è preoccupante. Il confine tra **minacce ibride** e guerra aperta è sfumato e confuso. La Russia sta conducendo una campagna ibrida online e offline contro l'UE e i suoi partner, per disarticolare e minare la coesione sociale e i processi democratici e per mettere alla prova la solidarietà dell'Unione nei confronti dell'Ucraina. Stati stranieri ostili e attori sponsorizzati da Stati cercano di infiltrarsi nelle infrastrutture critiche e nelle catene di approvvigionamento dell'Unione per perturbarle, appropriandosi di dati sensibili e conquistando una posizione che consenta loro in futuro di arrecare i danni più gravi. Questi soggetti utilizzano la criminalità come servizio e i criminali come mandatari. La dipendenza da paesi terzi per le catene di approvvigionamento aggrava la vulnerabilità dell'Unione di fronte alle campagne ibride condotte da Stati ostili.

In Europa proliferano potenti **reti della criminalità organizzata**; alimentate online, si diffondono nell'economia e colpiscono la società, come si illustra nella valutazione, da parte dell'Unione europea, della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA) presentata di recente da Europol[1]. Quando la criminalità organizzata si radica in una comunità o in un settore economico, la battaglia per eliminarla diventa assai ardua: un terzo delle reti criminali più temibili opera da oltre dieci anni. Queste organizzazioni sfruttano le criptovalute e i sistemi finanziari paralleli per riciclare e occultare i proventi dei loro reati.

Sull'**Europa continua a incombere la minaccia del terrorismo.** Le crisi regionali originate al di fuori dell'UE creano un effetto domino e offrono ai gruppi terroristici di ogni tendenza ideologica nuove occasioni per reclutare persone, mobilitare o sviluppare le proprie capacità. Costoro rivolgono gli sforzi di radicalizzazione e reclutamento specificamente alle fasce più vulnerabili delle nostre società, mirando in particolare ad alcuni segmenti della gioventù. Ispirano l'azione di "lupi solitari" e fomentano impennate di estremismo antisistemico, miranti a travolgere l'ordinamento giuridico democratico.

Il rapidissimo avanzare del **progresso tecnologico** offre strumenti essenziali per migliorare l'apparato di sicurezza. Gli attacchi informatici e la manipolazione delle informazioni da parte di attori stranieri costituiscono però un fenomeno sempre più diffuso, che sfrutta nuove

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

tecnologie come l'intelligenza artificiale. Bambini, giovani e anziani corrono rischi particolarmente gravi nelle attività online, mentre la diffusione dell'odio online minaccia la libertà di espressione e la coesione sociale.

La vita è divenuta meno sicura e questa sensazione si diffonde sempre più tra i cittadini europei, la cui **percezione della sicurezza nell'UE** si è erosa al punto che il 64 percento dei cittadini interrogati sul futuro manifesta preoccupazione per la sicurezza nell'UE[2]. Anche le imprese sono sempre più preoccupate; la disinformazione volontaria e involontaria, la criminalità, le attività illecite e lo spionaggio informatico figurano tutti tra i dieci rischi più gravi individuati nella "World Economic Forum Global Risks Report 2025"[3].

Gli europei dovrebbero essere **in grado di vivere liberi dalla paura** per strada, a casa, nei luoghi pubblici, sulla metropolitana o su internet. La protezione delle persone, in particolare di quelle più vulnerabili agli attacchi che tendenzialmente colpiscono in modo sproporzionato bambini, donne e minoranze, tra cui le comunità ebraiche e musulmane, è un elemento fondamentale dell'operato dell'UE in materia di sicurezza ed è essenziale per costruire società resilienti e coese.

La Commissione definisce una **strategia europea di sicurezza interna** per contrastare in maniera più adeguata le minacce negli anni a venire. Grazie a un pacchetto di strumenti giuridici più incisivo, a una cooperazione più intensa e a una maggiore condivisione delle informazioni, rafforzeremo la resilienza e la capacità collettiva di anticipare, prevenire e individuare le minacce alla sicurezza per rispondervi efficacemente. Un approccio unitario alla sicurezza interna consentirà agli Stati membri di sfruttare il potere della tecnologia per rafforzare - e non indebolire - la sicurezza, promuovendo nel contempo uno spazio digitale sicuro per tutti. Tale approccio favorisce inoltre una risposta comune degli Stati membri ai mutamenti politici ed economici a livello mondiale che si ripercuotono sulla sicurezza interna dell'Unione.

Questa strategia è guidata da **tre principi** e si fonda su un elemento essenziale: il rispetto dello Stato di diritto e dei diritti fondamentali.

In primo luogo definisce l'ambizione di introdurre un cambiamento culturale in materia di sicurezza. Abbiamo bisogno di un **approccio esteso a tutta la società** che coinvolga tutti i cittadini e i portatori di interessi, tra cui la società civile, la comunità della ricerca, il mondo accademico e i soggetti privati. Le azioni previste dalla strategia adottano pertanto ove possibile un approccio integrato e multilaterale.

In secondo luogo **occorre integrare le considerazioni relative alla sicurezza in tutta la legislazione, le politiche e i programmi dell'Unione**, compresa l'azione esterna dell'UE. Sarà necessario elaborare, rivedere e attuare legislazione, politiche e programmi alla luce di una prospettiva di sicurezza, assicurando che non siano trascurate le necessarie considerazioni in materia di sicurezza in modo da promuovere un approccio coerente e globale alla sicurezza stessa.

Un'Europa sicura e resiliente esige infine **ingenti investimenti da parte dell'UE, degli Stati membri e del settore privato**. Le priorità e le azioni delineate nella presente strategia richiedono risorse umane e finanziarie sufficienti per garantirne l'attuazione. Come si illustra nella comunicazione sulla strada verso il prossimo quadro finanziario pluriennale[4], l'Europa

[2] Indagine Eurobarometro Flash FL550: EU Challenges and Priorities.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, pag.17.
[4] COM (2025) 46 final.

dovrà accrescere la spesa pubblica per la sicurezza e promuovere la ricerca e gli investimenti in materia di sicurezza, rafforzando la propria autonomia strategica.

La presente strategia integra la **strategia europea per l'Unione della preparazione**[5], che definisce un approccio multirischio integrato per la preparazione a conflitti, calamità naturali e provocate dall'uomo e crisi, e il **Libro bianco sulla prontezza alla difesa europea per il 2030**[6], che promuove lo sviluppo e l'acquisizione di capacità di difesa in tutta l'UE per scoraggiare gli avversari stranieri. La Commissione proporrà inoltre uno **scudo europeo per la democrazia** volto a rafforzare la resilienza democratica nell'Unione. Nel loro insieme queste iniziative delineano una visione per un'Unione sicura e resiliente.

Nuova governance europea nella sicurezza interna

La Commissione collaborerà strettamente con gli Stati membri e gli organismi dell'UE per migliorare l'approccio dell'Unione alla sicurezza interna, a livello sia strategico che operativo.

Questo obiettivo sarà raggiunto:

- **individuando in maniera coerente, fin dall'inizio e nel corso dell'intero processo negoziale, le potenziali implicazioni delle iniziative nuove e rivedute della Commissione in termini di sicurezza e preparazione;**
- **tenendo riunioni periodiche del gruppo di progetto della Commissione sulla sicurezza interna europea, coadiuvate da una collaborazione strategica intersettoriale in tutta la Commissione;**
- **presentando le analisi delle minacce alla sicurezza interna a sostegno dei lavori dell'Accademia di sicurezza;**
- **avviando discussioni con gli Stati membri in sede di Consiglio sull'evoluzione delle sfide in materia di sicurezza interna in base all'analisi delle minacce e a uno scambio di opinioni sulle priorità politiche fondamentali;**
- **prevedendo relazioni periodiche al Parlamento europeo e al Consiglio per monitorare e sostenere l'attuazione sistematica delle iniziative fondamentali in materia di sicurezza.**

2. Conoscenza e analisi integrate della situazione e delle minacce

Doteremo l'Unione di nuovi strumenti per condividere e combinare le informazioni e formulare un'analisi periodica delle minacce alla sicurezza interna dell'UE, contribuendo a una valutazione completa dei rischi e delle minacce.

La sicurezza inizia con un'**anticipazione efficace**. L'UE deve basarsi su una conoscenza e un'analisi complete, sufficientemente autonome e aggiornate della situazione e delle minacce. L'intelligence utilizzabile, che gli Stati membri sono incoraggiati a rafforzare ulteriormente attraverso la capacità unica di analisi dell'intelligence (SIAC), quale punto di accesso unico per l'intelligence degli Stati membri, svolge un ruolo essenziale per valutare e contrastare le minacce, e in ultima analisi orientare l'azione politica e legislativa[7]. Dobbiamo sfruttare in

[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.
[7] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness, pag. 23.

maniera più efficace e collaborativa a livello di Unione l'**analisi basata sull'intelligence** e le **valutazioni delle minacce**.

Sulla base delle varie valutazioni dei rischi e delle minacce formulate a livello di Unione e per settori specifici[8], la Commissione preparerà **analisi periodiche delle minacce alla sicurezza interna dell'UE** per individuare le principali sfide in materia di sicurezza, allo scopo di orientare le priorità politiche. Queste analisi serviranno a sviluppare una politica di sicurezza interna agile e reattiva, che faccia efficacemente fronte alle minacce in evoluzione, protegga meglio i cittadini e le imprese dagli attacchi e consenta di effettuare tempestivamente interventi strategici mirati. Tali analisi delle minacce alla sicurezza interna dell'UE contribuiranno anche alla **valutazione completa (ossia intersettoriale e multirischio) dei rischi e delle minacce a livello di Unione** messa a punto dalla Commissione e dall'alto rappresentante, come si illustra nella strategia per l'Unione della preparazione.

La fiducia e la sicurezza nel trattamento sono essenziali per la condivisione delle informazioni; a tale scopo occorrono infrastrutture affidabili e sicure. Le istituzioni, gli organi e gli organismi dell'UE devono garantire la capacità di utilizzare **canali di comunicazione sicuri** per lo scambio di informazioni sensibili e classificate, tra loro e con gli Stati membri. Gli investimenti in **sistemi interoperabili sicuri** e tecnologia affidabile rafforzeranno l'autonomia dell'UE e ne potenzieranno la capacità di gestire le crisi e assicurare la resilienza operativa. In tale contesto la Commissione esorta i colegislatori a concludere i negoziati relativi alla **proposta di regolamento sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione**, in particolare allo scopo di garantire un quadro comune per il trattamento delle informazioni sensibili non classificate e classificate[9].

Per garantirsi sicurezza operativa e conoscenza della situazione, la Commissione riesaminerà il proprio quadro istituzionale di governance della sicurezza e costituirà un **centro operativo di sicurezza integrato (ISOC)** per proteggere le persone, i beni materiali e le operazioni in tutti i siti della Commissione. La Commissione rafforzerà le proprie capacità operative e analitiche per individuare e attenuare le minacce ibride.

In linea con la strategia per l'Unione della preparazione, gli aspetti della preparazione e della sicurezza saranno integrati sistematicamente nella normativa, nelle politiche e nei programmi dell'UE. In fase di elaborazione o di revisione della normativa, delle politiche o dei programmi in una prospettiva di preparazione e sicurezza, la Commissione indicherà sistematicamente gli effetti potenziali dell'opzione strategica prescelta sulla preparazione e sulla sicurezza. Il processo si baserà sulla formazione periodica dei responsabili politici della Commissione.

Per coadiuvare gli Stati membri la Commissione discuterà con il Consiglio l'evoluzione delle sfide in materia di sicurezza interna e le principali priorità politiche, aggiornando periodicamente il Consiglio in merito all'attuazione della strategia. La Commissione inoltre informerà il Parlamento europeo e i portatori di interessi, coinvolgendoli in tutte le azioni pertinenti.

[8] Le valutazioni settoriali delle minacce che contribuiranno a orientare tale analisi delle minacce comprendono la valutazione, da parte dell'Unione, della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA), la relazione sulla situazione e sulle tendenze del terrorismo nell'UE (TE-SAT), la relazione congiunta di valutazione informatica (JCAR) e le valutazioni delle minacce, dei rischi e dei metodi di riciclaggio di denaro e di finanziamento del terrorismo che la Commissione e l'Autorità per la lotta al riciclaggio dovranno effettuare in futuro.

[9] COM (2022)119 final.

Azioni fondamentali

La Commissione intende:

- **elaborare e presentare analisi periodiche delle minacce per le sfide in materia di sicurezza interna dell'UE.**

Gli Stati membri sono esortati a:

- **migliorare la condivisione di intelligence con la SIAC e assicurare una migliore condivisione delle informazioni con gli organi e gli organismi dell'UE.**

Il Parlamento europeo e il Consiglio sono incoraggiati a:

- **concludere i negoziati sulla proposta di regolamento sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione.**

3. Rafforzamento delle capacità di sicurezza dell'UE

Svilupperemo nuovi strumenti per le attività di contrasto, come il rinnovamento di Europol, e mezzi migliori per coordinare e garantire lo scambio sicuro di dati e l'accesso legittimo ai dati.

Per contrastare efficacemente l'evolversi delle minacce, l'UE deve rafforzare le capacità di sicurezza e promuovere l'innovazione. Le autorità di contrasto e giudiziarie, che sono gli attori principali nella lotta alle minacce per la sicurezza interna, hanno bisogno di capacità e strumenti operativi idonei che consentano di agire con tempestiva efficacia. Per prevenire, individuare, indagare e perseguire in modo efficiente, è importante che tali autorità siano in grado di comunicare e coordinarsi a livello transfrontaliero e interservizi.

Organi e organismi dell'UE per la sicurezza interna

Nell'architettura di sicurezza dell'UE gli organi e gli organismi dell'Unione attivi nei settori della giustizia, degli affari interni e della cibersicurezza svolgono un ruolo fondamentale, che continua ad estendersi con il progressivo ampliamento delle loro competenze.

