

dossier

XIX Legislatura

4 novembre 2024

15^a riunione del Gruppo di controllo parlamentare congiunto su Europol (JPSG)

Bruxelles, 12 novembre 2024



XIX LEGISLATURA

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

15^a riunione del Gruppo di controllo
parlamentare congiunto su Europol (JPSG)

Bruxelles, 12 novembre 2024

SENATO DELLA REPUBBLICA

SERVIZIO STUDI

SERVIZIO DEGLI AFFARI INTERNAZIONALI

UFFICIO DEI RAPPORTI CON LE ISTITUZIONI
DELL'UNIONE EUROPEA

N. 96

CAMERA DEI DEPUTATI

UFFICIO RAPPORTI CON L'UNIONE
EUROPEA

N. 51



SERVIZIO STUDI

TEL. 06 6706 2451 - studi1@senato.it - ✉ [@SR_Studi](https://www.instagram.com/SR_Studi)

Dossier n. 96

SERVIZIO DEGLI AFFARI INTERNAZIONALI

Ufficio dei rapporti con le istituzioni dell'Unione Europea

TEL. 06 6706 5785 – affeuropei@senato.it



UFFICIO RAPPORTI CON L'UNIONE EUROPEA

TEL. 06 6760 2145 - cdmue@camera.it - ✉ [@CD_europa](https://www.instagram.com/CD_europa) - europa.camera.it.

Dossier n. 51

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

L'ORDINE DEL GIORNO E L'ARTICOLAZIONE DELLA RIUNIONE

In base al programma, la riunione del Gruppo congiunto di controllo parlamentare si articolerà in due grandi fasi

Quella antimeridiana prevede, dopo gli interventi introduttivi, diversi temi all'ordine del giorno, connessi ad aspetti generali dell'attività di EUROPOL e ad alcuni adempimenti procedurali:

- la **nomina dei componenti del Forum consultivo sui diritti fondamentali** che assisterà Europol nella sua attività;
- la presentazione della bozza del **Documento di programmazione pluriennale** per Europol 2025-2027;
- una presentazione sulla **protezione dei dati** da parte dell'Agenzia, seguita da eventuale discussione;
- una presentazione sulla protezione dei diritti fondamentali da parte dell'Agenzia, seguita da eventuale discussione.

È poi previsto un aggiornamento sulle attività di Europol relative alla guerra in Ucraina.

Nella fase pomeridiana si svolgeranno invece due sessioni di “controllo” su aspetti specifici dell'attività dell'Agenzia in alcuni settori:

- la prima avrà ad oggetto la necessità di prevenire le minacce alla sicurezza come l'attacco di Solingen affrontando la migrazione illegale (sessione I);
- la seconda riguarderà la cooperazione di polizia nella lotta alla criminalità informatica, in particolare ai crimini che utilizzano l'intelligenza artificiale, esaminando anche le possibilità di condivisione delle conoscenze con la CEPOL – l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (sessione II).

Nel presente dossier, dopo un capitolo introduttivo che illustra mandato e composizione del Gruppo parlamentare di controllo saranno trattati i singoli temi oggetto delle due fasi della riunione.

**15th meeting of the Joint Parliamentary Scrutiny Group on Europol
(JPSG)**

DRAFT AGENDA

12 November 2024, 08:15 - 13:00 and 14:15 - 18:00

**Room: *tbc*
European Parliament, Brussels**

Tuesday, 12 November 2024, 08:15 - 13:00 (morning session)

08:15 - 08:45 **Troika meeting BE-HU-PL_EP delegations, meeting held in camera**
(see separate agenda)

08:45 - 09:00 **Adoption of the agenda and opening remarks**

- Mr. Javier ZARZALEJOS, Co-Chair of the JPSG and Chair of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament;
- Mr. Lajos KÓSA, Co-Chair of the JPSG and Chair of the Committee on Defence and Law Enforcement, Hungarian National Assembly;
- Mr. Imre VEJKEY, Co-Chair of the JPSG and Chair of the Committee on Justice, Hungarian National Assembly;
- Feedback following Troika meeting;
- Report by the JPSG Representatives to the Europol Management Board meeting.

09:00 - 09:05 **Appointment of the members of the Consultative Forum on Fundamental Rights**

09:05 - 09:30 **Keynote speeches to the JPSG**

- Ms. Ylva JOHANSSON, European Commissioner for Home Affairs (*tbc*);
- Mr. Sándor PINTÉR, Minister of Interior of Hungary (*tbc*).

09:30 - 11:15 **Europol activities March 2024 – November 2024; presentation of the Europol Draft Multiannual Programming Document 2025-2027 and reply to written contributions by delegations**

- Presentation by Ms. Catherine DE BOLLE, Europol Executive Director;
- Presentation by Mr. Peter DE BUYSSCHER, Chair of the Europol Management Board;
- Followed by an exchange of views.

11:15 - 11:45 ***Break***

11:45 - 12:30 **Data Protection**

- Presentation by Mr. Wojciech WIEWIÓROWSKI, European Data Protection Supervisor;
- Presentation by Mr. Daniel DREWER, Europol Data Protection Officer;
- Reply from Europol (*representative tbc*);
- Followed by an exchange of views.

12:30 - 13:00 **Fundamental Rights Protection**

- Presentation by Mr. Dirk ALLAERTS, Europol Fundamental Rights Officer;
- Followed by an exchange of views.

Family photo

13:00 - 14:15 ***Lunch reception (ASP 00 G Le Grand Café Spinelli, Altiero Spinelli Building)***

Tuesday, 12 November 2024, 14:15 - 18:00 (afternoon session)

14:15 - 14:45 **Update on Europol Activities linked to the war in Ukraine**

- Presentation by Europol (*representative tbc*);
- Followed by an exchange of views.

14:45-16:15 **Scrutiny Session I: Need to prevent security threats like the Solingen attack through addressing illegal migration**

- Presentation by Europol (*representative tbc*);
- Presentation by the European Commission (*representative tbc*);
- Mr. Sándor PINTÉR, Minister of Interior (*tbc*).

Video presentation by the Ministry of Interior of Hungary

- Followed by an exchange of views.

16:15: - 17:45 **Scrutiny Session II: The fight against cybercrime, in particular crimes using Artificial Intelligence; possibilities of knowledge sharing involving CEPOL**

- Mr. Sándor PINTÉR, Minister of Interior of Hungary (*tbc*);
- Presentation by Europol (*representative tbc*);
- Ms. Montserrat MARÍN LÓPEZ, Executive Director of CEPOL and Head of CEPOL EU Training Centre Unit (*tbc*);
- Followed by an exchange of views.

17:45 - 18:00 **Closing remarks**

Next meeting of the JPSG on Europol under the Polish presidency: 23-24 February 2025, Warsaw.

INDICE

L'ORDINE DEL GIORNO E L'ARTICOLAZIONE DELLA RIUNIONE

IL GRUPPO DI CONTROLLO PARLAMENTARE CONGIUNTO SULLE ATTIVITÀ DI EUROPOL 1

- Il Gruppo di controllo parlamentare congiunto (JPSG) sulle attività di Europol 1
- L'Agenzia Europol 3

IL RISPETTO DEI DIRITTI FONDAMENTALI NELL'AMBITO DELLE ATTIVITÀ DI EUROPOL - IL FORUM CONSULTIVO..... 7

- Principi 7
- Il responsabile per i diritti fondamentali 7
- Il Forum consultivo sui diritti fondamentali 8

LA PROTEZIONE DEI DATI PERSONALI NELL'AMBITO DELLE ATTIVITÀ DI EUROPOL 11

- Quadro normativo..... 11
- Relazioni con istituzioni, organi e organismi dell'Unione europea..... 12
- Rapporti con Paesi terzi e organizzazioni internazionali 12
- Scambio di dati personali con parti private 13
- Controllo sull'applicazione delle norme per la protezione dei dati 13

IL PROGETTO DI PROGRAMMAZIONE PLURIENNALE 2025-2027 DI EUROPOL..... 17

- Attuazione e preparazione di EMPACT 17
- Analisi del crimine e scambio di informazioni 18
- Nuovi adempimenti per attuare il sistema ETIAS e il quadro Prum II.... 19
- Obiettivi di alto valore..... 19
- Contrasto al traffico di stupefacenti 20

Traffico di migranti	20
Cybercrime	20
Pedopornografia	20
Terrorismo	21
Reati finanziari ed economici.....	21
Laboratorio per l'innovazione	22
Rapporti internazionali	22
Strategia di diversità e inclusione.....	23
Risorse umane e finanziarie per gli anni 2025-2027.....	23

AGGIORNAMENTO SULLE ATTIVITÀ DI EUROPOL CONNESSE ALLA GUERRA IN UCRAINA.....25

SESSIONE DI CONTROLLO I – NECESSITÀ DI PREVENIRE MINACCE ALLA SICUREZZA COME L'ATTACCO DI SOLINGEN, AFFRONTANDO IL PROBLEMA DELL'IMMIGRAZIONE ILLEGALE29