A 25 anni dall'istituzione **Europol** rappresenta oggi più che mai un elemento fondamentale per il quadro di sicurezza dell'UE. Collabora a indagini transfrontaliere complesse, favorisce lo scambio di informazioni, sviluppa strumenti innovativi per le attività di polizia e offre competenze avanzate per le attività di contrasto. Diversi fattori impediscono però a Europol di realizzare pienamente il proprio potenziale operativo nel sostegno alle attività investigative e operative volte a contrastare la criminalità transfrontaliera: tali fattori variano dall'insufficiente livello di risorse al fatto che l'attuale mandato non comprende le nuove minacce alla sicurezza, come il sabotaggio, le minacce ibride o la manipolazione delle informazioni. Per questo motivo la Commissione proporrà **una revisione ambiziosa del mandato di Europol** che la trasformi in una forza di polizia realmente operativa, in grado di sostenere con maggiore efficacia gli Stati membri. L'obiettivo è quello di potenziare le competenze tecnologiche e la capacità di Europol di sostenere le autorità di contrasto nazionali, migliorare il coordinamento con altri organi e organismi e con gli Stati membri, rafforzare i partenariati strategici con i paesi partner e il settore privato e assicurare un controllo rafforzato di Europol.

La Commissione si adopererà inoltre per **migliorare ulteriormente l'efficacia e la complementarità degli organi e organismi dell'UE per la sicurezza interna e per potenziare una cooperazione fluida** tra di loro.

Il mandato di **Eurojust** sarà valutato e rafforzato per rendere più efficace la cooperazione giudiziaria, potenziando la complementarità e la cooperazione con Europol. In questo contesto rientra il miglioramento dell'efficienza di Eurojust e della sua capacità di offrire un contributo

proattivo di sostegno e analisi alle autorità giudiziarie degli Stati membri. Poiché la competenza a indagare e perseguire i reati che ledono gli interessi finanziari dell'Unione spetta esclusivamente all'**EPPO**, la Commissione valuterà i metodi più opportuni per migliorare la capacità dell'EPPO di proteggere i fondi dell'Unione. Rientrerà in questo quadro il rafforzamento della cooperazione tra l'EPPO ed Europol.

Uno scambio di informazioni efficiente e sicuro tra organismi è essenziale per la cooperazione. Europol e Frontex necessitano di un rapido scambio reciproco di informazioni, anche a fini operativi, per dare seguito alla dichiarazione comune del gennaio 2024[10]. **eu-LISA** assolve una funzione fondamentale per la conservazione sicura e la disponibilità dei dati ai fini di un migliore coordinamento e di uno scambio di informazioni più efficiente tra gli organismi. L' **Agenzia dell'Unione europea per i diritti fondamentali** svolge opera di consulenza per la tutela dei diritti fondamentali nello sviluppo e nell'attuazione delle politiche di sicurezza.

All'**Autorità dell'UE per la lotta al riciclaggio (AMLA)** è stato conferito il potere di effettuare, sulla base di un riscontro positivo o negativo, la corrispondenza incrociata delle informazioni con quelle messe a disposizione da Europol, dall'EPPO, da Eurojust e dall'Ufficio europeo per la lotta antifrode al fine di svolgere analisi comuni dei casi transfrontalieri.

L'**ENISA** svolge un ruolo centrale nell'attuazione della legislazione europea in materia di cibersicurezza. Nella prossima **revisione del regolamento sulla cibersicurezza** la Commissione ne valuterà il mandato e proporrà di modernizzarlo per rafforzare il valore aggiunto dell'agenzia per l'UE.

La cooperazione tra le autorità doganali e le altre autorità di contrasto si intensificherà con la proposta creazione dell'**autorità doganale dell'UE** e del **centro doganale digitale dell'UE** nel quadro del pacchetto di riforma doganale dell'Unione. Le informazioni provenienti dal futuro centro e i relativi dati forniti da Europol, Eurojust, EPPO, OLAF, AMLA e Frontex, nell'ambito delle rispettive competenze, rafforzeranno l'analisi comune e contribuiranno a rendere più coerenti le attività operative, in particolare alle frontiere esterne. La Commissione incoraggia i colegislatori a portare rapidamente a termine i negoziati sulla riforma doganale dell'UE, e continuerà ad assisterli a tal fine.

Il rafforzamento della complementarità tra EPPO, OLAF, Europol, Eurojust, AMLA e la proposta autorità doganale dell'UE si baserà anche sui risultati della revisione dell'**architettura antifrode dell'UE** attualmente in corso. La sicurezza interna può trarre vantaggio da questo approccio olistico, concentrandosi su un migliore utilizzo dei mezzi sia penali che amministrativi, sull'interoperabilità dei sistemi informatici e su una migliore cooperazione.

Comunicazione critica

Attualmente nella maggior parte dei casi i **sistemi di comunicazione critica**[11] sono gestiti separatamente a livello nazionale. Ciò significa che spesso gli operatori di primo intervento non possono comunicare con i propri omologhi quando attraversano le frontiere per entrare in altri Stati membri. In alcuni Stati membri vi sono anche limitazioni alle comunicazioni tra diverse categorie di operatori di primo intervento (ad esempio polizia e ambulanze). Le norme della maggior parte dei sistemi non soddisfano gli attuali requisiti di funzionalità e resilienza: ciò limita sensibilmente la capacità di reazione degli operatori di primo intervento, in particolare a livello transfrontaliero.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

[11] Ossia le reti utilizzate dalle autorità di contrasto, dalle guardie di frontiera, dalle autorità doganali, dalla protezione civile, dai vigili del fuoco, dagli operatori sanitari di emergenza e da altri attori chiave per la sicurezza pubblica.

Per migliorare la capacità dell'UE di reagire alle crisi, la Commissione proporrà una legislazione volta a istituire un **sistema europeo di comunicazione critica (EUCCS)** al fine di collegare i sistemi di comunicazione critica di prossima generazione negli Stati membri dell'UE. L'obiettivo è quello di fondare l'EUCCS su tre pilastri strategici: mobilità operativa, forte resilienza e autonomia strategica. L'iniziativa EUCCS stabilirà requisiti armonizzati e contribuirà a modernizzare i sistemi di comunicazione critica degli Stati membri, consentendo loro di funzionare senza soluzione di continuità. Estenderà inoltre la copertura del sistema attraverso il futuro sistema multiorbitale IRIS^{2} [12]. I progetti finanziati dall'UE svilupperanno le capacità tecniche dell'EUCCS, facendo ricorso principalmente a fornitori europei di tecnologie, al fine di promuovere l'autonomia strategica dell'Unione in questo settore sensibile.

Accesso legittimo ai dati

Le autorità di contrasto e giudiziarie devono essere in grado di indagare e intervenire contro la criminalità. Quasi tutte le forme di criminalità grave e organizzata hanno oggi un'impronta digitale[13]: nell'85 % circa delle indagini penali le autorità di contrasto devono essere in grado di accedere a informazioni digitali[14].

Nella relazione conclusiva[15] il **gruppo ad alto livello sull'accesso ai dati per un'efficace azione di contrasto** ha evidenziato che nell'ultimo decennio le autorità di contrasto e giudiziarie hanno perso terreno nei confronti dei criminali; infatti questi ultimi si avvalgono di strumenti e prodotti provenienti da altre giurisdizioni, offerti da prestatori che hanno messo in atto misure che rendono di fatto impossibile la cooperazione in relazione a richieste legittime in singoli casi penali. La cooperazione sistematica tra le autorità di contrasto e i privati, tra cui i prestatori di servizi, sarà pertanto essenziale negli sforzi futuri volti a smantellare gli individui e le reti criminali più temibili nell'Unione e al di fuori di essa.

Via via che la digitalizzazione si fa più pervasiva e si afferma come fonte in costante crescita di nuovi strumenti per i criminali, è essenziale definire un regime di accesso ai dati in grado di soddisfare nell'Unione le esigenze di rispetto della legge e di salvaguardia dei valori. Allo stesso tempo il fatto che i sistemi digitali rimangano protetti contro l'accesso non autorizzato è altrettanto essenziale per preservare la cibersicurezza e offrire una protezione contro le minacce alla sicurezza che si profilano. I regimi di accesso devono rispettare i diritti fondamentali, garantendo tra l'altro un'adeguata tutela della vita privata e dei dati personali.

Negli ultimi anni l'UE ha adottato misure sia per contrastare la **criminalità online sia per facilitare l'accesso alle prove digitali per tutti i reati** grazie all'adozione di norme in materia di prove elettroniche che si applicheranno integralmente da agosto 2026[16] e saranno integrate dagli strumenti internazionali per lo scambio di informazioni e prove. La Commissione proporrà presto la firma e la conclusione della nuova **Convenzione delle Nazioni Unite contro la criminalità informatica**.

Per dar seguito alle raccomandazioni del gruppo ad alto livello[17], nella prima metà del 2025 la Commissione presenterà una **tabella di marcia per definire le misure giuridiche e pratiche**

[12] Infrastruttura dell'UE per la resilienza, l'interconnettività e la sicurezza via satellite.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52019PC0070.
[15] "Concluding report of the High-Level Group on access to data for effective law enforcement" - 15/11/2024, 4802e306-c364-4154-835b-e986a9a49281_en.
[16] Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali (GU L 191 del 28.7.2023, pag. 118).
[17] Conclusioni del Consiglio sull'accesso ai dati per un'efficace attività di contrasto (12 dicembre 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/it/pdf.

che propone di adottare **per assicurare l'accesso legittimo ed effettivo ai dati**. Nella scia di questa tabella di marcia la Commissione darà priorità a una valutazione dell'impatto delle **norme sulla conservazione dei dati** a livello di UE e alla compilazione di una **tabella di marcia tecnologica sulla cifratura**, al fine di individuare e valutare soluzioni tecnologiche che consentano alle autorità di contrasto di accedere legalmente ai dati cifrati, sempre salvaguardando la cibersicurezza e rispettando i diritti fondamentali.

Cooperazione operativa

La Commissione collaborerà con gli Stati membri, gli organi e gli organismi dell'UE e i paesi partner per rafforzare la cooperazione operativa, essenziale per un approccio più efficace alla lotta contro la criminalità organizzata transnazionale e il terrorismo.

In quanto principale quadro dell'UE per l'azione comune contro la criminalità organizzata e le forme gravi di criminalità, la **piattaforma multidisciplinare europea di lotta alle minacce della criminalità (EMPACT)** ha conseguito risultati operativi sostanziali. Il prossimo ciclo EMPACT 2026-2029 offre l'opportunità di rafforzare ulteriormente tale quadro. Per smantellare gli individui e le reti criminali più temibili l'Unione deve razionalizzare e concentrare gli sforzi sulle priorità più urgenti, intensificando gli impegni degli Stati membri e garantendo un uso efficace delle risorse.

A tal fine la Commissione collaborerà con le presidenze del Consiglio e gli Stati membri per **massimizzare il potenziale dell'EMPACT e rispondere alle priorità fondamentali per il prossimo ciclo EMPACT 2026-2029.** In questi settori prioritari sono necessarie attività di intelligence sulle reti criminali più temibili, indagini comuni e task force operative unite a una forte risposta giudiziaria, volta tra l'altro a seguire le tracce del denaro. L'Unione deve inoltre contrastare il reclutamento nelle fila della criminalità e le infiltrazioni della criminalità, rafforzando la cooperazione e la formazione nelle attività di contrasto a livello internazionale e multiagenzia.

La Commissione sosterrà anche altre forme di **cooperazione operativa transfrontaliera nell'attività di contrasto tra gli Stati membri e i paesi associati Schengen**. Per garantire un livello elevato di sicurezza interna lo spazio Schengen, senza controlli alle frontiere interne, richiede una stretta cooperazione e un intenso scambio di informazioni tra le autorità di contrasto degli Stati membri. Ancora oggi gli operatori delle autorità di contrasto si imbattono in difficoltà quando svolgono attività di osservazione o effettuano interventi urgenti a livello transfrontaliero[18]; anche per contrastare le minacce ibride è necessaria una cooperazione transfrontaliera più intensa. Sarebbe opportuno istituire un **gruppo ad alto livello sul futuro della cooperazione operativa nell'attività di contrasto** per sviluppare una visione strategica condivisa.

Uno scambio di dati efficiente tra le autorità di contrasto è essenziale anche per un'efficace cooperazione transfrontaliera. Una volta istituita, l'**architettura dell'interoperabilità** fornirà alle autorità di contrasto e a Europol un accesso effettivo a informazioni cruciali. Allo stesso tempo l'UE e gli Stati membri dovrebbero privilegiare lo scambio bilaterale e multilaterale di informazioni, attraverso l'attuazione giuridica e tecnica del **regolamento Prüm II**[19], in

[18] Come si segnala nella valutazione della Commissione dell'attuazione data dagli Stati membri alla raccomandazione (UE) 2022/915 del Consiglio, del 9 giugno 2022, sulla cooperazione operativa nell'attività di contrasto (5909/25).

[19] Regolamento (UE) 2024/982 del Parlamento europeo e del Consiglio, del 13 marzo 2024, sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia e che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio (regolamento Prüm II) (GU L, 2024/982, 5.4.2024).

cooperazione con eu-LISA ed Europol. In tal modo sarà possibile effettuare scambi automatizzati e sicuri di impronte digitali, profili DNA, dati di immatricolazione dei veicoli, immagini del volto ed estratti del casellario giudiziale attraverso router dell'UE. A livello nazionale gli Stati membri devono attuare la **direttiva relativa allo scambio di informazioni**[20] potenziando i canali di scambio di informazioni ai fini della fluidità del relativo flusso transfrontaliero, integrandoli nel contempo con i sistemi a livello di Unione, come SIENA[21].

Un'efficace cooperazione transfrontaliera si fonda anche sulla promozione di una **cultura comune dell'UE in materia di contrasto**. Formazione comune, centri di eccellenza e programmi di mobilità sono elementi essenziali per raggiungere questo obiettivo. La Commissione esaminerà in modo in cui l'UE possa meglio favorire la formazione delle autorità degli Stati membri, avvalendosi di **CEPOL**, l'agenzia dell'Unione europea per la formazione delle autorità di contrasto.