L'attacco di Solingen e il dibattito seguito in Parlamento europeo	29
Il ruolo di Europol nella lotta al terrorismo.....	30
Politiche dell'UE in materia di gestione delle frontiere, immigrazione irregolare, e rimpatri.....	32

SESSIONE DI CONTROLLO II – LA LOTTA ALLA CRIMINALITÀ INFORMATICA, IN PARTICOLARE AI CRIMINI COMMESSI MEDIANTE L'INTELLIGENZA ARTIFICIALE; POSSIBILITÀ DI SCAMBIO DI CONOSCENZE CON IL COINVOLGIMENTO DI CEPOL41

Strumenti di diritto derivato dell'UE per il contrasto alla criminalità informatica.....	41
Il ruolo di Europol nella lotta alla criminalità informatica.....	43
L'uso dell'intelligenza artificiale per finalità criminali	44
Il coinvolgimento di CEPOL nel contrasto al cybercrime	45

IL GRUPPO DI CONTROLLO PARLAMENTARE CONGIUNTO SULLE ATTIVITÀ DI EUROPOL

Il Gruppo di controllo parlamentare congiunto (JPSG) sulle attività di Europol

Istituzione

Il **Gruppo congiunto di controllo parlamentare su Europol** (*Joint Parliamentary Scrutiny Group - JPSG*), che ha avviato i suoi lavori nel 2017, è stato istituito in coerenza con quanto disposto dall'[articolo 88, paragrafo 2](#), del Trattato sul funzionamento dell'Unione europea.

Tale disposizione demanda ai regolamenti che disciplinano la struttura, il funzionamento, la sfera d'azione e i compiti di Europol la definizione delle **modalità di controllo delle attività** della medesima agenzia **da parte del Parlamento europeo, controllo cui sono associati i parlamenti nazionali**.

È stato quindi introdotto con il [regolamento](#) (UE) 2016/794 un meccanismo di **controllo** parlamentare che include il **Gruppo congiunto**. Esso esercita, in particolare, un **monitoraggio politico** delle attività di Europol nell'adempimento della sua missione, anche con riguardo all'impatto di tali attività sui **diritti** e sulle **libertà fondamentali**.

Composizione

Ciascun **Parlamento nazionale** (limitatamente agli Stati membri che abbiano aderito al regolamento Europol) deve essere rappresentato da un numero di **membri fino a 4**. Nel caso di Parlamenti bicamerali, ciascuna Camera può nominare fino a **due membri**. Il **Parlamento europeo** deve essere rappresentato con un numero massimo di **16 membri**.

[Il regolamento interno](#) del Gruppo, all'articolo 2, stabilisce che i rappresentanti dei Parlamenti nazionali siano **nominati ove possibile per l'intera durata del mandato parlamentare**, alla luce dell'esigenza di assicurare la **continuità e la maturazione di una competenza specifica**.

Il Gruppo è **presieduto congiuntamente** dal Parlamento del Paese che detiene la **Presidenza di turno** del Consiglio dell'Unione europea e dal Parlamento europeo (di norma questa ultima Co-Presidenza è esercitata dal Presidente della Commissione per le libertà civili, la giustizia e gli affari interni - LIBE del Parlamento europeo).

Si riunisce di norma **due volte** l'anno, **alternativamente** nel Parlamento del Paese che detiene la Presidenza di turno del Consiglio dell'UE e nel Parlamento europeo (a determinate condizioni, sono possibili riunioni straordinarie).

Attività di monitoraggio

Il regolamento Europol prevede che ai fini delle attività **monitoraggio** del Gruppo:

a) il **Presidente** del consiglio di amministrazione dell'Agenzia, il **direttore esecutivo** o i loro supplenti **compaiono dinanzi al Gruppo**, su richiesta di quest'ultimo, per discutere questioni riguardanti le attività dell'Agenzia, compresi gli aspetti di **bilancio** di tali attività, l'**organizzazione strutturale** e l'eventuale istituzione di **nuove unità e centri specializzati**, tenendo conto degli obblighi di segreto e riservatezza. Il Gruppo può decidere di invitare alle sue riunioni altre persone interessate, ove del caso;

b) il **Garante europeo per la protezione dei dati personali compare dinanzi al Gruppo**, su richiesta di quest'ultimo, a cadenza **almeno** annuale per discutere le questioni generali relative alla **protezione dei diritti e delle libertà fondamentali delle persone fisiche**, in particolare la protezione dei dati personali, nelle attività di Europol, tenendo conto degli obblighi di segreto e riservatezza;

c) il Gruppo è **consultato** per quanto riguarda la **programmazione pluriennale** di Europol.

Inoltre Europol trasmette al Gruppo, a titolo informativo, tra l'altro, i seguenti documenti, tenendo conto degli obblighi di segreto e riservatezza:

- le **valutazioni** delle minacce, le **analisi strategiche** e i **rapporti** di situazione in relazione all'obiettivo di Europol, nonché i risultati degli studi e delle valutazioni commissionate da Europol;
- le **intese amministrative** concluse ai sensi del regolamento di Europol;
- il documento contenente la **programmazione pluriennale** e il **programma** di lavoro **annuale** di Europol;
- la relazione annuale di attività consolidata sulle attività di Europol;
- la relazione di valutazione redatta dalla Commissione.

Il Gruppo può redigere **conclusioni sintetiche** sul monitoraggio politico delle attività di Europol e presentarle al Parlamento europeo e ai Parlamenti

nazionali. Il Parlamento europeo le trasmette, a titolo informativo, al Consiglio, alla Commissione e alla stessa Agenzia.

Ai sensi dell'articolo 14, paragrafo 3 del regolamento di Europol, il Consiglio di amministrazione dell'Agenzia può invitare a **partecipare** alle sue riunioni, in veste di **osservatore senza diritto di voto**, ogni persona il cui parere possa essere rilevante per le discussioni, compreso, se del caso, un **rappresentante del gruppo di controllo parlamentare congiunto**. In attuazione di tale ultima previsione:

- **due rappresentanti** del Gruppo partecipano come **osservatori non votanti**, per il tempo stabilito dal Gruppo stesso, alle riunioni del Consiglio di amministrazione di Europol;
- **uno dei rappresentanti** deve essere delegato dal **Parlamento europeo** e l'altro dalla delegazione al JPSG del **Parlamento dello Stato che detiene la Presidenza di turno** del Consiglio dell'UE. **Soltanto uno** di essi prende la parola al Consiglio di amministrazione a nome del JPSG. Prima di ciascuna riunione cui sono invitati, i due rappresentanti si accordano pertanto su chi sia **designato** allo scopo. I rappresentanti riferiscono per iscritto al JPSG dopo ogni riunione del Consiglio di amministrazione sui loro principali risultati.

L'Agenzia Europol

Europol, l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto, è espressamente prevista dall'art. 88 del Trattato sul funzionamento dell'UE che le affida il compito di “**sostenere e potenziare** l'azione delle autorità di polizia e degli altri servizi incaricati dell'applicazione della legge degli Stati membri e la **reciproca collaborazione** nella prevenzione e lotta contro la **criminalità grave** che interessa due o più Stati membri, il terrorismo e le forme di criminalità che ledono un interesse comune oggetto di una politica dell'Unione”.

Il medesimo articolo, al paragrafo 2, demanda al Parlamento europeo e al Consiglio, deliberando mediante **regolamenti secondo la procedura legislativa ordinaria**, la definizione della struttura, il funzionamento, la sfera d'azione e dei compiti di Europol. In attuazione di tale disposizione è stato adottato il [regolamento n. 2016/794](#), successivamente modificato con il [regolamento \(UE\) 2022/991](#).

Europol era entrata in funzione nel 1998 sulla base di una apposita Convenzione del 1995, poi sostituita dalla decisione 2009/371/GAI del Consiglio, più volte modificata e quindi abrogata e sostituita dal richiamato regolamento 2016/794.

Mandato

Il mandato di Europol, definito dal richiamato articolo [88, paragrafo, 1](#), del Trattato sul funzionamento dell'Ue ([TFUE](#)) e dal regolamento istitutivo, investe le seguenti tipologie di reato: **terrorismo**, **criminalità organizzata**, traffico di **stupefacenti**, attività di **riciclaggio** del denaro, criminalità nel settore delle materie nucleari e radioattive, organizzazione del **traffico di migranti**, **tratta di esseri umani**, criminalità connessa al traffico di **veicoli rubati**, **omicidio** volontario e lesioni personali gravi, **traffico illecito di organi** e tessuti umani, **rapimento**, **sequestro** e presa di ostaggi, **razzismo** e **xenofobia**, **rapina** e **furto** aggravato, traffico illecito di beni culturali, compresi gli oggetti d'antiquariato e le opere d'arte, **truffe** e **frodi**, **reati** contro gli **interessi finanziari dell'Unione**, abuso di informazioni privilegiate e **manipolazione del mercato finanziario**, *racket* ed estorsioni, contraffazione e pirateria in materia di prodotti, **falsificazione** di atti amministrativi e traffico di documenti falsi, **falsificazione di monete** e di altri mezzi di **pagamento**, criminalità informatica, corruzione, **traffico illecito di armi**, munizioni ed esplosivi, traffico illecito di **specie animali protette**, traffico illecito di specie e di essenze vegetali protette, criminalità ambientale, compreso l'inquinamento provocato dalle navi, traffico illecito di sostanze ormonali e altri fattori di crescita, **abuso** e **sfruttamento sessuale**, compresi materiale **pedopornografico** e adescamento di minori per scopi sessuali, genocidio, crimini contro l'umanità e crimini di guerra.