Rafforzare la sicurezza delle frontiere

Rafforzare la resilienza e la sicurezza delle frontiere esterne è una misura essenziale per contrastare le minacce ibride quali l'uso della migrazione come arma, per impedire l'ingresso nell'UE di autori di minacce e di merci che rappresentano minacce, oltre che per combattere efficacemente la criminalità e il terrorismo transfrontalieri. Nel 2026 **si prevede di potenziare il sistema d'informazione Schengen (SIS)** per consentire agli Stati membri di inserire segnalazioni di cittadini di paesi terzi implicati nel terrorismo (compresi i combattenti terroristi stranieri) e in altre forme gravi di criminalità, sulla base dei dati condivisi da paesi terzi con Europol.

Una migliore **interoperabilità** dei sistemi di informazione dell'UE su larga scala fornirà agli Stati membri informazioni essenziali sulle persone provenienti da paesi terzi che attraversano o intendono attraversare le frontiere esterne, aiutando le autorità a valutare le condizioni per autorizzare l'ingresso nel territorio degli Stati membri[22]. La Commissione continuerà a collaborare strettamente con gli Stati membri ed eu-LISA per attuare rapidamente tali sistemi, in particolare il **sistema di ingressi/uscite (EES), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e il sistema di informazione visti (VIS) riveduto**, al fine di garantirne il buon funzionamento e i vantaggi in termini di sicurezza.

Per rafforzare ulteriormente la sicurezza delle frontiere e consolidare la cooperazione dell'UE di fronte all'evoluzione delle minacce, **la Commissione proporrà di potenziare Frontex.** Nel corso del tempo il personale della guardia di frontiera e costiera europea dovrebbe triplicare fino a raggiungere 30 000 unità. L'Agenzia dovrebbe dotarsi di tecnologie avanzate di sorveglianza e conoscenza situazionale, tra cui l'intelligence utile per la gestione europea integrata delle frontiere e l'accesso a solidi servizi pubblici di osservazione della Terra basati nell'UE per il controllo di frontiera, da realizzare entro il 2027. Queste misure dovrebbero migliorare ulteriormente la capacità di individuare, prevenire e combattere la criminalità transfrontaliera alle frontiere esterne, rafforzando allo stesso tempo il sostegno agli Stati

[20] Direttiva (UE) 2023/977 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri e che abroga la decisione quadro 2006/960/GAI del Consiglio (GU L 134 del 22.5.2023, pag. 1).

[21] Applicazione di rete per lo scambio sicuro di informazioni (Secure Information Exchange Network Application).

[22] In particolare il sistema di ingressi/uscite (EES) consentirà agli Stati membri di identificare i cittadini di paesi terzi alle frontiere esterne dello spazio Schengen e di registrarne gli ingressi e le uscite, consentendo un'identificazione sistematica dei soggiornanti fuoritermine. Prima dell'arrivo di un cittadino di un paese terzo alle frontiere esterne, il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e il sistema di informazione visti (VIS) consentiranno agli Stati membri di valutare preventivamente se la presenza di un cittadino di un paese terzo nel territorio dell'UE rappresenti un rischio per la sicurezza.

membri nell'attuazione dei rimpatri, in particolare in relazione ai cittadini di paesi terzi che rappresentano un rischio per la sicurezza.

La **frode documentale e d'identità** favorisce il traffico di migranti, la tratta di esseri umani, i movimenti clandestini di natura criminosa e il traffico di merci illecite. Una volta operativo, il **rilevatore di identità multiple (MID)**[23] migliorerà la capacità delle autorità nazionali di identificare le persone che utilizzano identità multiple e contrastare la frode di identità. La Commissione esaminerà le modalità per migliorare la sicurezza dei documenti di viaggio e di soggiorno rilasciati ai cittadini dell'UE e di paesi terzi. Valuterà in che modo i portafogli di identità digitale dell'UE, da introdurre ai sensi del quadro europeo relativo a un'identità digitale entro la fine del 2026, possano contribuire a migliorare la sicurezza dei documenti di viaggio e la verifica dell'identità, integrando le proposte sulle credenziali di viaggio digitali e sull'applicazione di viaggio digitale dell'UE[24].

Le **informazioni sui viaggi** sono fondamentali per consentire alle autorità di individuare i movimenti di criminali, terroristi e altri soggetti che rappresentano minacce per la sicurezza, e di indagare in materia. Mentre esiste un quadro dell'UE per le informazioni sui viaggi aerei commerciali[25], il trattamento a fini di contrasto dei dati provenienti da altri modi di trasporto è frammentato. Di conseguenza criminali e terroristi possono sfruttare per attività illegali diversi modi di trasporto, senza essere individuati. La Commissione collaborerà con gli Stati membri e con il settore dei trasporti allo scopo di **rafforzare il quadro per le informazioni sui viaggi**, esplorando la possibilità di introdurre un sistema dell'Unione che imponga agli operatori di voli privati di raccogliere e trasferire i dati dei passeggeri, valutando le norme sul trattamento dei dati del codice di prenotazione nonché le modalità per razionalizzare il trattamento delle informazioni sui viaggi marittimi. Per quanto riguarda il trasporto su strada, la Commissione valuterà la possibilità di utilizzare più ampiamente i **sistemi di riconoscimento automatico del numero di targa (ANPR)** e accrescerà le possibili sinergie con il SIS.

Approccio fondato sulla previsione, l'innovazione e le capacità

La Commissione svilupperà **un approccio globale fondato sulla previsione in materia di sicurezza interna a livello di Unione**, basandosi sulle migliori pratiche individuate a livello nazionale. Questo approccio favorirà l'elaborazione delle politiche e orienterà gli investimenti nelle pertinenti attività di ricerca e innovazione nel campo della sicurezza, finanziate dall'UE.

La ricerca e l'innovazione svolgono un ruolo cruciale nella sicurezza interna elaborando soluzioni per contrastare le minacce emergenti, anche quelle derivanti dall'uso improprio della tecnologia[26]. L'UE deve continuare a investire, attraverso la ricerca e l'innovazione in materia di sicurezza finanziate dall'UE[27], nello sviluppo di strumenti e soluzioni innovativi per affrontare le minacce alla sicurezza, nel rispetto delle norme e dei diritti fondamentali dell'UE. La Commissione dovrebbe promuovere la transizione dalla ricerca all'applicazione per garantire l'effettiva diffusione di tali capacità moderne, privilegiando le **tecnologie moderne**

[23] Il MID è una delle componenti dell'interoperabilità introdotte dal regolamento (UE) 2019/818 e dal regolamento (UE) 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/it/ip_24_5047.
[25] Quadro relativo ai dati del codice di prenotazione (PNR) e alle informazioni anticipate sui passeggeri (API) istituito dalla direttiva (UE) 2016/681 ("direttiva PNR") e dai regolamenti (UE) 2025/12 e (UE) 2025/13 ("regolamenti API").
[26] Cfr. la relazione del Centro comune di ricerca della Commissione "Emerging risks and opportunities for EU internal security stemming from new technologies"https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] "Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation" – 2025, https://data.europa.eu/doi/10.2837/0004501.

come l'IA. Quest'approccio dovrebbe comprendere la formazione per migliorare l'uso dei sistemi di IA e di altre capacità tecniche da parte delle autorità di contrasto e giudiziarie. Laddove opportuno le tecnologie potenzialmente a duplice uso si dovrebbero sfruttare in entrambe le direzioni (dal settore civile a quello della difesa, e dal settore della difesa a quello civile)[28].

Il **polo di innovazione dell'UE per la sicurezza interna**[29], rete di laboratori per l'innovazione che offre i più recenti aggiornamenti in materia di innovazione oltre a soluzioni efficaci per coadiuvare il lavoro dei soggetti impegnati nella sicurezza interna nell'UE e negli Stati membri, contribuirà a integrare la ricerca nella pratica e nelle politiche. È necessario potenziare l'archivio degli strumenti di Europol (ETR) per rendere più efficace l'operato di quest'agenzia, consentendole di individuare, sviluppare, acquisire assieme e applicare tecnologie avanzate a livello operativo. La Commissione istituirà inoltre presso il Centro comune di ricerca un **campus per la ricerca e l'innovazione nel settore della sicurezza** che riunirà i ricercatori per abbreviare il ciclo che va dai risultati della ricerca all'innovazione, allo sviluppo e alla positiva attuazione, riducendo contemporaneamente i costi di sviluppo, sperimentazione e convalida.

Lo **Spazio europeo della ricerca** è per sua natura collaborativo e quindi permeabile alle ingerenze straniere e alla disinformazione. A seguito dell'adozione della raccomandazione del Consiglio relativa al rafforzamento della sicurezza della ricerca[30], la Commissione e gli Stati membri adottano misure per mettere i soggetti pertinenti in grado di lavorare, tra l'altro istituendo un centro europeo di competenza sulla sicurezza della ricerca.

Azioni fondamentali

La Commissione adotterà:

- **una proposta legislativa per trasformare Europol in un'agenzia di contrasto realmente operativa nel 2026;**
- **una proposta legislativa per potenziare Eurojust nel 2026;**
- **una proposta legislativa per rafforzare il ruolo e i compiti di Frontex nel 2026;**
- **una proposta legislativa per istituire un sistema europeo di comunicazione critica nel 2026.**

La Commissione intende:

- **presentare una tabella di marcia che definisca il percorso da seguire per l'accesso legittimo ed effettivo ai dati nelle attività di contrasto nel 2025;**
- **preparare se del caso una valutazione d'impatto nel 2025 al fine di aggiornare le norme sulla conservazione dei dati a livello dell'UE;**
- **presentare una tabella di marcia tecnologica sulla cifratura per individuare e valutare soluzioni tecnologiche che consentano alle autorità di contrasto di accedere legalmente ai dati nel 2026;**
- **lavorare all'istituzione di un gruppo ad alto livello per rafforzare la cooperazione operativa nell'attività di contrasto;**
- **creare un campus per la ricerca e l'innovazione nel settore della sicurezza presso il Centro comune di ricerca nel 2026.**

[28] Come indicato nella relazione Niinistö.
[29] EU Innovation Hub for Internal Security | Europol.
[30] GU C/2024/3510, 30.5.2024.

La Commissione, in collaborazione con gli Stati membri e gli organismi competenti dell'UE, intende:

- **consolidare l'architettura dell'EMPACT;**
- **adoperarsi per introdurre rapidamente l'architettura di interoperabilità e attuare il regolamento Prüm II;**
- **rafforzare il quadro per le informazioni sui viaggi.**

Gli Stati membri sono esortati a:

- **recepire e attuare integralmente la direttiva relativa allo scambio di informazioni.**

4. Resilienza alle minacce ibride e ad altri atti ostili

Rafforzeremo la resilienza alle minacce ibride migliorando la protezione delle infrastrutture critiche, potenziando la cibersicurezza, garantendo la sicurezza dei nodi di trasporto e dei porti e contrastando le minacce online.

Gli atti ostili che compromettono la sicurezza dell'UE diventano sempre più frequenti e sofisticati, a opera di soggetti malintenzionati che arricchiscono considerevolmente il proprio arsenale. Le campagne ibride che hanno per obiettivo l'UE, gli Stati membri e i loro partner si sono intensificate e vanno da atti di sabotaggio contro le infrastrutture critiche a incendi dolosi, attacchi informatici, ingerenze elettorali, manipolazione delle informazioni e ingerenze da parte di attori stranieri, compresa la disinformazione, fino all'uso della migrazione come arma. A causa del loro ruolo politico e operativo e della natura delle informazioni che trattano, le istituzioni, gli organi e gli organismi dell'Unione ("soggetti dell'Unione") non rimangono indenni.

L'UE deve **rafforzare la propria resilienza**, utilizzare gli strumenti vigenti in modo efficace e sviluppare nuovi metodi per far fronte all'evoluzione di queste minacce arrecate da attori statali e non statali, sia oggi che in futuro.

Infrastrutture critiche

Le minacce alle **infrastrutture critiche**, tra cui le minacce ibride come il sabotaggio e le attività informatiche dolose, costituiscono un grave motivo di preoccupazione, in particolare per le infrastrutture che collegano gli Stati membri (si tratti di interconnettori dell'energia o di cavi di comunicazione transfrontaliera) e per i trasporti. Dall'inizio della guerra di aggressione della Russia contro l'Ucraina gli atti di sabotaggio contro le infrastrutture critiche sono aumentati, in particolare nel 2024, e hanno colpito numerosi Stati membri. La cooperazione tra le autorità di contrasto, i servizi di sicurezza e cibersicurezza, la protezione civile e militare e gli operatori privati è essenziale per anticipare, prevenire e individuare le minacce alla sicurezza e rispondervi efficacemente.

Per garantire l'erogazione ininterrotta di servizi essenziali, indispensabili all'economia e alla società, è assolutamente necessario ridurre le vulnerabilità e rafforzare la resilienza dei soggetti critici. A tale riguardo è pertanto fondamentale, per tutti gli Stati membri, recepire tempestivamente e attuare correttamente la **direttiva sulla resilienza dei soggetti critici**

(CER)[31] e la **direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS2)**[32].

Per garantire progressi rapidi la Commissione coadiuverà gli Stati membri nell'individuazione dei soggetti critici[33] e nello scambio di buone pratiche sulle strategie nazionali e sulle valutazioni dei rischi per quanto riguarda i servizi essenziali, in collaborazione con il **gruppo per la resilienza dei soggetti critici e il gruppo di cooperazione NIS**. Qualora si verifichino perturbazioni delle infrastrutture critiche aventi un impatto transfrontaliero significativo, il **programma dell'UE per le infrastrutture critiche** coordinerà le risposte a livello dell'UE. La Commissione incoraggia il Consiglio ad adottare rapidamente il **programma dell'UE per la cibersicurezza**, che rafforzerà ulteriormente il coordinamento nel contesto della gestione delle crisi, facilitando una collaborazione più stretta tra le autorità in materia di resilienza fisica e digitale. Dopo il successo registrato nel 2023 dalle prove di stress nel settore dell'energia, la Commissione promuoverà **prove di stress volontarie** in altri settori chiave per la sicurezza interna. Preparerà una **rassegna, a livello dell'Unione, dei rischi transfrontalieri e intersettoriali** per la prestazione dei servizi essenziali, volta a sostenere le valutazioni dei rischi degli Stati membri e a orientare una valutazione globale dei rischi a livello dell'UE. In linea con la strategia per l'Unione della preparazione, la Commissione collaborerà con gli Stati membri al fine di individuare ulteriori settori e servizi, non contemplati dalla legislazione vigente, per i quali potrebbe essere necessario intervenire.

La **task force UE-NATO sulla resilienza delle infrastrutture critiche** ha promosso un'eccellente cooperazione nella condivisione delle migliori pratiche e nel rafforzamento della resilienza nei settori dell'energia, dei trasporti, delle infrastrutture digitali e dello spazio. I lavori proseguiranno nell'ambito del **dialogo strutturato UE-NATO sulla resilienza**. Il **pacchetto di strumenti dell'UE contro le minacce ibride** assicura agli Stati membri e ai partner un forte sostegno nella preparazione alle minacce ibride e nella lotta contro di esse. I **gruppi di risposta rapida alle minacce ibride**[34] offrono, su richiesta, assistenza personalizzata a breve termine agli Stati membri, a varie missioni dell'UE e ai partner. La Commissione porterà avanti la cooperazione dell'UE in materia di lotta al sabotaggio attraverso attività di esperti[35], tra cui un **apposito programma di lavoro comune** che consenta agli esperti di razionalizzare lo scambio di informazioni e mettere a punto le contromisure.

Gli incidenti che interessano i **cavi sottomarini** in Europa sottolineano la necessità di misure più incisive e di risposte più chiare. Come indicato nel **piano d'azione dell'UE sulla sicurezza dei cavi**[36], la Commissione, insieme all'alto rappresentante, collaborerà con gli Stati membri, gli organismi dell'UE e partner come la NATO in un'opera di prevenzione, individuazione, risposta, e deterrenza in relazione alle minacce ai cavi sottomarini. Al fine di elaborare un quadro situazionale integrato delle minacce, la Commissione collaborerà con gli Stati membri

[31] Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio.
[32] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
[33] La direttiva contempla i settori dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della sanità, delle acque potabili, delle acque reflue, delle infrastrutture digitali, della pubblica amministrazione, dello spazio, della produzione, trasformazione e distribuzione di alimenti.
[34] Bussola strategica dell'UE per la sicurezza e la difesa 2022, pag. 22.
[35] I consulenti dell'UE sulla sicurezza protettiva, la rete europea di bonifica di ordigni esplosivi (EEODN), la rete ATLAS, la rete UE "alto rischio di sicurezza" (EU HRSN), il gruppo consultivo in materia di sicurezza CBRN e il gruppo per la resilienza dei soggetti critici (CERG).
[36] JOIN (2025) 9 final.

per sviluppare e attuare, su base volontaria, un meccanismo di sorveglianza integrata dei cavi sottomarini per bacino marittimo, a partire da un polo regionale nordico/baltico.

Cibersicurezza

La natura persistente delle **attività informatiche dolose**, che spesso rientrano in una gamma più ampia di minacce multidimensionali e ibride, richiede un'attenzione e un'azione costanti a livello europeo. Negli ultimi anni l'Unione ha adottato una serie di provvedimenti legislativi sulla cibersicurezza che rafforzano la ciberresilienza dei soggetti NIS2 operanti in settori critici dell'UE[37], nonché dei soggetti dell'Unione, migliorano la sicurezza dei prodotti digitali (regolamento sulla ciberresilienza) e istituiscono un quadro per il sostegno alla preparazione e alla risposta agli incidenti (regolamento sulla cibersolidarietà). A gennaio 2025 la Commissione ha adottato il **piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria**[38] per migliorare l'individuazione delle minacce, la preparazione e la risposta alle crisi. La completa attuazione di questo piano è fondamentale. Allo stesso tempo per far fronte alle nuove minacce e ai nuovi sviluppi dobbiamo intensificare l'azione, in particolare nei settori dello scambio di informazioni, della sicurezza della catena di approvvigionamento, del ransomware, degli attacchi informatici e della sovranità tecnologica.

Per attuare il piano è necessario colmare l'attuale deficit di competenze in materia di cibersicurezza, quantificabile in 299 000 persone. La Commissione collaborerà con gli Stati membri nell'ambito dell'Unione delle competenze[39] per ampliare la forza lavoro nel settore della cibersicurezza, in particolare utilizzando la nuova accademia per le competenze in materia di cibersicurezza. Il piano strategico per l'istruzione STEM[40] contribuisce a migliorare il bacino di talenti e la risposta dell'Europa alle esigenze del mercato del lavoro in materia di cibersicurezza.

Parallelamente al rafforzamento della propria resilienza, l'UE continuerà a sfruttare appieno il quadro relativo a una sua risposta diplomatica comune alle attività informatiche dolose (**il pacchetto di strumenti della diplomazia informatica)** per svolgere opera di prevenzione, deterrenza e risposta alle minacce informatiche poste da attori statali e non statali.

Sicurezza delle catene di approvvigionamento delle TIC

Il **pacchetto di strumenti sulla cibersicurezza del 5G** offre il quadro idoneo per proteggere le reti 5G; attualmente però gli Stati membri non lo attuano in misura sufficiente. Permangono rischi inaccettabili per la sicurezza, in particolare per quanto riguarda la sostituzione dei fornitori ad alto rischio. Un approccio armonizzato alla sicurezza della catena di approvvigionamento delle TIC può servire per risolvere il problema dell'attuale frammentazione del mercato interno, causata da approcci diversi a livello nazionale, evitare dipendenze critiche e mettere le catene di approvvigionamento TIC al riparo dai fornitori ad alto rischio, garantendo in tal modo la sicurezza delle infrastrutture critiche dell'Unione.

In linea con tale approccio, nella prossima **revisione del regolamento sulla cibersicurezza** la Commissione esaminerà più in generale la sicurezza e la resilienza delle catene di approvvigionamento e delle infrastrutture TIC. Proporrà di migliorare il **quadro europeo di**

[37] Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (GU L, 2023/2841, 18.12.2023).

[38] https://digital-strategy.ec.europa.eu/it/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

[39] COM (2025) 90 final.

[40] COM (2025) 89 final.

certificazione della cibersicurezza, per garantire che i futuri sistemi di certificazione possano essere adottati tempestivamente e rispondere alle esigenze politiche.

Sulla base delle valutazioni settoriali già effettuate o in corso[41], la Commissione elaborerà, insieme agli Stati membri, una **pianificazione strategica per le valutazioni coordinate dei rischi per la cibersicurezza**.

I servizi cloud e di telecomunicazione sono diventati un elemento fondamentale delle catene di approvvigionamento delle infrastrutture critiche, delle imprese e delle autorità pubbliche. La Commissione adotterà misure per incoraggiare i soggetti critici a scegliere **servizi cloud e di telecomunicazione che offrano un livello adeguato di cibersicurezza**, tenendo conto non solo dei rischi tecnici ma anche dei rischi strategici e delle dipendenze.

Ransomware e attacchi informatici

Nell'UE e a livello mondiale una delle principali sfide persistenti è rappresentata dal **ransomware**: una relazione ne stima il costo annuo globale a oltre 250 miliardi di EUR da qui al 2031[42]. Sia la **direttiva NIS2** sia il **regolamento sulla ciberresilienza** miglioreranno sensibilmente la posizione dei soggetti in materia di sicurezza, rendendo più costoso per le reti ransomware sferrare attacchi. La Commissione inoltre collaborerà strettamente con gli Stati membri affinché sia segnalato alle autorità di contrasto un numero maggiore di attacchi ransomware (in particolare di minacce avanzate e persistenti) e di pagamenti di riscatti, in modo da facilitare le indagini.

Per prevenire e bloccare gli attacchi informatici l'UE deve intensificare lo scambio di informazioni tra le autorità di contrasto, le autorità e i soggetti responsabili della cibersicurezza e i privati, sotto l'egida di Europol e dell'Agenzia dell'UE per la cibersicurezza (ENISA).

Europol ed Eurojust dovrebbero continuare a basarsi sui risultati conseguiti nella rimozione delle operazioni di ransomware, promuovendo la cooperazione nell'attività di contrasto. A tal fine le autorità di contrasto dovrebbero massimizzare l'uso dei meccanismi di cooperazione, tra cui il **modello internazionale di risposta al ransomware di Europol** e l'**iniziativa internazionale "Counter Ransomware"**[43]; l'ENISA ed Europol dovrebbero cooperare per ampliare l'archivio degli strumenti di decrittazione per i ceppi ransomware[44].

Sovranità tecnologica

La cibersicurezza e la sovranità tecnologica sono strettamente interconnesse, e occorre in via prioritaria affrontare la questione delle dipendenze tecnologiche. L'Unione deve **guidare lo sviluppo e la diffusione di nuove tecnologie**; la Commissione da parte sua si adopera per **rafforzare le capacità nelle tecnologie strategiche** come l'IA, la connettività quantistica, la connettività avanzata, il cloud, l'edge e l'internet delle cose[45], attraverso iniziative di prossima realizzazione quali il piano d'azione per il continente dell'IA, la strategia quantistica e altre[46]. La Commissione continuerà a sostenere la tempestiva diffusione dei più recenti **protocolli internet** concordati a livello internazionale, che sono essenziali per mantenere la scalabilità e

[41] Ad esempio sulle reti 5G, le telecomunicazioni, l'energia elettrica, le energie rinnovabili e i veicoli connessi.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Disponibile tramite il progetto No More Ransom, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_it#step-scope.
[46] Ad esempio EuropHPC JU https://eurohpc-ju.europa.eu/index_en, l'iniziativa faro sulle tecnologie quantistiche - Homepage dell'iniziativa faro sulle tecnologie quantistiche| Iniziativa faro sulle tecnologie quantistiche, le reti 3C (COM(2024) 81 final) e il piano d'azione dell'UE sulla sicurezza dei cavi (JOIN(2025) 9 final).

l'efficienza di internet con un livello rafforzato di cibersicurezza. Sono inoltre necessarie ulteriori azioni per far fronte alle **sfide connesse allo spettro radio** come quelle relative alle dipendenze, ai rischi per la catena di approvvigionamento, al jamming e allo spoofing in relazione al GNSS, quali ad esempio l'impiego di tecnologie di rilevamento quantistico e l'esame dello sviluppo della capacità di controllo delle radiofrequenze.

L'impiego di soluzioni di **crittografia post-quantistica** sarà fondamentale per salvaguardare le comunicazioni sensibili e i dati a riposo, e per proteggere le identità digitali nella nuova era quantistica. Sulla base della raccomandazione del 2024 relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica[47], la Commissione collabora con gli Stati membri per promuovere tale transizione. A questo riguardo gli Stati membri dovrebbero individuare i casi ad alto rischio presso i soggetti critici e garantire la cifratura quantum-safe per tali casi ad alto rischio quanto prima e comunque entro la fine del 2030. La Commissione collabora altresì con gli Stati membri e con l'Agenzia spaziale europea (ESA) per lo sviluppo e l'impiego dell'**infrastruttura europea di comunicazione quantistica (EuroQCI)**[48] sulla base della distribuzione quantistica delle chiavi (QKD), nel quadro di **IRIS²**, il programma dell'Unione per una connettività sicura. Entrambe le iniziative consentiranno in ultima analisi ai soggetti di trasmettere dati e conservare le informazioni in modo sicuro.

Le **tecnologie quantistiche** svolgeranno anche un ruolo fondamentale nelle applicazioni di sicurezza: nell'ambito della **strategia quantistica** sarà elaborata una **tabella di marcia per il rilevamento quantistico nelle applicazioni di sicurezza**. Analogamente la Commissione si adopera per rendere a prova di computer quantistici i sistemi critici per la sua sicurezza istituzionale, compresi i sistemi informatici classificati.

Un quadro per la cibersicurezza favorevole alle imprese

L'imminente revisione del regolamento sulla cibersicurezza offre l'occasione di **semplificare la legislazione dell'UE in materia di cibersicurezza,** in linea con la bussola per la competitività. La Commissione collaborerà strettamente con gli Stati membri per garantire un'attuazione rapida, coerente e favorevole alle imprese del quadro orizzontale in materia di cibersicurezza di cui alla direttiva NIS 2, al regolamento sulla ciberresilienza e al regolamento sulla cibersolidarietà, promuovendo la semplicità e la coerenza ed evitando la frammentazione o la duplicazione delle norme in materia di cibersicurezza nelle legislazioni nazionali e dell'UE.

Per consentire un accesso sicuro ai servizi online e rafforzare la sicurezza digitale in tutta l'UE, il **quadro europeo relativo a un'identità digitale** offrirà a tutti i cittadini e residenti dell'UE portafogli di identità digitale affidabili entro la fine del 2026. Il **portafoglio europeo delle imprese** di prossima realizzazione faciliterà interazioni transfrontaliere sicure tra le imprese e le pubbliche amministrazioni. Entrambi sono prerequisiti per un funzionamento sicuro e più efficiente del mercato unico basato sui dati con strumenti quali lo sportello digitale unico, la fatturazione elettronica, gli appalti elettronici e il passaporto digitale dei prodotti.

Sicurezza online

Sono attuate online alcune delle più gravi minacce ibride che mettono a repentaglio la sicurezza e l'incolumità dei cittadini in Europa e sono dirette contro la sfera democratica dell'UE. Si tratta di attività illegali e contenuti illegali online, manipolazione delle informazioni che comporta amplificazione artificiale, informazioni fuorvianti nonché manipolazione delle informazioni e ingerenze da parte di attori stranieri.

[47] Raccomandazione relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica |Plasmare il futuro digitale dell'Europa.
[48] https://digital-strategy.ec.europa.eu/it/policies/european-quantum-communication-infrastructure-euroqci.