In relazione a queste fattispecie, l'Agenzia funge da:

- centro di **sostegno** per le operazioni di contrasto;
- centro di **informazioni** sulle attività criminali;
- centro di **competenze** in tema di **applicazione della legge**.

Oltre alla raccolta, conservazione, trattamento, analisi e scambio di informazioni, l'Agenzia può sostenere e rafforzare le azioni delle autorità competenti degli Stati membri svolgendo attività di **coordinamento**, **organizzazione** e svolgimento di **indagini** e **azioni** operative comuni.

Europol **non applica misure coercitive** nello svolgimento dei suoi compiti, trattandosi di **competenza esclusiva** delle pertinenti **autorità nazionali**.

La decisione in merito a quali siano i **reati** da considerare come **prioritari** compete all'[EMPACT](#), la **piattaforma** di cooperazione multidisciplinare strutturata finalizzata a contrastare la criminalità organizzata e le forme gravi di criminalità internazionale, coordinata dagli **Stati membri** e sostenuta da **istituzioni**, organismi e agenzie dell'UE, in linea con i loro rispettivi mandati.

In tale contesto Europol, contribuisce al funzionamento di EMPACT, tra l'altro predisponendo il documento [EU SOCTA](#) (European Union Serious and Organised Crime Threat Assessment (EU SOCTA)), che il Consiglio usa come base per l'individuazione dei **settori criminali ritenuti prioritari**.

Organizzazione

Con sede a L'Aja, la struttura di gestione di Europol consta del **direttore esecutivo** (rappresentante legale dell'Agenzia), di **vice direttori**, nominati dal Consiglio dell'Ue (nella composizione Giustizia e affari interni) e di un **consiglio di amministrazione**, composto da un **rappresentante di ciascuno Stato membro** e da un rappresentante della Commissione. Ciascun rappresentante ha diritto di voto. Il consiglio di amministrazione può servirsi di organi consultivi.

Dal maggio 2018 **Catherine De Bolle** è la direttrice esecutiva di Europol. È assistita da tre vicedirettori esecutivi:

- **Jean-Philippe Lecouffe**, dipartimento Operativo;
- **Jürgen Ebner**, dipartimento *Governance*;
- **Andrei Linta**, dipartimento Capacità.

Europol **riferisce** al Consiglio dell'UE Giustizia e affari interni, che è competente per il **controllo in via principale** degli **orientamenti** dell'Agenzia, oltre che, come già detto, per la nomina del **direttore esecutivo** e dei **vice direttori**. Il Consiglio inoltre approva il bilancio dell'Agenzia (parte del bilancio generale dell'Ue) congiuntamente al Parlamento europeo. Ogni anno inoltre il Consiglio trasmette una relazione speciale al Parlamento europeo sull'attività di Europol.

L'Agenzia si è progressivamente dotata di centri **specializzati in** vari settori criminali facenti capo alla **direzione operativa**:

- il Centro operativo e di analisi;
- il Centro per la criminalità **grave ed organizzata**;
- il Centro per la criminalità **informatica**;
- il Centro per il contrasto al **terrorismo**;
- il Centro per i **reati economici e finanziari**.

Europol include infine un [Centro europeo contro il traffico di migranti](#) con il compito di supportare la polizia e le autorità di frontiera degli Stati membri nel coordinamento di operazioni transfrontaliere **anti-traffico**.

Bilancio

In base all'ultimo [bilancio rettificato](#) 2024 riportato sul suo sito, Europol ha disposto di un volume di entrate nel **2024** pari a circa **223 milioni di euro**, registrando un aumento costante di risorse rispetto ai circa **213 milioni** nel **2023** e **199 milioni** nel **2022**.

Per quanto riguarda le uscite, la parte più significativa è costituita dalle spese per l'impiego di **personale** le cui voci principali ammontano a circa **122 milioni di euro**. Le spese per le **attività operative** sono tra l'altro articolate in quelle per le **operazioni** in senso stretto (pari a circa **15 milioni di euro**) e quelle per la **tecnologia informatica operativa** che ammontano a quasi **46 milioni** di euro.

Le risorse umane impiegate da Europol nel 2024 consistono in:

- **754 agenti temporanei**, rispetto ai 716 del 2023;
- **255 agenti a contratto**, rispetto ai 235 del 2023;
- **376 esperti nazionali distaccati**, rispetto ai 356 del 2023.

Per le prospettive relative alle risorse finanziarie e umane nei prossimi anni si rinvia alla sezione del dossier sul **Programma pluriennale 2025-2027** dell'Agenzia.

IL RISPETTO DEI DIRITTI FONDAMENTALI NELL'AMBITO DELLE ATTIVITÀ DI EUROPOL - IL FORUM CONSULTIVO

Principi

In base al considerando 76 il [regolamento Europol](#) rispetta la [Carta dei diritti fondamentali dell'UE](#), segnatamente i diritti alla protezione dei **dati** di carattere **personale** e al rispetto della **vita privata**, tutelati dagli **articoli 8 e 7** della Carta. Tale principio trova ulteriore riscontro nel considerando 50 della medesima disciplina, ove si sottolinea che **strutture di controllo indipendenti**, trasparenti, responsabili ed efficaci sono essenziali per la tutela delle persone relativamente al trattamento dei dati personali.

Le modifiche al quadro giuridico di Europol entrate in vigore nel giugno 2022 hanno ulteriormente ribadito il principio, prima di tutto con il nuovo articolo 4, paragrafo 5 bis, ai sensi del quale **Europol** deve rispettare i **diritti** e le **libertà fondamentali** (nel loro complesso) sanciti nella Carta dei diritti fondamentali dell'Unione europea nello **svolgimento dei suoi compiti**.

Il responsabile per i diritti fondamentali

Il nuovo articolo 41 quater del regolamento Europol obbliga l'Agenzia a dotarsi di un *Fundamental Rights Officer* (FRO), **responsabile per i diritti fondamentali**.

Il FRO ha il compito di sostenere Europol per quanto riguarda il rispetto dei diritti fondamentali in tutte le attività relative al mandato dell'Agenzia, con particolare riferimento alle **attività operative**, tra l'altro fornendo **consulenza al direttore esecutivo**. L'organismo emette inoltre **pareri non vincolanti** sugli **accordi** di lavoro con **Paesi terzi** o con altri organismi esterni, producendo altresì valutazioni in materia di diritti fondamentali con particolare riguardo allo **sviluppo** e all'**uso di nuove tecnologie**, come ad esempio **l'intelligenza artificiale**. Infine il FRO offre **formazione** in materia di diritti fondamentali a tutto il personale operativo di Europol.

Tale ultima funzione è strettamente collegata all'obbligo previsto dal nuovo articolo 41 *quinquies*, in base al quale **tutto il personale Europol** coinvolto in compiti operativi che comportano il trattamento di dati personali **deve ricevere una formazione obbligatoria** in materia di **protezione dei diritti** e delle **libertà fondamentali**, anche in relazione al trattamento dei dati personali. Tale formazione è organizzata in cooperazione con l'Agenzia

dell'UE per i diritti fondamentali (FRA) e l'Agenzia dell'UE per la formazione delle autorità di contrasto (CEPOL).

Da ultimo, in linea con l'articolo 41 quater del regolamento Europol il FRO ha pubblicato la [prima relazione annuale](#) riferita al 2023 sulle sue attività, compreso il livello di rispetto dei diritti fondamentali da parte delle attività di Europol.

Il Forum consultivo sui diritti fondamentali

Ai sensi dell'articolo 52-bis del [regolamento](#) Europol, il **Gruppo di controllo parlamentare congiunto** deve istituire un **Forum consultivo** che lo assista, su richiesta, nelle questioni legate ai **diritti fondamentali** fornendogli una **consulenza indipendente** e ne stabilisce la **composizione** e i **metodi di lavoro** nonché le modalità di **trasmissione delle informazioni** al Forum stesso.

Per dare seguito alla disposizione, il **JPSG**, nel corso della riunione del 18 e 19 febbraio 2024 a Ghent, ha approvato per consenso un **adeguamento** del proprio **regolamento interno**, inserendo un [Addendum](#) relativo all'istituzione del Forum consultivo sui diritti fondamentali.