La rigorosa applicazione del **regolamento sui servizi digitali** è fondamentale per garantire un ambiente online sicuro e accessibile con attori responsabili, che sia resiliente anche alle minacce ibride. Il regolamento sui servizi digitali obbliga i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi a effettuare valutazioni dei rischi e a mettere in atto misure di attenuazione dei rischi sistemici derivanti dalla progettazione, dal funzionamento o dall'uso dei loro servizi. Tali rischi possono includere effetti negativi sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica, come le ingerenze di vasta portata da parte di attori statali stranieri malintenzionati, ad esempio nei processi elettorali. La formazione delle autorità competenti degli Stati membri sull'uso degli strumenti giuridici per rimuovere tempestivamente i contenuti illegali online è importante, soprattutto per quanto riguarda la violenza di genere online. Il regolamento sui servizi digitali prevede un meccanismo di risposta alle crisi che può essere attivato qualora circostanze eccezionali comportino una minaccia grave per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative della stessa. Per integrare tale meccanismo la Commissione e le autorità nazionali competenti designate come coordinatori dei servizi digitali hanno anche elaborato un **quadro volontario di risposta agli incidenti ai sensi del regolamento sui servizi digitali**. I coordinatori dei servizi digitali hanno inoltre intrapreso azioni per contribuire a proteggere l'integrità delle elezioni, ad esempio organizzando tavole rotonde elettorali e prove di stress[49]. Il regolamento sui servizi digitali, insieme al regolamento sulla pubblicità politica[50], costituisce uno dei diversi filoni legati alla salvaguardia della democrazia e dell'integrità dei processi democratici, che sono vulnerabili agli attacchi di attori ostili, sferrati anche attraverso strumenti digitali e sui social media.

L'attuazione del pacchetto di strumenti per la **manipolazione delle informazioni e le ingerenze da parte di attori stranieri** rappresenta un'altra componente importante che offre un sostegno fondamentale a livello di Unione. Anche il sostegno all'alfabetizzazione digitale e mediatica e al pensiero critico è un elemento centrale di questi sforzi[51].

Contrastare l'uso della migrazione come arma

La Russia, con l'aiuto e il sostegno determinante della Bielorussia, ha strumentalizzato intenzionalmente la migrazione e agevolato illegalmente i flussi migratori verso le frontiere esterne dell'UE, con l'obiettivo di destabilizzare le società dell'Unione e minarne l'unità. Ciò mette a repentaglio non solo la sicurezza nazionale e la sovranità degli Stati membri, ma anche la sicurezza e l'integrità dello spazio Schengen e la sicurezza dell'Unione nel suo complesso. Nelle conclusioni dell'ottobre 2024 il Consiglio europeo ha sottolineato che né alla Russia, né alla Bielorussia, né a nessun altro paese può essere consentito di abusare dei nostri valori, compreso il diritto di asilo, e di minare la nostra democrazia.

Come si illustra nella comunicazione della Commissione del 2024 sull'uso della migrazione come arma, oltre a esprimere un forte sostegno politico, l'Unione ha adottato misure finanziarie, operative e diplomatiche, compresa la cooperazione con i paesi di origine e transito, per rispondere in modo efficace a queste minacce[52]. Tale risposta comporta il ricorso al nuovo quadro istituito dal Consiglio per applicare sanzioni alle persone e alle organizzazioni implicate in azioni e politiche quali l'uso della migrazione come arma da parte della Russia, imponendo

[49] Kit di strumenti elettorali DSA per i coordinatori dei servizi digitali 2025 https://digital-strategy.ec.europa.eu/it/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al targeting della pubblicità politica (GU L, 2024/900, 20.3.2024).
[51] Piano d'azione per l'istruzione digitale (2021-2027) - Spazio europeo dell'istruzione.
[52] COM (2024) 570 final.

il congelamento dei beni e i divieti di viaggio[53]. Ove necessario l'Unione continuerà a servirsi di detto quadro e a sostenere gli Stati membri nel contrasto a tale minaccia.

Sicurezza dei trasporti

I porti marittimi, gli aeroporti e le infrastrutture terrestri sono punti di entrata e di uscita fondamentali, che assolvono una funzione vitale nell'economia e nella società dell'UE e sono essenziali per la mobilità militare. Allo stesso tempo però tali nodi e mezzi di trasporto costituiscono un bersaglio privilegiato per le minacce esterne e le attività criminali. I recenti incidenti, tra cui le violazioni della sicurezza del trasporto aereo di merci e gli attacchi alle infrastrutture ferroviarie, mettono in evidenza gravi rischi. Per i soggetti malintenzionati gli **operatori dei trasporti** possono rappresentare sia obiettivi che strumenti. I vigenti strumenti giuridici dell'UE hanno rafforzato la sicurezza aerea[54], ma l'elevato livello di rischio cui è esposta l'aviazione civile richiede un mezzo per prevedere gli incidenti e consultare rapidamente gli Stati membri interessati. La Commissione collaborerà con gli Stati membri per modificare la vigente normativa di attuazione nel settore della sicurezza aerea, al fine di condividere informazioni classificate sugli **eventi relativi alla sicurezza aerea**. La Commissione inoltre prenderà in considerazione **misure normative** per far fronte a nuove minacce quali gli **incidenti che si verificano durante il trasporto aereo di merci** e per rendere più stringenti le norme sulla sicurezza aerea. Ciò comporterà anche il rafforzamento della **normativa sulla sicurezza aerea** per consentire misure di risposta immediata, mantenendo nel contempo la zona del sistema di sicurezza unico negli aeroporti dell'UE.

Nell'elaborare la **strategia portuale dell'UE** di prossima realizzazione sulla base dell'**alleanza europea dei porti**, la Commissione esaminerà le modalità per rafforzare ulteriormente la normativa in materia di sicurezza marittima al fine di fare efficacemente fronte alle minacce emergenti, garantire la sicurezza dei porti e rafforzare la sicurezza della catena di approvvigionamento dell'UE. A tal fine ne garantirà la rigorosa attuazione e si adopererà per armonizzare le pratiche nazionali e potenziare i controlli dei precedenti nei porti. Nella scia dei protocolli di sicurezza stabiliti per il trasporto aereo di merci, la Commissione collaborerà con gli Stati membri e il settore privato per ampliarli ai fini della sicurezza delle catene di trasporto marittimo.

La proposta autorità doganale dell'UE analizzerà e valuterà i rischi sulla base delle **informazioni doganali** relative alle merci in entrata, in uscita e in transito nell'UE, per aiutare gli Stati membri a prevenire lo sfruttamento delle catene di approvvigionamento internazionali da parte di attori malintenzionati. In linea con la strategia per la sicurezza marittima dell'UE[55], il prossimo **patto europeo per gli oceani** svolgerà un ruolo fondamentale nel rafforzare la sicurezza marittima nei bacini marittimi intorno all'UE e al di fuori di essa, anche incoraggiando il potenziamento delle operazioni e delle esercitazioni marittime multifunzionali.

Resilienza delle catene di approvvigionamento

L'Europa deve ridurre il ricorso alle tecnologie di paesi terzi, che può provocare rischi in fatto di dipendenza e sicurezza. La Commissione mira ad attenuare le dipendenze da singoli fornitori stranieri, mettere le catene di approvvigionamento al riparo dai fornitori ad alto rischio e garantire la sicurezza delle infrastrutture critiche e della capacità industriale sul suolo dell'UE,

[53] Regolamento (UE) 2024/2642 del Consiglio, dell'8 ottobre 2024, concernente misure restrittive in considerazione delle attività di destabilizzazione praticate dalla Russia (ST/8744/2024/INIT) (GU L, 2024/2642, 9.10.2024).
[54] Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile (GU L 97 del 9.4.2008, pag. 72).
[55] JOIN (2023) 8 final.

come si illustra nella **bussola per la competitività**[56]e nel **patto per l'industria pulita**[57]. La Commissione promuoverà una **politica industriale per la sicurezza interna** collaborando con gli operatori industriali dell'UE in settori chiave (ad esempio nodi di trasporto, infrastrutture critiche) per produrre soluzioni di sicurezza quali attrezzature di rilevamento, tecnologie biometriche e droni, integrando le caratteristiche di sicurezza fin dalla progettazione. Nel **rivedere le norme dell'UE in materia di appalti** la Commissione valuterà se le considerazioni in materia di sicurezza contenute nella direttiva del 2009 relativa agli appalti nel settore della difesa e della sicurezza[58] siano sufficienti per rispondere alle esigenze di resilienza dei soggetti critici e di contrasto.

La Commissione coadiuverà gli Stati membri nel **controllo degli investimenti esteri diretti (IED)** e nell'acquisizione di materiale per i poli logistici, garantendo la sicurezza delle infrastrutture e delle tecnologie critiche.

Una volta entrato in vigore, il **regolamento relativo alle emergenze e alla resilienza nel mercato interno (IMERA)** aiuterà l'UE a gestire le crisi che perturbano le catene di approvvigionamento critiche e la libera circolazione di merci, servizi e persone. Il regolamento consentirà di coordinare rapidamente le crisi e di individuare beni e servizi di rilevanza per le crisi; offrirà altresì un pacchetto di strumenti per garantirne la disponibilità. In stretta cooperazione con gli Stati membri, la Commissione proporrà di istituire un **meccanismo di allerta multiagenzia per la sicurezza dei trasporti e delle catene di approvvigionamento**, al fine di garantire la condivisione sicura e tempestiva delle informazioni necessarie per anticipare e contrastare le minacce.

Con l'attuazione del regolamento sulle materie prime critiche e del regolamento sull'industria a zero emissioni nette, il maggiore ricorso ai criteri di sostenibilità, resilienza e preferenza europea negli appalti pubblici dell'UE promuoverà lo sviluppo di mercati guida. Il rafforzamento dei legami commerciali, ad esempio mediante i partenariati sulle materie prime e i partenariati per il commercio e gli investimenti puliti, contribuirà a diversificare le catene di approvvigionamento.

Resilienza e preparazione alle minacce chimiche, biologiche, radiologiche e nucleari

La guerra di aggressione russa contro l'Ucraina ha aumentato il rischio di **minacce chimiche, biologiche, radiologiche e nucleari (CBRN)**. Per far fronte alla potenziale acquisizione e al possibile uso di materiali CBRN come arma, la Commissione sosterrà gli Stati membri e i paesi partner attraverso attività di formazione ed esercitazioni specifiche. La Commissione rafforzerà le capacità di preparazione e risposta CBRN con la definizione di un ordine di priorità delle minacce, il finanziamento dell'innovazione per le contromisure, le risorse rescEU e la costituzione di scorte di contromisure mediche, nell'ambito di un nuovo **piano d'azione per la preparazione e la risposta CBRN** La **strategia dell'UE sulle contromisure mediche** promuoverà lo sviluppo di contromisure mediche, dalla ricerca alla produzione fino alla distribuzione, per proteggere l'UE da pandemie e minacce CBRN.

Sulla base dell'esperienza della pandemia di COVID-19, l'UE ha rafforzato il quadro per la sicurezza sanitaria[59]. La Commissione sta designando laboratori di riferimento dell'UE per la

[56] COM (2025) 30 final.
[57] COM (2025) 85 final.
[58] Direttiva 2009/81/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa al coordinamento delle procedure per l'aggiudicazione di taluni appalti di lavori, di forniture e di servizi nei settori della difesa e della sicurezza da parte delle amministrazioni aggiudicatrici/degli enti aggiudicatori (GU L 216 del 20.8.2009, pag. 76).
[59] In particolare mediante il regolamento (UE) 2022/2371 relativo alle gravi minacce per la salute a carattere transfrontaliero.

sanità pubblica allo scopo di potenziare le capacità di sorveglianza e rilevamento rapido nazionali e dell'UE. Nel 2025 sarà pubblicato un piano dell'Unione per la preparazione, prevenzione e risposta in materia di sicurezza sanitaria.

Azioni fondamentali

La Commissione intende:

- **riesaminare e rivedere il regolamento sulla cibersicurezza nel 2025;**
- **elaborare misure per garantire la cibersicurezza nell'impiego dei servizi cloud;**
- **proporre una strategia portuale dell'UE nel 2025;**
- **rivedere le norme dell'UE in materia di appalti per la difesa e la sicurezza nel 2026;**
- **presentare un nuovo piano d'azione per la preparazione e la risposta CBRN nel 2026.**

La Commissione intende, in collaborazione con gli Stati membri:

- **sviluppare e realizzare l'infrastruttura europea di comunicazione quantistica (EuroQCI);**
- **garantire l'effettiva applicazione del regolamento sui servizi digitali;**
- **adoperarsi per contrastare l'uso della migrazione come arma;**
- **istituire un sistema di eventi relativi alla sicurezza aerea;**
- **adoperarsi per istituire un meccanismo di allerta multiagenzia per la sicurezza dei trasporti e delle catene di approvvigionamento;**

Il Consiglio è esortato a:

- **adottare la raccomandazione del Consiglio sul programma dell'UE per la cibersicurezza.**

Gli Stati membri sono esortati a:

- **recepire e attuare integralmente le direttive CER e NIS2.**

5. Serrare le maglie contro la criminalità organizzata e le forme gravi di criminalità

Contribuiremo a debellare la criminalità organizzata proponendo norme più rigorose per contrastare le sue reti, anche per quanto riguarda le indagini, a rendere i giovani dell'UE meno vulnerabili al reclutamento nelle fila della criminalità e a intensificare le misure per impedire l'accesso a proventi e strumenti di reato.

La criminalità organizzata sfrutta un panorama in evoluzione e si espande in maniera esponenziale; si giova di tecnologie avanzate, agisce in molteplici giurisdizioni e dispone di saldi legami oltre i confini dell'UE. Alla luce di queste minacce complesse e transnazionali, diventano essenziali il coordinamento e il sostegno a livello di Unione.

Prevenzione della criminalità

Il reclutamento di giovani nelle fila della criminalità organizzata è fonte di crescente preoccupazione nell'UE. Per combattere la criminalità organizzata è necessario affrontarne le **cause profonde**, offrendo istruzione e alternative a una vita dedita al crimine attraverso un approccio che coinvolga l'intera società. La Commissione è favorevole a integrare le considerazioni sulla sicurezza nelle politiche dell'UE in campo sociale e regionale e in materia

di istruzione e occupazione. L'UE **promuoverà politiche di prevenzione della criminalità basate su dati concreti**[60] e adattate ai contesti locali.

Per proteggere i destinatari dei servizi online, in particolare i minori, dagli autori di abusi sessuali su minori, dai trafficanti di esseri umani e dal reclutamento online nelle fila della criminalità o dell'estremismo violento, le misure previste dal **regolamento sui servizi digitali** impongono ai fornitori di piattaforme online accessibili ai minori di gestire i rischi e agire contro i contenuti illegali, compreso l'incitamento all'odio. La Commissione intende emanare **orientamenti sulla protezione dei minori** per aiutare i fornitori di piattaforme online a garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online. Gli orientamenti riporteranno una serie di raccomandazioni per tutti i servizi digitali che operano nell'Unione, al fine di migliorare la protezione dei minori online. Nel 2025 la Commissione prevede di favorire una soluzione di **verifica dell'età rispettosa della vita privata**, che colmerà la lacuna prima che sia disponibile il portafoglio EUDI alla fine del 2026. La Commissione presenterà un piano d'azione contro il bullismo online.

Continuerà inoltre a promuovere il dialogo volontario multipartecipativo con le piattaforme online e altri attori pertinenti, anche attraverso il forum dell'UE su internet e i codici di condotta mirati nell'ambito del regolamento sui servizi digitali, come il codice di condotta del 2025 contro l'incitamento all'odio online. L'obiettivo è quello di sensibilizzare, di dare una risposta comune alle minacce attuali ed emergenti e di produrre e condividere buone pratiche per le misure di attenuazione.

A livello locale l'impatto della criminalità organizzata mette in luce la necessità di soluzioni regionali per ridurre la vulnerabilità e l'attrattiva delle attività illegali. L'agenda dell'Unione per le città tratterà delle sfide di sicurezza che si profilano nelle città basandosi sull'iniziativa "Città dell'UE contro la radicalizzazione". La Commissione sosterrà gli Stati membri nel rafforzamento della sicurezza urbana e regionale attraverso il Fondo europeo di sviluppo regionale**.**

Basi e competenze educative più robuste costituiscono il fondamento di società resilienti e coese. Attraverso l'**Unione delle competenze** e il **piano d'azione per l'integrazione e l'inclusione**, l'Unione si adopererà per aiutare le persone a diventare più resilienti alla disinformazione volontaria e involontaria, alla radicalizzazione e al reclutamento nelle fila della criminalità.

La protezione dei minori da tutte le forme di violenza, tra cui la criminalità e la violenza fisica o mentale, online e offline, è uno degli obiettivi fondamentali dell'Unione. Per rispondere alle esigenze specifiche di gruppi particolarmente vulnerabili come i minori, che sono sempre più esposti al reclutamento e alla radicalizzazione, all'adescamento e agli abusi sessuali, al bullismo online, alla disinformazione e ad altre minacce, l'UE elaborerà un **piano d'azione per la protezione dei minori dalla criminalità** che comprenda le dimensioni online e offline. Definirà un approccio coerente e coordinato sulla base dei quadri e degli strumenti disponibili, tra cui il futuro Centro dell'UE di prevenzione e lotta contro l'abuso sessuale su minori e altri organi e organismi dell'UE, e proporrà soluzioni per le lacune che dovessero permanere.

Smantellare le reti criminali e i loro favoreggiatori

Occorre intensificare la lotta contro le reti criminali ad alto rischio, i loro capi e favoreggiatori. Nonostante gli importanti successi recenti[61], norme obsolete e definizioni incoerenti delle reti criminali ostacolano una risposta efficace della giustizia penale e la cooperazione transfrontaliera. La Commissione riesaminerà la legislazione obsoleta in questo settore,

[60] https://www.eucpn.org/.
[61] Compresi i recenti casi EMPACT.

proponendo un **quadro giuridico rinnovato sulla criminalità organizzata**, in grado di potenziare la risposta.

L'azione amministrativa può integrare l'attività di contrasto per ottenere risultati più rapidi, come dimostra l'opera svolta dall'EPPO e dall'Ufficio europeo per la lotta antifrode (OLAF) contro le **frodi transfrontaliere e i reati che ledono gli interessi finanziari dell'Unione**. Le frodi in materia di sovvenzioni si concentrano su settori quali le energie rinnovabili, i programmi di ricerca e l'agricoltura[62]. La Commissione esaminerà le modalità per coordinare l'uso degli strumenti penali e amministrativi, rafforzando la cooperazione con Europol, Eurojust e l'EPPO. Continuerà a sostenere una più ampia applicazione dell'**approccio amministrativo** per consentire alle autorità amministrative locali e ad altre autorità amministrative di stroncare le infiltrazioni criminali[63].

L'UE si adopera per rafforzare il quadro giuridico in materia di lotta contro la **corruzione**[64]. Il Parlamento europeo e il Consiglio dovrebbero concludere rapidamente i negoziati sul quadro anticorruzione aggiornato proposto dalla Commissione. La Commissione presenterà una strategia anticorruzione dell'UE per promuovere l'integrità e rafforzare il coordinamento fra tutte le autorità e i portatori di interessi in questo settore.

Le armi da fuoco sono uno degli elementi essenziali della sempre maggiore violenza di cui si rendono colpevoli i gruppi della criminalità organizzata. La Commissione proporrà norme comuni di diritto penale sul traffico illecito di armi da fuoco. Un nuovo **piano d'azione dell'UE sul traffico di armi da fuoco** sarà incentrato sulla salvaguardia del mercato legale, sulla limitazione delle attività criminali (grazie a una migliore intelligence) e sul consolidamento della cooperazione internazionale, con particolare attenzione all'Ucraina e ai Balcani occidentali.

Il commercio illegale di articoli pirotecnici utilizzati nei reati impone l'adozione di misure volte a migliorare la prevenzione e la tracciabilità. La Commissione valuta attualmente la direttiva sugli articoli pirotecnici e vaglierà anche l'ipotesi di prevedere **sanzioni penali per il traffico di tali articoli**.

Seguire le tracce del denaro

Seguire le tracce del denaro è fondamentale per combattere la criminalità organizzata e il terrorismo, ma rimane un'impresa assai ardua. Il nesso tra criminalità organizzata e flussi di denaro esige sforzi intensi e concertati per bloccare l'accesso delle reti criminali alle fonti di finanziamento e proteggere meglio i cittadini, le imprese e i bilanci pubblici.

L'UE ha intensificato l'impegno con le nuove norme antiriciclaggio, compresa l'istituzione dell'**Autorità dell'UE per la lotta al riciclaggio (AMLA)**[65]. La collaborazione tra AMLA, OLAF, EPPO, Eurojust ed Europol è essenziale per condurre indagini finanziarie efficaci. La Commissione sosterrà la creazione di **partenariati** volti sia a favorire la cooperazione tra agenzie sia a coinvolgere il settore privato.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.
[64] Proposta di direttiva del Parlamento europeo e del Consiglio sulla lotta contro la corruzione, che sostituisce la decisione quadro 2003/568/GAI del Consiglio e la convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea, e che modifica la direttiva (UE) 2017/1371 del Parlamento europeo e del Consiglio (COM(2023) 234 final del 3 maggio 2023).
[65] https://www.amla.europa.eu/index_it.

È essenziale eliminare le motivazioni finanziarie che stanno alla base della criminalità organizzata, sequestrare i beni e confiscare i proventi di reato. Gli Stati membri dovrebbero recepire senza indugio le norme più stringenti in materia di **recupero e confisca dei beni**[66] recentemente adottate, sfruttandone appieno il potenziale. La lotta contro i sistemi finanziari paralleli che eludono il quadro antiriciclaggio dell'UE, compresi i sistemi basati sulle cripto-attività, richiede azioni innovative, la condivisione delle migliori pratiche tra gli Stati membri e un maggiore sostegno da parte di Europol ed Eurojust. La Commissione esaminerà la fattibilità di un nuovo sistema a livello UE per monitorare i profitti della criminalità organizzata e il finanziamento del terrorismo e incoraggerà anche il passaggio di flussi di informazioni tempestivi e ampliati dalle **unità di informazione finanziaria** alle autorità di contrasto. La Commissione esaminerà le modalità per colmare le lacune, sosterrà gli Stati membri nello sviluppo di capacità e continuerà a operare per consolidare la cooperazione con i paesi terzi utilizzati abusivamente dai criminali per operazioni bancarie sotterranee.

Lotta alle forme gravi di criminalità

Oltre allo smantellamento delle reti criminali, la lotta contro le forme gravi di criminalità richiede iniziative mirate. Per rafforzare la capacità dell'UE di contrastare le **frodi online**, che provocano danni finanziari considerevoli[67], la Commissione sosterrà misure di prevenzione e più efficaci azioni di contrasto e collaborerà con gli Stati membri e i portatori di interessi per sostenere e proteggere le vittime, anche offrendo assistenza nel recupero dei fondi. Tali iniziative saranno formalizzate in un **piano d'azione sulle frodi online**.

Sulla base della strategia dell'UE 2020-2025 contro gli **abusi sessuali sui minori**[68], la Commissione sosterrà i colegislatori nella messa a punto delle due proposte legislative[69] volte a prevenire e contrastare l'abuso sessuale sui minori online e ad assicurare una maggiore efficacia delle azioni di contrasto contro l'abuso e lo sfruttamento sessuale dei minori. Fino all'aprile 2026 saranno in vigore norme provvisorie, ma è essenziale istituire un quadro giuridico permanente: la Commissione incoraggia i colegislatori ad avviare negoziati sul progetto di regolamento che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori. Si invitano inoltre i colegislatori a progredire sulla strada dei negoziati concernenti la direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e il materiale pedopornografico, che stabilirà norme minime sulla definizione dei reati e delle sanzioni in materia di sfruttamento sessuale dei minori.

La metà delle reti criminali più pericolose dell'UE è implicata nel **traffico violento di droga**. Sebbene l'UE abbia recentemente intensificato la lotta contro questo tipo di criminalità[70], in particolare ampliando il mandato dell'**Agenzia dell'Unione europea sulle droghe**, sono necessarie ulteriori azioni. La Commissione lavorerà in stretta collaborazione con gli Stati membri per proporre una nuova **strategia dell'UE in materia di droghe**. Riesaminerà il **quadro giuridico sui precursori di droghe** e proporrà un **piano d'azione dell'UE contro il traffico di droga** per smantellare le rotte di approvvigionamento e perturbare i modelli di attività**.** Il **partenariato pubblico-privato dell'alleanza europea dei porti**, destinato a rafforzare la protezione dei porti, sarà esteso ai porti più piccoli e interni e garantirà l'applicazione delle norme di sicurezza marittima. Consapevole dei gravi effetti locali del traffico di droga, la Commissione continuerà a sostenere una politica in materia di droga

[66] Direttiva (UE) 2024/1260 del Parlamento europeo e del Consiglio, del 24 aprile 2024, riguardante il recupero e la confisca dei beni (GU L, 2024/1260, 2.5.2024).
[67] Global Anti-Scam Report 2024.
[68] COM (2020) 607 final
[69] COM (2022) 209 final e COM (2024) 60 final.
[70] COM (2023) 641 final.

equilibrata, basata su dati concreti e multidisciplinare, che permetta di far fronte a improvvisi afflussi di droghe, in particolare di oppioidi sintetici.

Per combattere lo sfruttamento delle persone l'UE ha adottato nuove norme[71] e introdurrà una **strategia rinnovata dell'UE per la lotta alla tratta di esseri umani** (2026-2030), che spazierà su tutte le fasi, dalla prevenzione all'azione penale, con particolare attenzione per il sostegno alle vittime a livello sia internazionale che di Unione.

Nella lotta contro il **traffico di migranti**, la Commissione guiderà le iniziative con i partner fondamentali tramite la nuova alleanza mondiale per contrastare il traffico di migranti, in cooperazione con Europol, Eurojust e Frontex, anche nella dimensione online. Occorre adottare e attuare senza indugio le proposte della Commissione in materia di lotta contro il traffico di migranti[72]. A seguito dell'adozione del **pacchetto di misure sugli operatori dei trasporti**[73], la Commissione ha intensificato l'attività di informazione rivolta alle autorità e agli operatori stranieri e continuerà a dialogare con il settore aeronautico e le organizzazioni dell'aviazione civile[74] per sensibilizzare in merito al traffico di migranti per via aerea[75].

La **criminalità ambientale** minaccia a lungo termine l'ambiente, la salute pubblica e le economie. La Commissione sosterrà gli Stati membri nell'attuazione della direttiva sulla tutela penale dell'ambiente[76] e rafforzerà le azioni e le reti operative in questo settore[77]. Una rigorosa azione di contrasto è essenziale. La recente Convenzione del Consiglio d'Europa sulla protezione dell'ambiente attraverso il diritto penale[78] contribuirà ad attività di contrasto alla criminalità ambientale risolute e comparabili, sia in Europa che nel resto del mondo.

Risposta della giustizia penale

La criminalità e il terrorismo possono colpire ognuno di noi; è quindi essenziale promuovere e salvaguardare i diritti delle **vittime** al fine di ridurre i danni e accrescere la sicurezza generale e la fiducia nelle autorità. Sulla base della direttiva riguardante i diritti delle vittime, la Commissione introdurrà una nuova **strategia dell'UE sui diritti delle vittime**.

I **sistemi di giustizia penale dell'UE** necessitano di strumenti efficaci per fare fronte alle minacce emergenti. A tal fine la Commissione ha varato un **forum ad alto livello sul futuro della giustizia penale dell'UE**, che riunisce gli Stati membri, il Parlamento europeo, gli organi e gli organismi dell'UE e altri portatori di interessi. Il forum si prefigge l'obiettivo di discutere le modalità per garantire che i sistemi di giustizia penale dell'UE rimangano efficaci, equi e

[71] Direttiva (UE) 2024/1712 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che modifica la direttiva 2011/36/UE concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime (GU L, 2024/1712, 24.6.2024).
[72] COM (2023) 755 final e COM (2023) 754 final.
[73] Pacchetto di strumenti per contrastare l'utilizzo di mezzi di trasporto commerciali per favorire la migrazione irregolare verso l'UE.
[74] Tra cui l'Organizzazione per l'aviazione civile internazionale (ICAO).
[75] La Commissione promuoverà altresì la messa a punto del regolamento relativo a misure nei confronti degli operatori di trasporto che agevolano o praticano la tratta di persone o il traffico di migranti, COM(2021) 753 final.
[76] Direttiva (UE) 2024/1203 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, sulla tutela penale dell'ambiente (GU L, 2024/1203, 30.4.2024).
[77] Rete dell'UE per l'attuazione e l'applicazione della normativa ambientale (IMPEL), Rete europea dei procuratori per l'ambiente (ENPE), EnviCrimeNet e Forum europeo - Unione dei giudici per l'ambiente (EUFJE).
[78] Comitato di esperti sulla protezione dell'ambiente attraverso il diritto penale (PC-ENV) - Comitato europeo per i problemi criminali (CDPC).

resilienti in un contesto di sfide in evoluzione, rafforzando nel contempo la cooperazione giudiziaria e la fiducia reciproca, anche attraverso la digitalizzazione[79].