Nomina

Per la **nomina** dei membri del Forum consultivo il JPSG deve lanciare un **invito a manifestare interesse** rivolto ad agenzie e organismi nazionali e dell'Ue, organizzazioni internazionali e intergovernative, nonché al mondo accademico e civile.

L'invito e l'elenco dei richiedenti devono essere pubblicati sulle pagine del JPSG sul sito web [IPEX](#) (*InterParliamentary EU information eXchange*).

Il JPSG ha lanciato quindi, con scadenza al 2 settembre 2024, un **invito a manifestare interesse** per diventare membri del Forum dal **1° dicembre 2024** fino alla fine del mandato del Parlamento europeo nel **luglio 2029**. La nomina è rinnovabile una sola volta.

Hanno risposto all'invito i seguenti soggetti (le rispettive lettere motivazionali sono disponibili sulla [pagina del sito web IPEX](#) dedicata al JPSG):

- Foundation The London Story;
- Sign. Alen Tahiri;
- European Network Against Racism (ENAR);

- Sign. Luca Tosoni;
- Sign. Thorsten Wetzling;
- Sign. Arndt Sinn.

Nella sua 15^a riunione, il 12 novembre 2024 a Bruxelles, il JPSG deciderà quali organizzazioni o persone dovranno essere membri del Forum consultivo, sulla base della **proposta della Troika**.

La Troika Presidenziale del JPSG è composta dal capo delegazione del Parlamento europeo, del Parlamento dello Stato membro che detiene la presidenza di turno del Consiglio, del Parlamento della Presidenza precedente e del Parlamento della Presidenza successiva. Nel caso in cui l'adesione sia connessa a un'organizzazione, l'organizzazione interessata deve nominare un rappresentante che partecipa a suo nome all'FC entro un mese dalla conferma dell'adesione e deve di conseguenza informare il Segretariato del JPSG.

Nella procedura di nomina e nella valutazione di coloro che hanno manifestato interesse, la Troika presidenziale e il JPSG devono considerare alcuni **criteri di selezione**:

- **competenza;**
- **comprovata esperienza;**
- **rilevanza**, ovvero un coinvolgimento passato o in corso in progetti o azioni dell'UE relative ai diritti fondamentali;
- **ambito geografico**, ovvero il grado di presenza a livello nazionale, regionale, europeo o internazionale (anche in paesi terzi) e l'area geografica di interesse dell'organizzazione;
- **indipendenza;**
- **grado di riconoscimento** del lavoro da parte dei soggetti interessati;
- **attività di rete europea**, ovvero il coinvolgimento passato o in corso in progetti o azioni dell'Ue comprese le attività di formazione o accademiche nel campo dell'applicazione della legge;
- **capacità di lavorare con un'ampia gamma di organizzazioni di diversa natura;**
- **equilibrio** di genere tra i membri del Forum.

La scelta deve inoltre essere conforme ai criteri di composizione del Forum stabiliti nell'*addendum*. In particolare, i **componenti** del FC devono essere al **massimo 11**. Il JPSG inoltre potrà invitare a partecipare al Forum l'Agenzia dell'UE per i diritti fondamentali.

Principi generali e metodi di lavoro

L'*Addendum* relativo all'istituzione del Forum consultivo contiene, tra l'altro, anche indicazioni relative ai **metodi di lavoro** e ai **principi generali** che devono orientarne l'azione.

Nel fornire la propria consulenza al JPSG il Forum dovrà operare secondo i principi di **indipendenza, trasparenza, integrità, rispetto reciproco e consenso** ed entro 3 mesi dalla sua costituzione dovrà adottare i propri **metodi di lavoro**.

Si riunirà **a distanza**, sebbene possano essere organizzate anche riunioni in formato fisico o ibrido. I componenti del CF dovranno altresì eleggere, per un mandato di 5 anni rinnovabile una volta, un **presidente**, che potrà essere invitato alle riunioni del JPSG, e un **vicepresidente**.

Il JPSG potrà chiedere la consulenza del FC su **qualsiasi questione relativa ai diritti fondamentali**, nell'ambito del mandato stabilito dal regolamento Europol e delle competenze del JPSG, ma i copresidenti del JPSG dovranno assicurare che il FC non riceva un numero eccessivo di richieste di consulenza. I membri del JPSG potranno chiedere una consulenza **per iscritto**. Le richieste scritte saranno trasmesse al FC dopo che la loro **ammissibilità** sarà stata verificata dai copresidenti del JPSG e ritenuta conforme al regolamento Europol. Anche il **direttore esecutivo di Europol** potrà consultare l'FC sui diritti fondamentali inviando una richiesta scritta al presidente dello stesso.

L'FC, che potrà collaborare con il responsabile per i diritti fondamentali di Europol, deve approvare il **parere per consenso** e fornirlo **per iscritto**, entro **4 settimane** prima della successiva riunione del JPSG. Le risposte saranno pubblicate anche sul sito web di IPEX (saranno rese anonime per quanto riguarda i dati personali). I membri del FC presteranno servizio *pro bono*.

LA PROTEZIONE DEI DATI PERSONALI NELL'AMBITO DELLE ATTIVITÀ DI EUROPOL

Quadro normativo

Il [regolamento](#) Europol (ER) reca una specifica disciplina relativa ai **dati personali operativi** trattati al fine di raggiungere gli **obiettivi dell'Agazia**.

Per **dati personali operativi**, secondo il [regolamento](#) sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione (EUDPR), a cui l'ER rimanda, si intendono tutti i dati personali trattati da organi o organismi dell'Unione nell'esercizio di attività rientranti nella **cooperazione giudiziaria in materia penale** e nella **cooperazione di polizia** per conseguire gli obiettivi ed eseguire i compiti stabiliti negli atti giuridici che li istituiscono.

Nell'ER sono integrate pertanto anche le norme pertinenti stabilite nel [regolamento](#) EUDPR. Europol applica tale regolamento anche ai **dati personali amministrativi**.

Il quadro giuridico di Europol in materia di protezione dei dati si basa inoltre sui principi contenuti nella [Convenzione 108](#) del Consiglio d'Europa sulla **protezione delle persone rispetto al trattamento automatizzato dei dati personali**, nonché sulla raccomandazione del Comitato dei Ministri del Consiglio d'Europa n. R (87) 15 che disciplina l'**uso dei dati personali nel settore della polizia**.

Per il trattamento dei **dati personali sensibili** che, per loro natura, possono esporre gli interessati a un rischio, è necessario garantire una maggiore protezione, pertanto esso è consentito solo con **garanzie specifiche**.

Appartengono a tale categoria e devono essere trattati secondo il principio di **proporzionalità** e **necessità** i dati che riconducono a: l'**origine razziale** o **etnica**; le **opinioni politiche**, le **convinzioni religiose** o di altro genere; l'**appartenenza sindacale**; **dati genetici**; **dati biometrici** al fine di identificare in modo univoco una persona fisica; la **salute** o la **vita sessuale** o l'orientamento sessuale di una persona fisica.

L'ER prevede poi un'ulteriore protezione per **particolari categorie** di interessati, ovvero **vittime**, **testimoni** o altre persone che possono fornire informazioni su reati, o minori. In questi casi il trattamento dei dati personali è consentito solo se è **strettamente necessario** e **proporzionato** per prevenire o combattere il **crimine**.

Ove sia necessario allo svolgimento dei suoi compiti, Europol può instaurare e mantenere **relazioni di cooperazione** con gli organismi dell'Unione, conformemente ai loro obiettivi, le autorità di Paesi terzi, le organizzazioni internazionali e le parti private. Per lo scambio di dati personali con tali soggetti, con cui Europol può concludere anche **accordi di lavoro**, sono previste disposizioni specifiche.

Relazioni con istituzioni, organi e organismi dell'Unione europea

Gli scambi di dati personali con istituzioni, organi, missioni, uffici e agenzie istituiti dal TUE e dal TFUE o sulla base di questi ultimi (ad es. quelli di più diretto interesse per le attività di Europol come OLAF, Frontex, CEPOL, Eurojust, EPPO e Commissione europea) sono considerati conformi alla protezione dei dati nella misura in cui lo **scambio di informazioni** sia **necessario e proporzionato** per il legittimo svolgimento dei compiti.

Merita ricordare che Frontex, a seguito di due [pareri](#) emessi il 7 giugno 2022 dal **Garante europeo per la protezione dei dati personali**, ha interrotto di fatto la **condivisione sistematica e regolare di dati personali** con Europol in merito a persone sospette di aver commesso reati transfrontalieri.

Secondo **fonti informali**, a seguito dei citati rilievi GEPD, Frontex è attualmente **abilitata** trasmettere ad Europol dati personali **esclusivamente** sulla base di **richieste *ad hoc*** e motivate da parte dell'Agenzia. Per ripristinare un flusso più sistematico dei dati acquisiti nel corso di operazioni delle due agenzie sarebbero tuttora in corso negoziati per uno scambio di lettere tra il Direttore Esecutivo di Frontex e quello di Europol, che definisca allo scopo **nuove modalità rispettose** delle indicazioni del Garante.

Rapporti con Paesi terzi e organizzazioni internazionali

Europol collabora con **Paesi terzi e organizzazioni internazionali** al di fuori dell'UE sulla base di **accordi operativi, accordi strategici** e accordi di **lavoro**.

Per quanto riguarda i trasferimenti di dati personali al di fuori dell'UE, Europol può trasferire dati personali a un'autorità di un Paese terzo o a un'organizzazione internazionale solo nella misura in cui tale **trasferimento** sia **necessario per lo svolgimento dei compiti di Europol**, sulla base di:

- una “**decisione di adeguatezza**” della **Commissione**, adottata ai sensi dell'art. 36 della [direttiva \(UE\) 2016/680](#), che constata che il Paese terzo o un territorio o un settore specifico all'interno di tale Paese terzo o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato;
- un **accordo internazionale** concluso tra l'Unione e il Paese terzo o l'organizzazione internazionale in questione, ai sensi dell'articolo 218 del TFUE, che preveda **adeguate garanzie** in materia di tutela della vita privata e dei diritti e delle libertà fondamentali delle persone;
- un **accordo di cooperazione** concluso, prima del 1° maggio 2017, tra Europol e il Paese terzo o l'organizzazione internazionale in questione, conformemente all'articolo 23 della decisione [2009/371/GAI](#).

Scambio di dati personali con parti private

L'ultima modifica del regolamento Europol ha rafforzato la capacità operativa di Europol per quanto riguarda la **cooperazione con parti private** e l'analisi e lo scambio di dati personali con parti private. L'ER a determinate condizioni consente a Europol, tra l'altro, di condividere i dati personali con determinate **parti private** per impedire la diffusione di contenuti *online* relativi al **terrorismo** o all'**estremismo violento** in situazioni di crisi o di materiale *online* relativo ad **abusi sessuali su minori**.

Controllo sull'applicazione delle norme per la protezione dei dati

L'applicazione delle norme sulla protezione dei dati da parte di Europol è supervisionata da diversi soggetti e controllata a vari livelli.

Il responsabile della protezione dei dati

Per garantire che il trattamento dei dati personali avvenga in modo conforme al quadro giuridico applicabile in materia, Europol si è dotato di un *Data Protection Function – DPF* guidata da un *Data Protection Officer (DPO)* **responsabile della protezione dei dati**, nominato dal **consiglio di amministrazione** di Europol.

Il DPF è un punto di contatto iniziale per tutte le questioni relative alla protezione dei dati e lavora a stretto contatto con il personale Europol,

offrendo consulenza e orientamenti in linea con le migliori pratiche in materia di trattamento dei dati personali.

Il DPO, tra l'altro, garantisce l'applicazione interna dei regolamenti relativi al trattamento dei dati personali, la tenuta di un registro del trasferimento, della trasmissione e della ricezione dei dati personali in conformità al regolamento Europol (ER), nonché di un registro delle violazioni dei dati personali.

Il **responsabile della protezione dei dati**, il cui ruolo ha natura consultiva, **garantisce** l'applicazione del quadro giuridico in materia di protezione dei dati, anche con riferimento al trattamento e allo scambio dei dati tra **Europol e gli Stati membri** dell'UE. In tale ambito il DPF ha accesso a tutti i dati trattati da Europol e a tutti i locali di Europol.

Nel contesto delle sue attività, il DPF ha istituito una **piattaforma di collaborazione online**: la rete di esperti in protezione dei dati di Europol (**EDEN**), con l'obiettivo principale di scambiare competenze e migliori pratiche tra le varie parti interessate, dagli esperti delle forze dell'ordine a rappresentanti di soggetti privati, del mondo accademico, e delle ONG.

Il Garante europeo per la protezione dei dati (GEPD)

Mentre il DPO è parte integrante di Europol, il [Garante europeo della protezione dei dati](#) (GEPD) ha il compito di supervisionare “esternamente” l'agenzia di polizia dell'UE.

Elementi generali

Istituito nel 2004, il **Garante europeo** della protezione dei dati (GEPD):

- **controlla** il **trattamento** dei dati personali da parte dell'amministrazione dell'UE allo scopo di assicurare il rispetto delle norme sulla *privacy*;
- è **consulente** per le Istituzioni e gli organi dell'UE su tutti gli aspetti del trattamento dei dati personali e delle relative **politiche e legislazione**; in particolare fornisce **consulenza** alle istituzioni, agli organi e agli organismi europei in merito alle **nuove proposte legislative** e alle iniziative connesse alla protezione dei dati personali;
- gestisce le **denunce** e conduce **indagini**;
- collabora con le **amministrazioni nazionali** dei Paesi dell'UE per assicurare la coerenza nell'ambito della protezione dei dati;
- controlla le **nuove tecnologie** che possono influire sulla protezione dei dati.

La carica di Garante ha una durata rinnovabile di **5 anni** ed esercitata attualmente da **Wojciech Wiewiórowski** (Polonia) nominato il 5 dicembre 2019 con [decisione](#) del PE e del Consiglio. Per svolgere le funzioni correnti il GEPD conta su due sezioni principali: controllo e rispetto delle norme; politica e consultazione.

Ove si ritenga che il proprio **diritto** alla *privacy* sia stato violato da un'Istituzione o da un organo dell'UE, è possibile rivolgersi in prima istanza al **personale dell'UE responsabile del trattamento** dei propri dati nel servizio in cui si ritiene sia stata commessa la violazione. Se i risultati non sono soddisfacenti, è possibile in secondo luogo contattare il **responsabile della protezione dati** dell'istituzione o dell'organo dell'UE che si ritiene abbia commesso la violazione. Se ciò non ha effetto, si può presentare un **reclamo al GEPD** il quale ha il compito di indagare e comunicare agli interessati se concorda con il reclamo presentato e, in caso affermativo, come si sta procedendo a correggere la situazione.

In particolare, quando le istituzioni, gli organi e gli organismi dell'UE non rispettano le norme sulla protezione dei dati, il GEPD può utilizzare i seguenti poteri di applicazione conferiti dal regolamento (UE) 2018/1725:

- rivolgere **avvertimenti** o ammonimenti all'istituzione dell'UE che tratta illecitamente o abusivamente i dati personali;
- ingiungere all'istituzione dell'UE di soddisfare le richieste dell'interessato di esercitare i propri diritti (ad esempio, **accedere** ai propri dati);
- imporre un **divieto provvisorio** o definitivo a una particolare operazione di **trattamento** dei dati;
- imporre una **sanzione amministrativa pecuniaria** alle istituzioni dell'UE;
- adire la Corte di giustizia dell'Unione europea.

Se si è in disaccordo con la decisione del GEPD è possibile deferire la questione alla **Corte di giustizia dell'UE**.

Il monitoraggio su Europol

L'articolo 51 del regolamento Europol prevede, tra l'altro, che **il GEPD compaia dinanzi al Gruppo di controllo parlamentare congiunto**, su richiesta di quest'ultimo, **a cadenza almeno annuale** per discutere le questioni generali relative alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare la protezione dei dati personali, nelle attività di Europol, tenendo conto degli obblighi di segreto e riservatezza.

In particolare, il GEPD ha il compito di **sorvegliare** e assicurare l'applicazione delle norme relative alla tutela dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al **trattamento di dati**

personali da parte di Europol, e di fornire alla medesima e agli interessati **pareri** su tutte le questioni relative al trattamento dei dati personali.

Più in dettaglio, il GEPD:

- tratta i **reclami** e compie i relativi accertamenti, e ne comunica l'esito agli interessati entro un termine ragionevole;
- svolge **indagini** di propria iniziativa o in seguito a un reclamo e ne comunica l'esito agli interessati entro un termine ragionevole;
- **sorveglia e garantisce l'applicazione** da parte di Europol di tutte le norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali;
- **consiglia Europol**, di propria iniziativa o su richiesta, in ordine a qualsiasi argomento relativo al trattamento di dati personali, in particolare **prima che adotti regolamentazioni interne** relative alla tutela dei diritti e delle libertà fondamentali riguardo al trattamento di dati personali;
- tiene un **registro dei nuovi tipi di trattamento** che gli vengono notificati;
- procede ad una **consultazione preventiva** sui trattamenti notificatigli.

Infine il GEPD ha il potere di:

- ottenere da Europol **l'accesso a tutti i dati personali** e a tutte le informazioni necessarie alle sue indagini; b) **accedere a tutti i locali** in cui Europol svolge le sue attività se si può ragionevolmente supporre che in essi sia svolta un'attività in applicazione del regolamento che disciplina tale Agenzia.

Nell'esercizio dei propri poteri, il 17 ottobre 2024, il GEPD ha espresso un [parere](#) di sorveglianza riguardante il progetto di decisione del consiglio di amministrazione di Europol in relazione all'attuazione dell'obbligo giuridico, previsto dall'articolo 27 bis, paragrafo 3, del regolamento Europol, di adottare norme per determinare i termini di conservazione dei dati personali amministrativi.