Azioni fondamentali

La Commissione intende:

- **presentare una proposta legislativa per modernizzare le norme sulla criminalità organizzata nel 2026;**
- **presentare una proposta legislativa per rivedere il quadro giuridico sui precursori di droghe nel 2025;**
- **presentare una proposta legislativa relativa a norme di diritto penale comuni sul traffico illecito di armi da fuoco nel 2025;**
- **valutare la necessità di rivedere le direttive sugli articoli pirotecnici e sugli esplosivi per uso civile;**
- **valutare la necessità di rafforzare ulteriormente l'ordine europeo di indagine e il mandato d'arresto europeo;**
- **presentare una nuova strategia dell'UE per la lotta alla tratta degli esseri umani nel 2026;**
- **presentare una nuova strategia dell'UE sui diritti delle vittime nel 2026;**
- **presentare un piano d'azione per la protezione dei minori dalla criminalità entro il 2027;**
- **presentare un piano d'azione dell'UE contro il traffico di droga nel 2025;**
- **presentare un piano d'azione dell'UE sul traffico di armi da fuoco nel 2026;**
- **ampliare successivamente l'Alleanza europea dei porti a partire dal 2025;**
- **adottare gli orientamenti sulla protezione dei minori previsti dal regolamento sui servizi digitali nel 2026;**
- **presentare un piano d'azione dell'UE contro il bullismo online nel 2026.**

Gli Stati membri sono esortati a:

- **recepire integralmente le nuove norme in materia di recupero e confisca dei beni entro la fine del 2026 sfruttandone appieno il potenziale;**
- **attuare l'approccio amministrativo nella lotta contro le infiltrazioni criminali;**
- **istituire partenariati pubblico-privato contro il riciclaggio di denaro;**
- **recepire e attuare integralmente la direttiva sulla lotta alla violenza contro le donne e alla violenza domestica.**

Il Parlamento europeo e il Consiglio sono esortati a:

- **progredire sulla strada dei negoziati concernenti il regolamento che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori e la direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e il materiale pedopornografico;**
- **concludere i negoziati sulla direttiva sulla lotta contro la corruzione.**

[79] In particolare con l'elaborazione della comunicazione nell'ambito della giustizia elettronica attraverso lo scambio di dati online (eCODEX) e del sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN).

6. Lotta al terrorismo e all'estremismo violento

L'Unione introdurrà una nuova agenda globale antiterrorismo per prevenire la radicalizzazione, mantenere in sicurezza gli spazi online e pubblici, bloccare i canali di finanziamento e rispondere agli attacchi quando si verificano

Il livello della minaccia terroristica nell'UE rimane elevato ed è strettamente connesso agli effetti di ricaduta degli eventi geopolitici, delle nuove tecnologie e dei nuovi mezzi di finanziamento del terrorismo. Occorre che l'UE disponga degli strumenti necessari per anticipare le minacce, prevenire la radicalizzazione (sia offline che online), proteggere i cittadini e gli spazi pubblici dagli attacchi e rispondere efficacemente agli attacchi quando si verificano. Nel 2025 sarà presentato **un nuovo programma dell'UE per la prevenzione e la lotta al terrorismo e all'estremismo violento**, volto a delineare la futura azione dell'UE. In linea con il nuovo programma, nel 2025 l'UE e i Balcani occidentali firmeranno il nuovo **piano d'azione comune** per la prevenzione e la lotta al terrorismo e all'estremismo violento.

Prevenzione della radicalizzazione e protezione delle persone online

Analogamente a quanto avviene nella lotta contro la criminalità organizzata, per contrastare il terrorismo e l'estremismo violento occorre anzitutto **affrontarne le cause profonde**. Il **polo di conoscenze dell'UE sulla prevenzione della radicalizzazione** intensificherà il sostegno agli operatori e ai responsabili politici con un nuovo **pacchetto completo di strumenti per la prevenzione**, così da consentire un'individuazione precoce e interventi incentrati sulle persone vulnerabili, in particolare i minori**.** La radicalizzazione avviene spesso nelle carceri; per aiutare gli Stati membri ad affrontare la questione la Commissione formulerà nuove raccomandazioni.

Terroristi ed estremisti violenti utilizzano le piattaforme online per diffondere contenuti terroristici e dannosi, raccogliere fondi e svolgere opera di reclutamento. La radicalizzazione online degli utenti vulnerabili, in particolare dei minori, segna un ritmo allarmante. Il **regolamento relativo al contrasto della diffusione di contenuti terroristici online** è stato determinante per contrastare la diffusione di tali contenuti, giacché consente la rapida rimozione del materiale più odioso e pericoloso[80]. La Commissione ne valuta attualmente il funzionamento e individuerà il modo migliore per rafforzarlo.

Il **protocollo di crisi dell'UE** per una rapida risposta comune delle autorità di contrasto e del settore tecnologico a un attacco terroristico sarà modificato in modo da garantire scalabilità e flessibilità per rispondere alla sempre più accentuata dimensione online degli attacchi terroristici. Il Forum dell'UE su internet rimarrà il principale luogo di cooperazione volontaria con il settore tecnologico per contrastare i contenuti terroristici e dannosi online. La Commissione s'impegna in iniziative internazionali quali la Christchurch Call Foundation e il Forum Internet mondiale per la lotta contro il terrorismo (GIFCT).

Contrasto al finanziamento del terrorismo

I terroristi finanziano le proprie attività con campagne di crowdfunding, cripto-attività, neobanche o piattaforme di pagamento online. Le autorità di contrasto devono individuare questi flussi finanziari e indagare su di essi, cosa che richiede mezzi, strumenti e competenze. La **rete di investigatori finanziari antiterrorismo** assolve una funzione fondamentale. La Commissione esaminerà la possibilità di costituire un **nuovo sistema a livello di Unione per tracciare i finanziamenti diretti al terrorismo**, che abbracci le operazioni all'interno dell'UE e della SEPA, i trasferimenti di cripto-attività e i pagamenti online ed elettronici, a

[80] Al 31 dicembre 2024 erano stati emessi 1 426 ordini di rimozione per eliminare contenuti terroristici o bloccarne l'accesso; la maggior parte di questi ordini ha colpito contenuti terroristici jihadisti ma anche contenuti terroristici di destra.

integrazione dell'accordo UE-USA sul programma di controllo delle transazioni finanziarie dei terroristi (TFTP).

Occorre **proteggere** il bilancio dell'UE **da abusi volti a promuovere opinioni radicali/estremistiche** negli Stati membri. Il **regolamento finanziario** riveduto include ora una condanna per "aver incitato alla discriminazione, all'odio o alla violenza" tra i motivi di esclusione dai finanziamenti dell'UE. La Commissione continuerà a esaminare le modalità migliori per sfruttare l'intero potenziale del pacchetto di strumenti, anche in sede di selezione dei potenziali beneficiari. La protezione del bilancio dell'UE dipende anche da una solida cooperazione e condivisione di informazioni con le autorità nazionali, gli organi e gli organismi dell'UE.

Protezione dagli attacchi

Oltre agli investimenti nella prevenzione della radicalizzazione, una componente importante della protezione dei cittadini consiste nel limitare i mezzi a disposizione dei terroristi e dei criminali per commettere attacchi. È necessario intervenire sia sugli strumenti utilizzati dai terroristi sia per proteggere gli obiettivi a rischio di attacco.

Oltre alle azioni intraprese per le armi da fuoco, la Commissione **riesaminerà le norme** sui **precursori di esplosivi** per includervi le sostanze chimiche ad alto rischio. Gli **spazi pubblici** rimangono gli obiettivi più comuni per gli attacchi terroristici, in particolare per i "lupi solitari". Per tutelare i cittadini, il **programma dei consulenti UE sulla sicurezza protettiva** sarà rafforzato così che possa effettuare valutazioni delle vulnerabilità degli spazi pubblici, delle infrastrutture critiche e degli eventi ad alto rischio, su richiesta degli Stati membri e con il finanziamento del bilancio dell'UE nell'ambito del Fondo Sicurezza interna. L'UE punterà ad ampliare i finanziamenti disponibili per la protezione dello spazio pubblico. La Commissione sostiene le autorità degli Stati membri e gli operatori privati con orientamenti e strumenti specifici, come il polo della conoscenza sulla protezione degli spazi pubblici[81]; dal 2020 ha già messo a disposizione a tale scopo 70 milioni di EUR.

La Commissione vaglierà l'ipotesi di introdurre requisiti che impongano alle organizzazioni di prendere in considerazione o utilizzare misure di sicurezza nei luoghi accessibili al pubblico, tramite un dialogo con le autorità locali e i partner privati.

Date le evidenti vulnerabilità, la **strategia dell'UE 2021-2030 sulla lotta contro l'antisemitismo e il sostegno alla vita ebraica** continuerà a guidare le azioni della Commissione per proteggere la comunità ebraica. La Commissione curerà la messa a punto di strumenti adeguati per coadiuvare gli Stati membri nella lotta contro l'**odio anti-islamico.**

L' uso di **droni** per lo spionaggio e gli attacchi rappresenta una sfida sempre più grave per la sicurezza. La Commissione elaborerà una **metodologia di prova armonizzata per i sistemi antidrone**, istituirà un **centro di eccellenza antidrone** e valuterà la necessità di armonizzare la normativa e le procedure degli Stati membri[82].

Combattenti terroristi stranieri

Per identificare alle frontiere esterne dell'UE i combattenti terroristi stranieri sulla via del ritorno o in procinto di entrare, è necessario disporre di dati sulle persone che costituiscono una minaccia terroristica. A tal fine la Commissione, insieme a Europol, intensificherà la **cooperazione con i principali paesi terzi per ottenere i dati biografici e biometrici di persone che potrebbero costituire una minaccia terroristica**, tra cui i combattenti terroristi

[81] Polo della conoscenza sulla protezione degli spazi pubblici.

[82] Facendo seguito alla serie di azioni fondamentali contenute nella comunicazione del 2023 sul contrasto alle potenziali minacce poste dai droni, COM(2023) 659 final.

stranieri, che potranno poi essere inseriti nel sistema d'informazione Schengen nel totale rispetto dei quadri giuridici nazionali e dell'UE applicabili. È pertanto fondamentale che gli Stati membri utilizzino tutti gli strumenti esistenti. Ciò comprende l'inserimento di tutte le informazioni utili nel **SIS**, il perfezionamento dei controlli biometrici e lo svolgimento di verifiche sistematiche obbligatorie su tutte le persone alle frontiere esterne dell'UE[83]. Le autorità di controllo delle frontiere degli Stati membri continueranno a giovarsi degli **indicatori comuni di rischio** sviluppati da Frontex per individuare e valutare il rischio di viaggi sospetti da parte di potenziali combattenti terroristi stranieri.

Affinché gli Stati membri mantengano l'accesso alle **prove raccolte sul campo di battaglia** dalla squadra investigativa delle Nazioni Unite per la promozione dell'assunzione di responsabilità per i reati commessi dal Da'esh/ISIL (UNITAD) al fine di perseguire i combattenti terroristi stranieri, la Commissione vaglierà insieme a Eurojust la possibilità di conservare tali prove nella banca dati di Eurojust sulle prove di crimini internazionali fondamentali. Il nuovo **registro giudiziario europeo antiterrorismo** continuerà a sostenere le autorità giudiziarie degli Stati membri nella rapida individuazione dei collegamenti transfrontalieri nei casi di terrorismo.

Azioni fondamentali

La Commissione intende:

- **adottare un nuovo programma dell'UE per la prevenzione e la lotta al terrorismo e all'estremismo violento nel 2025;**
- **firmare con i Balcani occidentali un nuovo piano d'azione comune per la prevenzione e la lotta al terrorismo e all'estremismo violento nel 2025;**
- **sviluppare un nuovo pacchetto completo di strumenti per la prevenzione con il polo di conoscenze dell'UE;**
- **valutare l'applicazione del regolamento relativo al contrasto della diffusione di contenuti terroristici online nel 2026;**
- **modificare il protocollo di crisi dell'UE nel 2025;**
- **presentare una proposta legislativa per rivedere il regolamento relativo all'immissione sul mercato e all'uso di precursori di esplosivi nel 2026;**
- **valutare la fattibilità di un nuovo sistema UE per tracciare i finanziamenti destinati al terrorismo.**

Gli Stati membri sono esortati a:

- **perfezionare i controlli biometrici e svolgere verifiche sistematiche obbligatorie alle frontiere esterne dell'UE;**
- **avvalersi pienamente del registro giudiziario europeo antiterrorismo.**

7. Ruolo mondiale dell'UE incisivo per la sicurezza

Per rafforzare la sicurezza dell'UE promuoveremo la cooperazione operativa attraverso partenariati con regioni fondamentali come i partner dell'allargamento e del vicinato, l'America latina e la regione mediterranea. Gli interessi dell'UE in materia di sicurezza saranno presi in considerazione nella cooperazione internazionale, anche sfruttando gli strumenti di cui l'UE dispone.

[83] Nel totale rispetto del codice frontiere Schengen e del regolamento sugli accertamenti.