IL PROGETTO DI PROGRAMMAZIONE PLURIENNALE 2025-2027 DI EUROPOL

In base all'articolo 12 del proprio [regolamento istitutivo](#) e agli articoli 32 e 33 della rispettiva [disciplina finanziaria](#), il 31 gennaio 2024 Europol ha inviato al Parlamento europeo il **progetto di programmazione pluriennale 2025-2027** approvato dal consiglio di amministrazione dell'Agenzia.

Nella **prima sezione**, il documento offre una panoramica dei **fattori politici** attuali e previsti che dovrebbero influenzare il lavoro di Europol nei prossimi anni.

La **seconda sezione** riporta la **programmazione strategica 2025-2027** di Europol, compresa la pianificazione delle risorse, richiamando le **sei priorità** già individuate dal *board* dell'Agenzia con l'adozione nel giugno 2023 della strategia "Garantire la sicurezza in partenariato".

In particolare Europol nel triennio 2025-2027 dovrebbe mirare a:

1. fungere da **centro di informazioni** sui reati dell'UE, anche per quanto riguarda l'acquisizione dei **dati**;
2. fornire un **supporto operativo** agile in tempo reale;
3. funzionare quale **piattaforma** per le soluzioni di polizia europee;
4. riunire i partner interessati per la **cooperazione transfrontaliera** e l'**azione congiunta**;
5. porsi all'avanguardia nell'**innovazione** e nella **ricerca** in materia di forze dell'ordine;
6. rappresentare un **modello organizzativo** dell'UE per la cooperazione delle forze dell'ordine.

La **terza sezione** Europol fornisce una descrizione completa del **portafoglio** delle attività e degli obiettivi dell'Agenzia nel **2025**.

Di seguito una sintesi della **programmazione 2025** di Europol.

Attuazione e preparazione di EMPACT

La Piattaforma multidisciplinare europea contro le minacce criminali ([EMPACT](#)) 2022-2025 rimane il motore principale del supporto operativo fornito alle autorità competenti degli Stati membri nel 2025.

EMPACT è finalizzata a contrastare la criminalità organizzata e le forme gravi di criminalità internazionale. È coordinata dagli **Stati membri** e sostenuta da istituzioni, organismi e agenzie dell'UE, in linea con i loro rispettivi mandati.

Oltre a contribuire all'attuazione di tutti i piani d'azione, Europol svolge il coordinamento con riferimento a **quattro obiettivi strategici** orizzontali comuni (quadro di *intelligence*; **reti** criminali ad alto rischio; **commercio online** e *offline* di beni e servizi illeciti; **finanziamento** delle attività criminali, **riciclaggio** di denaro e recupero dei beni).

È previsto che nel 2025, l'Agenzia prepari la valutazione sulle minacce di criminalità grave e organizzata (Serious and Organised Crime Threat Assessment - [SOCTA](#)), fornendo la base della **decisione** del **Consiglio dell'UE** recante le prossime priorità EMPACT.

Analisi del crimine e scambio di informazioni

Al centro delle attività di Europol rimane il lavoro di **analisi** dei crimini, di cui si preannuncia il rafforzamento attraverso una maggiore attenzione alla produzione e al controllo della **qualità**, alla **standardizzazione** e ai programmi di **formazione**. Nel 2025 si prevede la maturazione del **sistema di gestione dei casi** e della **piattaforma di analisi congiunta** volta a una collaborazione più stretta ed efficace con gli Stati membri. L'Agenzia sta altresì pianificando lo sviluppo e il lancio di un nuovo programma di **formazione** e *coaching* in materia di analisi per soddisfare l'esigenza di competenze analitiche presso Europol e gli Stati membri.

La gestione delle informazioni, ivi comprese le **tecnologie** dell'informazione e della comunicazione (ICT), continueranno a consolidare le capacità di analisi di Europol.

Sono previsti miglioramenti nell'uso delle **reti di comunicazione** sicure come il [SIENA](#), nell'adempimento degli obblighi in materia di **scambio di informazioni**, e nella realizzazione del principio di **interoperabilità** (in collaborazione con [l'Agenzia eu-Lisa](#)). Il programma preannuncia nel 2025 i lavori per la realizzazione di un secondo centro di dati, per consentire ai sistemi di Europol di essere in linea con i requisiti di interoperabilità.

Nuovi adempimenti per attuare il sistema ETIAS e il quadro Prüm II

Con l'entrata in funzione nel 2026 del **Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)** seguito dai controlli sistematici tramite il Sistema informativo dei visti (VIS) il Centro operativo e di analisi di Europol dovrà garantire il rapido follow-up (24 ore su 24, 7 giorni su 7) sui riscontri di domande di **autorizzazione di viaggio** e di **visto** rispetto ai dati di Europol.

L'ETIAS è un **sistema informatico automatizzato** creato per il rilevamento dei **rischi** per la **sicurezza** o dei rischi legati alla **migrazione irregolare** posti dai visitatori **esenti dal visto** che viaggiano nello spazio Schengen garantendo al contempo i diritti fondamentali e la protezione dei dati.

Nel 2025, l'agenzia dovrebbe anche rafforzare le sue capacità di elaborazione dei **dati biometrici** in vista del suo **coinvolgimento** nel quadro rivisto di **Prüm II**.

Il [regolamento Prüm II](#) istituisce un quadro per la ricerca e lo **scambio di informazioni** tra le autorità competenti degli Stati membri (quadro Prüm II) stabilendo:

a) le condizioni e le procedure per la consultazione automatizzata di profili **DNA**, **dati dattiloscopici**, determinati dati di **immatricolazione dei veicoli**, immagini del **volto** ed estratti del **casellario giudiziale**; e

b) le norme relative allo scambio di **dati di base** a seguito di una corrispondenza confermata relativa a **dati biometrici**.

L'Agenzia sottolinea come l'adempimento di tutti questi compiti sia possibile nella misura in cui le risorse a disposizione lo consentiranno.

Obiettivi di alto valore

Europol continuerà a fornire supporto agli Stati membri nell'identificazione di **obiettivi di alto valore** (High Value Targets, HVT) che rappresentano il **rischio più elevato** di criminalità organizzata e grave, in particolare attraverso l'istituzione di task force operative (OTF). Nel 2025, il **Centro europeo per la criminalità organizzata** e grave (ESOCC) si concentrerà ulteriormente sull'implementazione del concetto HVT/OTF e sosterrà lo sviluppo e l'implementazione di strumenti, comprese le relative possibilità di finanziamento.

Contrasto al traffico di stupefacenti

Il contrasto al traffico degli stupefacenti prenderà particolarmente di mira gli **hub di scambio** e altre strutture principali come i **porti**. Il programma prevede altresì la valutazione di un rafforzamento della cooperazione con [l'Agencia dell'Unione europea in materia di droghe](#) (EUDA).

Traffico di migranti

Il [Centro europeo per il traffico di migranti](#) (*vedi infra*) rivedrà, insieme alle controparti interessate a livello nazionale e internazionale, le soluzioni per migliorare il **coordinamento operativo**, la raccolta **dati** e la loro **condivisione**, incluso il **monitoraggio** dei **social media**, con particolare riguardo alle rotte e alle reti del traffico di migranti; il Centro intensificherà gli **aspetti finanziari** del supporto fornito alle indagini, in stretta collaborazione il [Centro europeo per il crimine finanziario ed economico](#) (EFECC).

Cybercrime

Il [Centro europeo per il Cybercrime](#) (EC3) intende rafforzare l'attenzione sulla raccolta, l'elaborazione e la produzione di intelligence in materia di **minacce informatiche**, in particolare ottenendo ed elaborando set di dati come **comunicazioni legalmente intercettate** e **decifrate** nell'ambito di reti criminali, nonché server del **dark web** sequestrati, già utilizzati per traffici criminali e diffusione di **materiale pedopornografico**.

Per affrontare la domanda crescente dai Paesi membri, l'EC3 nel 2025 continuerà a supportare le indagini relative alle **criptovalute**, tramite l'aggiornamento del nuovo *CryptoPortal* e la *Digital Support Unit* nonché contribuendo all'implementazione del [piano d'azione UE Forensic Science Area 2.0](#), in particolare, nei settori della **biometria**, **dell'intelligenza artificiale** e delle **tecnologie emergenti**.

Pedopornografia

In vista del [nuovo regolamento UE](#) per la prevenzione e il contrasto degli **abusi sessuali** sui **minori**, Europol continuerà a realizzare gli adeguamenti tecnici e operativi per garantire una gestione efficace dell'**aumento** dei

contributi di dati e il supporto agli Stati membri. L'Agenzia avvierà il **Servizio europeo di segnalazione degli abusi sui minori** (EU-CARES) un nuovo sistema automatizzato volto a facilitare la **segnalazione**, la **ricezione** e l'**elaborazione** di materiale pedopornografico da parte di soggetti pertinenti non appartenenti alle forze dell'ordine, e il **controllo incrociato** automatico dei dati.

Terrorismo

Anche nell'area dell'antiterrorismo, continueranno gli sforzi per concentrarsi su individui ritenuti obiettivi di alto valore, e per smantellare le organizzazioni **terroristiche/estremiste** violente. In particolare il [Centro europeo anti terrorismo](#) (ECTC) fornirà supporto a un numero maggiore di **Task Force**, promuovendo lo scambio di informazioni tra i partner pertinenti a livello UE. Data la crescente tendenza del **terrorismo di destra** e dell'estremismo violento, il centro eseguirà azioni prioritarie volte a identificare obiettivi in casi di alto profilo e supportare gli Stati membri attraverso un nuovo progetto di analisi dedicato esclusivamente a quest'area criminale. Inoltre, nel 2025, l'**Unità di riferimento Internet dell'UE** (IRU) nell'ambito dell'ECTC rafforzerà l'attenzione sull'**estremismo violento di sinistra** e sull'**anarchismo violento**. Parallelamente, Europol dovrebbe garantire il funzionamento efficiente della piattaforma dell'UE per la segnalazioni e gli ordini di rimozione (PERCI) di **contenuti terroristici online**, e delle notifiche di imminente minaccia per la vita, in conformità ai requisiti del [regolamento sui contenuti terroristici online](#) (TCO) e della [legge sui servizi digitali](#). Inoltre, è previsto che l'IRU promuova la competenza in materia di indagini *open source*, di monitoraggio sui social media, e di soluzioni software per contrastare le *fake news* e i *troll*.

Reati finanziari ed economici

Il Programma preannuncia l'impegno del [Centro europeo per la criminalità finanziaria ed economica](#) (EFECC) per migliorare la reattività e le performance operative nei settori della **frode**, del **riciclaggio di denaro**, del **recupero** dei beni, della **corruzione** e della **contraffazione**, in particolare contro i gruppi e professionisti della criminalità organizzata che forniscono servizi di **riciclaggio di denaro** ad altri gruppi criminali. Il Centro mira altresì a rafforzare le proprie capacità di rapido feedback in materia di

rintracciamento e analisi dei **beni virtuali** tenendo conto dell'elevato numero di casi registrati dagli Stati membri.

Il Programma sottolinea l'importanza di un rapporto efficace con la nuova [Autorità antiriciclaggio dell'UE](#) (AMLA), che dovrebbe entrare in funzione nel 2025, e nell'ambito del Meccanismo di cooperazione e supporto con le UIF (**Unità di informazione finanziaria**). In tale contesto si sottolinea la necessità di un canale di **comunicazione** sicuro tra Europol e la nuova Agenzia e di una cooperazione strutturata ad esempio mediante **squadre congiunte di analisi**. L'EFEECC sfrutterà le nuove possibilità per migliorare la cooperazione con le UIF e per aumentare il numero dei Paesi che offrono il loro contributo a Europol in materia di intelligence finanziaria.

L'EFEECC continuerà a promuovere la collaborazione con le **autorità doganali**, la loro partecipazione all'EMPACT e ai progetti di analisi di Europol. Nel 2025, il centro dovrebbe beneficiare della connessione tra il **sistema informativo doganale** e le **banche dati di Europol**, consentendo controlli incrociati automatizzati. L'agenzia seguirà da vicino gli sviluppi relativi alla riforma europea in materia doganale, preparandosi ad assumere i nuovi compiti da essa derivanti. Parallelamente, Europol sosterrà operativamente e strategicamente l'attuazione del pacchetto anticorruzione della Commissione europea, contribuendo al lavoro della nuova Rete dell'UE contro la corruzione.

Laboratorio per l'innovazione

Particolare attenzione viene attribuita al **Laboratorio per l'Innovazione** di Europol ([Innovation Lab](#)), che guida il [Polo d'innovazione dell'UE per la sicurezza interna](#) insieme alle altre Agenzie europee nel settore della giustizia e degli affari interni. Nel 2025 il laboratorio dovrebbe predisporre un **ambiente informatico** dove sviluppare, formare e certificare insieme agli Stati membri modelli e strumenti per l'uso operativo di dati, fornendo anche la possibilità di ospitare **ricercatori** nel campo delle tecnologie emergenti, appartenenti o al di fuori delle autorità delle forze dell'ordine.

Rapporti internazionali

Nell'ambito delle relazioni estere, Europol avvierà l'attuazione della sua **nuova strategia esterna** e proseguirà la cooperazione con **Paesi terzi** e

organizzazioni internazionali ritenuti prioritari. Parallelamente, l'agenzia valuterà l'efficacia degli **accordi** già esistenti, eventualmente procedendo a una revisione strategica della cooperazione con i Paesi associati a Schengen. Inoltre, nel 2025, Europol si concentrerà sul miglioramento della raccolta dal **settore privato** di informazioni rilevanti per arricchire il quadro di intelligence criminale.

Strategia di diversità e inclusione

Nel 2025 l'Agenzia continuerà ad attuare la sua **strategia** in materia di **diversità e l'inclusione**, con l'obiettivo di una gestione efficiente ed efficace del bilancio e delle risorse, mentre la tabella di marcia strategica per gli alloggi progredirà ulteriormente per consentire la crescita dell'Agenzia. Nel 2025 è prevista la restituzione dell'edificio satellite temporaneo 1 allo Stato ospitante, mentre diventerà operativo l'edificio satellite temporaneo 2.

Risorse umane e finanziarie per gli anni 2025-2027

Il Programma include una sezione sulle risorse umane e finanziarie previste per il triennio dal 2025 al 2027, recante, tra l'altro, tabelle ricognitive dell'andamento degli **aumenti** in termini di **personale** e di **fondi** a disposizione dell'Agenzia. In particolare le tabelle sottostanti mettono in evidenza le **richieste aggiuntive** dell'Agenzia (vedi righe "**Additional Agency request**") in termini di fondi e personale rispetto agli aumenti **già previsti** a quadro vigente (i valori in neretto costituiscono la somma delle due categorie di dati).

<p>Il Programma sottolinea in più parti che l'adempimento alle funzioni aggiuntive di Europol derivanti dalle nuove normative in materia di sicurezza e scambio di informazioni sarà possibile nella misura consentita dal volume di risorse messe a disposizione dell'Agenzia.</p>

Human Resources (TA, CA, SNE) ³⁷	Yearly increase		
	2025	2026	2027
Establishment plan (TA) - TOTAL	77	77	48
<i>Amended Europol Regulation</i>	19	9	5
<i>Prüm II Regulation</i>	-	(2)	-
<i>Proposal on a Regulation to prevent and fight migrant smuggling</i>	3	4	3
<i>Additional Agency Request</i>	55	66	40
Contract Agents - TOTAL	25	9	6
<i>Proposal on a Regulation to prevent and fight migrant smuggling</i>	5	9	6
<i>Additional Agency Request</i>	20	-	-
SNE - TOTAL	13	8	5
<i>Proposal on a Regulation to prevent and fight migrant smuggling</i>	11	6	3
<i>Additional Agency Request</i>	2	2	2

Financial Resources (€)	Yearly increase		
	2025	2026	2027
TOTAL	45,713,377	54,309,064	61,415,221
<i>Proposal on a Regulation to prevent and fight migrant smuggling</i>	15,758,000	19,679,000	13,456,000
<i>Additional Agency Request³⁸</i>	29,955,377	34,630,064	47,959,221

AGGIORNAMENTO SULLE ATTIVITÀ DI EUROPOL CONNESSE ALLA GUERRA IN UCRAINA

In base alle informazioni riportate sulla pagina dedicata del suo [sito](#), Europol sostiene l'UE e gli Stati membri rispetto a una serie di **minacce criminali** che traggono origine dalla **crisi in Ucraina** a causa dell'invasione russa, tra l'altro con particolare riguardo alla **tragedia umanitaria** che ha spinto un gran numero di profughi a fuggire dal Paese.

In particolare, l'Agenzia è in stretto contatto con gli **Stati membri confinanti** con l'Ucraina (ossia Lituania, Polonia, Slovacchia, Ungheria, Romania, Moldavia), impiegando in tali Paesi **esperti e funzionari di sostegno** alle autorità di polizia locali e **squadre operative**, come mostra la mappa sottostante (*Fonte: Europol*).