Negli ultimi anni sono emersi con evidenza i nessi che legano intrinsecamente la sicurezza esterna e quella interna dell'UE. La guerra di aggressione russa contro l'Ucraina, il conflitto a Gaza, la situazione in Siria e i conflitti emergenti in tutto il mondo hanno avuto gravi effetti di ricaduta sulla sicurezza interna dell'UE. Per contrastare l'impatto dell'instabilità globale sulla sua sicurezza interna, l'**UE deve difendere attivamente i propri interessi in materia di sicurezza** facendo fronte alle minacce esterne, smantellando le rotte del traffico e tutelando i corridoi di interesse strategico come le rotte commerciali. Allo stesso tempo l'UE resterà un solido alleato per i paesi partner, deciso a collaborare per rafforzare la sicurezza mondiale e accrescere la resilienza reciproca contro le minacce.

Negli ultimi anni l'UE ha adottato misure significative per rafforzare la cooperazione in materia di sicurezza. Ha concluso accordi operativi in materia di cooperazione giudiziaria e di contrasto e altri tipi di accordi con i paesi partner. Persegue attivamente la conclusione di ulteriori accordi internazionali, in linea con le direttive di negoziato impartite dal Consiglio, e iniziative di sviluppo delle capacità, grazie al sostegno degli organi e degli organismi dell'UE. Lo strumento NDICI-Europa globale è fondamentale anche per rafforzare la sicurezza con i paesi partner.

L'**ordine multilaterale basato su regole** è uno dei fondamenti per rinsaldare la sicurezza globale. I dialoghi sulla sicurezza, compresi quelli tematici, sono essenziali per consolidare le iniziative in tal senso. L'attuazione della **bussola strategica per la sicurezza e la difesa**, unita a modalità di cooperazione bilaterale e multilaterale come gli accordi di stabilizzazione e di associazione e gli accordi di associazione, e la collaborazione con organizzazioni come l'ONU e la NATO sono fondamentali per sviluppare soluzioni di sicurezza efficaci. L'UE continuerà a fare la sua parte nei consessi multilaterali[84] e intensificherà la cooperazione con le organizzazioni e le sedi internazionali e regionali d'interesse, tra cui la NATO, le Nazioni Unite, il Consiglio d'Europa, Interpol, il G7, l'OSCE e la società civile.

Cooperazione regionale

Il continuo e deciso sostegno dell'UE all'**Ucraina**, insieme al potenziamento della sicurezza e della resilienza dei **paesi interessati dall'allargamento dell'UE**, costituisce un imperativo politico e geostrategico prioritario. Il sostegno alla sicurezza dell'UE dovrebbe andare di pari passo con l'**integrazione accelerata dei paesi candidati** nell'**architettura di sicurezza dell'UE**, parallelamente al consolidamento della cooperazione regionale. La Commissione utilizzerà la politica di allargamento dell'UE per sostenere le capacità dei paesi candidati e potenziali candidati di rispondere alle minacce, intensificare la cooperazione operativa e lo scambio di informazioni e garantire l'allineamento ai principi, alla legislazione e agli strumenti dell'UE. Lo strumento di assistenza preadesione (IPA III) e gli strumenti per l'Ucraina, la Moldova e i Balcani occidentali sono elementi fondamentali per il consolidamento della sicurezza sia nei paesi candidati che nei potenziali candidati.

L'UE integrerà ulteriormente i **partner del vicinato** nell'architettura di sicurezza dell'UE. Mediante il **nuovo patto per il Mediterraneo** e il prossimo **approccio strategico nei confronti del Mar Nero**, l'Unione intende proseguire verso la cooperazione regionale e la conclusione di partenariati strategici globali bilaterali che prevedano una dimensione di sicurezza e se del caso dialoghi periodici ad alto livello in materia di sicurezza. S'intensificherà la cooperazione operativa con il Nord Africa, il **Medio Oriente e il Golfo**, in particolare per quanto riguarda la

[84] Forum globale contro il terrorismo, Coalizione internazionale per combattere il Da'esh, Forum Internet mondiale per la lotta contro il terrorismo (GIFCT), Christchurch Call Foundation, Coalizione globale per affrontare le minacce delle droghe sintetiche.

lotta al terrorismo e al riciclaggio, al traffico di armi da fuoco e alla produzione e al traffico di droga, in particolare del Captagon**.**

Per far fronte alla crescente aggressività delle attività terroristiche e criminali e ai potenziali effetti di ricaduta nell'**Africa subsahariana, soprattutto nel Sahel, nel Corno d'Africa e nell'Africa occidentale**, l'UE intensificherà il sostegno all'Unione africana, alle comunità economiche regionali e ai paesi della regione. In linea con la strategia per la sicurezza marittima dell'UE[85], l'Unione intensificherà la cooperazione nel **Golfo di Guinea, nel Mar Rosso e nell'Oceano Indiano** per contrastare i traffici e la pirateria, promuovendo la cooperazione intra-africana e regionale anche con il sostegno delle presenze marittime coordinate dell'UE e del Centro di analisi e operazioni contro il narcotraffico marittimo (MAOC-N).

Con l'**America latina e i Caraibi** l'UE rafforzerà la cooperazione operativa per smantellare e perseguire le reti criminali ad alto rischio e smantellare le attività illecite e le rotte del traffico, potenziando i quadri di cooperazione, come l'UE-CLASI (comitato latino-americano per la sicurezza interna) e il meccanismo di coordinamento e cooperazione sulle droghe UE-CELAC. Tra le priorità figureranno la resilienza dei poli logistici, i partenariati e gli approcci ispirati al principio "seguire le tracce del denaro". L'UE sosterrà ulteriormente lo sviluppo della comunità di polizia delle Americhe (AMERIPOL) affinché diventi l'equivalente regionale di Europol e rafforzi la cooperazione giudiziaria tra gli Stati membri e la regione. L'UE collaborerà con l'**Asia meridionale e centrale** sulle sfide comuni in materia di sicurezza connesse al terrorismo, al traffico di merci illecite (tra cui le droghe), alla tratta di esseri umani e al traffico di migranti.

L'Unione sosterrà inoltre i quadri di cooperazione regionale nei paesi terzi per aiutarli ulteriormente a bloccare il traffico illecito alla fonte, in linea con il principio della responsabilità condivisa per l'intera catena di approvvigionamento criminale. L'UE farà altresì la sua parte per contribuire a rafforzare la sicurezza dei poli logistici all'estero, coordinando **ispezioni comuni nei porti dei paesi terzi**.

Cooperazione operativa

Il **Global Gateway** promuoverà progetti infrastrutturali sostenibili e di alta qualità nei settori digitale, climatico ed energetico, dei trasporti, della sanità, dell'istruzione e della ricerca. Se del caso la Commissione includerà ora nei futuri investimenti del Global Gateway considerazioni in materia di sicurezza, tra cui iniziative fondamentali per l'autonomia strategica dell'UE e dei suoi paesi partner, come i progetti infrastrutturali che comprendono valutazioni della sicurezza e misure di attenuazione dei rischi.

La Commissione perseguirà la conclusione di ulteriori **accordi tra l'UE e i paesi terzi sulla cooperazione con Europol ed Eurojust**, in particolare con i paesi dell'America latina.

La partecipazione proattiva dei paesi terzi all'**EMPACT** è uno dei mezzi più efficaci per intensificare la cooperazione operativa: l'UE incoraggerà ulteriormente il coinvolgimento di paesi terzi, in particolare dei paesi dei Balcani occidentali, del vicinato orientale, dell'Africa subsahariana, del Nord Africa, del Medio Oriente, dell'America latina e dei Caraibi. Un altro strumento per intensificare la cooperazione con i paesi terzi in materia di lotta alla criminalità è costituito dalle task force operative formate da diversi Stati membri e coordinate da Europol alle quali i paesi terzi possono partecipare. La Commissione intende concludere i negoziati per l'accordo internazionale **UE-Interpol** [86], ai fini di un approccio maggiormente unitario alle minacce alla sicurezza globale e alla lotta contro i reati transnazionali.

[85] JOIN (2023) 8 final.
[86] Decisione (UE) 2021/1312 del Consiglio, del 19 luglio 2021, e decisione (UE) 2021/1313 del Consiglio, del 19 luglio 2021.

L'**Unione deve essere presente sul campo con un approccio Team Europa**. Il personale specializzato dell'Unione e degli Stati membri assolve una funzione fondamentale a garanzia di un'azione esterna dell'UE ben informata, coordinata e reattiva. Per innalzare di livello tale approccio la Commissione, con il sostegno dell'alto rappresentante per gli affari esteri e la politica di sicurezza, rafforzerà le **reti di collegamento** e agevolerà l'impiego di **funzionari di collegamento regionali Europol ed Eurojust**, in linea con le esigenze operative degli Stati membri.

L'UE punterà a rinsaldare la cooperazione operativa tra autorità di contrasto e giudiziarie, promuoverà la condivisione di informazioni in tempo reale e le operazioni comuni attraverso **squadre investigative comuni** nei paesi terzi con il sostegno di Europol ed Eurojust. La Commissione sosterrà gli Stati membri nella creazione di **centri di fusione comuni** che riuniscano esperti e operatori dei servizi locali di contrasto nei paesi terzi strategici.

Strumenti di politica estera e di sicurezza comune (PESC)

Si sfrutteranno inoltre appieno le **missioni della politica di sicurezza e di difesa comune (PSDC)** allo scopo di individuare e affrontare con maggiore efficacia le minacce esterne alla sicurezza interna dell'UE, in linea con i rispettivi mandati stabiliti dal Consiglio. Per sviluppare le capacità dei paesi terzi l'alto rappresentante per gli affari esteri e la politica di sicurezza e la Commissione sosterranno le azioni della PSDC con appositi strumenti di finanziamento ed esploreranno tutte le possibilità di finanziamento adeguate.

Le **misure restrittive dell'UE** sono uno strumento della PESC consolidato, utilizzato anche per la lotta contro il terrorismo. Sulla base dei suggerimenti dell'alto rappresentante per gli affari esteri e la politica di sicurezza, degli Stati membri o della Commissione, il Consiglio potrebbe valutare il modo in cui rendere più efficaci, operative e agili le vigenti misure restrittive autonome dell'UE (elenco UE dei terroristi). Il Consiglio potrebbe valutare la possibilità di esplorare ulteriori misure restrittive nei confronti delle reti criminali, in linea con gli obiettivi della PESC.

Politica in materia di visti e scambio di informazioni

La politica dell'UE in materia di visti è uno strumento fondamentale per cooperare con i paesi terzi e rendere sicure le nostre frontiere controllando l'ingresso nell'UE e stabilendo le relative condizioni. La Commissione integrerà pienamente le **considerazioni di sicurezza nella politica dell'UE in materia di visti** mediante una prossima strategia dell'UE in questo campo. La Commissione collaborerà con i colegislatori per adottare la proposta di revisione e ottimizzazione del meccanismo di sospensione dei visti, in particolare per casi specifici di uso improprio del regime di esenzione dal visto[87]. I paesi terzi saranno incoraggiati a condividere informazioni sulle persone che possono comportare minacce alla sicurezza; tali informazioni saranno inserite nei sistemi di informazione e nelle banche dati dell'UE.

Per coordinare le politiche e intervenire a monte dando vita a una cooperazione più efficiente, rapida e agevole, la Commissione opererà per istituire **accordi sul flusso di dati** e prenderà in esame modalità per **migliorare lo scambio di informazioni** a fini di contrasto e di gestione delle frontiere con paesi terzi di fiducia, nel rispetto dei diritti fondamentali e delle norme in materia di protezione dei dati.

Azioni fondamentali
La Commissione intende:

[87] COM (2023) 642.

- **concludere accordi internazionali tra l'UE e i paesi terzi prioritari sulla cooperazione con Europol ed Eurojust;**
- **incoraggiare la partecipazione dei paesi partner all'EMPACT per combattere la criminalità organizzata e il terrorismo;**
- **sostenere gli organi e gli organismi dell'UE nella definizione e nel rafforzamento delle modalità operative con i paesi partner;**
- **rispecchiare ulteriormente le considerazioni di sicurezza nella politica dell'UE in materia di visti mediante la prossima strategia in questo campo;**
- **potenziare lo scambio di informazioni con paesi terzi di fiducia a fini di contrasto e di gestione delle frontiere.**

La Commissione, in cooperazione con l'alto rappresentante per gli affari esteri, intende:

- **sfruttare appieno le missioni civili nell'ambito della politica di sicurezza e di difesa comune (PSDC);**
- **coordinare le ispezioni comuni nei porti dei paesi terzi entro il 2027.**

La Commissione, in collaborazione con l'alto rappresentante per gli affari esteri e gli Stati membri, intende:

- **rafforzare le reti di collegamento e la cooperazione con un approccio Team Europa;**
- **costituire centri di fusione e squadre operative comuni nei paesi terzi a partire dal 2025.**

Il Parlamento europeo e il Consiglio sono esortati a:

- **concludere i negoziati sulla revisione del meccanismo di sospensione dei visti.**

8. Conclusioni

In un mondo denso di incertezze è necessario potenziare la capacità dell'Unione di anticipare e prevenire le minacce alla sicurezza e rispondervi.

Non è sufficiente limitarsi a rispondere alle crisi quando si verificano. Dobbiamo rafforzare la consapevolezza con un quadro completo delle minacce nella loro progressiva evoluzione, e far sì che gli strumenti e le capacità a nostra disposizione siano all'altezza del compito.

La serie completa di misure illustrate in dettaglio nella presente strategia contribuirà a creare un'Unione più forte nel mondo: un'Unione in grado di anticipare e pianificare le proprie esigenze di sicurezza e provvedervi, in grado di reagire efficacemente alle minacce alla sicurezza interna e di chiamare i responsabili a rispondere delle loro azioni, e che protegge le società e le democrazie che la compongono, aperte, libere e prospere.

A questo scopo s'impone un cambiamento di mentalità per quanto riguarda la sicurezza interna. Lavoreremo per contribuire a promuovere una nuova cultura della sicurezza dell'UE, in cui si tenga conto delle considerazioni in materia di sicurezza in ogni aspetto della legislazione, delle politiche e dei programmi, dall'inizio all'attuazione, e in cui la collaborazione tra i vari settori di intervento ci consenta di gettare nuove basi.

Questo compito non spetta a una sola istituzione, a un singolo governo o a un unico attore: è un'impresa comune dell'Europa.