In particolare, con riferimento alla **raccolta e comunicazione di informazioni di intelligence**, Europol:

- collabora attivamente con le forze dell'ordine ucraine tramite l'**ufficiale di collegamento ucraino** presso la sede di Europol, supportando le specifiche richieste di tale ufficio di collegamento;
- raccoglie informazioni ed esegue il monitoraggio operativo degli **estremisti violenti che si recano in Ucraina**, con particolare riguardo alle reti di **comunicazione**, al **finanziamento** o al **reclutamento**;
- risponde alle richieste operative (anche da parte di **Ucraina e Moldavia**) per rimuovere specifici **canali di Telegram** utilizzati per la **disinformazione filo-russa** e per la diffusione di **notizie false** (in particolare tramite le unità EC3 e EU Internet Referral Unit);
- ha sostenuto l'attivazione del **protocollo di risposta** alle emergenze delle forze dell'ordine per i principali **attacchi informatici transfrontalieri**;
- garantisce un monitoraggio rafforzato delle **minacce informatiche** attraverso contatti permanenti con gli Stati membri, la Cybercrime Action Taskforce (J-CAT) e il monitoraggio *open source*.

Per quanto riguarda il sostegno alle **indagini sui crimini di guerra**, l'Agenzia ha avviato un progetto di analisi *core international crimes* e ha istituito una *task force* operativa di esperti per assistere le indagini condotte dall'Ucraina, da altri Paesi e dalla **Corte penale internazionale**, sui crimini di guerra commessi in Ucraina.

In tale contesto, merita ricordare che il 25 aprile 2023, il giudice **Piotr Hofmański, Presidente della Corte penale internazionale (CPI)**, e **Catherine De Bolle, direttore esecutivo di Europol**, hanno firmato un accordo di lavoro, recante un quadro giuridico per rafforzare la cooperazione, lo scambio di informazioni, conoscenze, esperienze e competenze. Inoltre, secondo il [comunicato stampa](#) della stessa Agenzia, Europol è entrata a far parte della **squadra investigativa comune** (“**joint investigation team**” o “**JIT**”) sui presunti **crimini internazionali di base** commessi in Ucraina: i procuratori generali dei Paesi partner e la stessa De Bolle hanno firmato il relativo accordo il 5 ottobre 2023, durante la **17a riunione del Forum consultivo dei procuratori generali** presso Eurojust.

Si ricorda che il JIT è stato istituito il 25 marzo 2022 da Lituania, Polonia e Ucraina con il sostegno di Eurojust. Il 31 maggio 2022, Estonia, Lettonia e Slovacchia sono diventate membri, seguite dalla Romania il 13 ottobre 2022. Il 3

marzo 2023, le sette autorità nazionali della squadra hanno firmato un **memorandum d'intesa** con il Dipartimento di Giustizia degli Stati Uniti. Eurojust, l'Ufficio del Procuratore della Corte penale internazionale (CPI) e ora Europol partecipano alla squadra.

In linea con il suo mandato, **Europol** fornirà **supporto analitico e forense** ai membri della squadra e sosterrà la **raccolta** e l'**analisi di dati** ottenuti legalmente da *social media*, le trasmissioni televisive e radiofoniche (la c.d. "Open Source Intelligence" o "OSINT").

Europol metterà anche a disposizione le proprie competenze ed esperienze nel campo dei crimini di guerra, dei crimini contro l'umanità e di altri crimini internazionali attraverso il [Progetto analitico](#) sui **crimini internazionali fondamentali**. Eurojust fornisce invece supporto legale, logistico, finanziario e analitico alla squadra. Dal marzo 2022, l'Agenzia ha ospitato 19 riunioni di coordinamento della squadra e di altre autorità nazionali che stanno indagando su presunti crimini internazionali fondamentali commessi in Ucraina.

Nel settore della **lotta alla tratta di esseri umani**, Europol ha istituito un **posto di comando virtuale** dedicato a tale crimine per facilitare lo scambio operativo in tempo reale tra **Ucraina, Romania, Austria, Ungheria, Germania, Repubblica slovacca, Moldavia e Polonia**, nonché un **gruppo temporaneo** di gestione delle attività sulla tratta degli esseri umani per discutere di questioni operative e rafforzare la cooperazione con le ONG del settore affidabili.

Riguardo le attività criminali favorite dallo scenario di guerra, oltre alla stretta collaborazione con l'Ucraina per ridurre il rischio di **traffico di armi** durante (e dopo) la guerra, l'Agenzia ha lanciato, tra l'altro, l'operazione OSCAR volta a effettuare un controllo incrociato degli **elenchi** delle **sanzioni** dell'UE con i dati operativi disponibili, a identificare i collegamenti con la criminalità organizzata e il **riciclaggio di denaro**, e a sostenere il rintracciamento e il sequestro dei **beni criminali**.

In questo ultimo ambito, Europol collabora altresì con la *task force* istituita dalla Commissione europea "*Freeze and Seize*", che mira a garantire il **congelamento** e la **confisca** effettivi dei beni di individui e di enti sottoposti a sanzione. Inoltre, sostiene anche il [Piano](#) comune anti-tratta per l'Ucraina, la [Piattaforma di solidarietà](#) e le riunioni del [Piano](#) di preparazione alla migrazione e alle crisi dell'UE.

**SESSIONE DI CONTROLLO I – NECESSITÀ DI PREVENIRE MINACCE
ALLA SICUREZZA COME L'ATTACCO DI SOLINGEN, AFFRONTANDO IL
PROBLEMA DELL'IMMIGRAZIONE ILLEGALE**

L'attacco di Solingen e il dibattito seguito in Parlamento europeo

Il **24 agosto 2024** un uomo di origine siriana ha aggredito i partecipanti del Festival della diversità a Solingen, in Germania, provocando **tre morti** e **otto feriti** per poi essere arrestato il giorno seguente, dopo che il cosiddetto gruppo dello Stato Islamico ha rivendicato la responsabilità dell'attacco, secondo quanto riportato, “per vendicare i musulmani in Palestina e ovunque”.

Dopo l'attacco di Solingen, la Germania ha deciso di reintrodurre i [controlli di frontiera](#) alle frontiere con **Francia, Belgio, Paesi Bassi, Lussemburgo e Danimarca**, a partire dal 16 settembre 2024 fino al 15 marzo 2025, per i rischi per la sicurezza legati alla migrazione irregolare. Lo stesso Stato membro ha reintrodotta a vario titolo controlli con altri Paesi, quali, tra l'altro, la Polonia, la Svizzera e la Repubblica Ceca.

Il 16 settembre scorso il Parlamento europeo ha svolto la [discussione](#) sulla “Necessità di prevenire le minacce per la sicurezza come l'attentato di Solingen con la lotta alla migrazione illegale e con rimpatri efficaci”, alla quale ha partecipato anche la Commissaria agli affari interni Johansson (in fase di scadenza del mandato), il cui portafoglio include la **sicurezza interna** dell'UE, compresa la promozione di misure per **prevenire e rispondere al terrorismo** e perseguire i responsabili, anche con una rigorosa attuazione della legislazione.

Nel corso della discussione sono state affrontate, tra l'altro, le questioni concernenti:

- **i movimenti non autorizzati** di cittadini di Paesi terzi all'interno dell'UE, e le decisioni adottate da Stati UE di **ripristinare i controlli** di frontiera alle frontiere interne (in particolare da parte della Germania), per migliorare l'individuazione degli ingressi illegali;
- la politica UE di **prevenzione e contrasto al terrorismo**, comprese le misure per combattere la **propaganda online** di contenuti **terroristici** e la **radicalizzazione**;

- l'attuazione del **Nuovo patto sulla migrazione e asilo** e le misure per una efficace politica di **rimpatrio**.

In particolare, la Commissaria Johansson ha sottolineato:

- l'importanza del nuovo [regolamento Eurodac](#) ai fini del miglior **tracciamento** dei richiedenti asilo che si spostano tra gli Stati membri, segnalando le minacce alla sicurezza;
- la necessità di **proteggere meglio i confini esterni dell'UE** e **controllare meglio gli ingressi**, anche attraverso il nuovo Patto sulla migrazione e asilo;
- la necessità di **contrastare la radicalizzazione**, anche **online**, ricordando, a tal proposito, il lancio dell'[hub di conoscenza per contrastare la radicalizzazione nell'UE](#)".

Il ruolo di Europol nella lotta al terrorismo

Il terrorismo è tra i settori criminali prioritari per i quali Europol ha il compito di **sostenere gli Stati membri** nelle attività di **prevenzione** e contrasto.

Gli **sforzi di Europol** sono coordinati dal [Centro europeo antiterrorismo \(ECTC\)](#), ufficialmente operativo dal **1° gennaio 2016**, che mira nel **rafforzamento della cooperazione transfrontaliera** tra le autorità antiterrorismo competenti. L'ECTC funge da *hub* informativo per la condivisione di intelligence in materia di terrorismo con le autorità di contrasto degli Stati membri dell'UE e di altri Paesi

L'approccio dell'ECTC è basato su quattro pilastri:

- facilitazione dello **scambio di informazioni** e della cooperazione transfrontaliera;
- **supporto operativo** efficace, coordinamento e competenze per le indagini degli Stati membri dell'UE;
- attenuazione proattiva dell'uso dei **social media** a fini di **radicalizzazione** e sostegno all'analisi operativa nelle indagini *online*;
- capacità di supporto strategico centrale.

I servizi chiave forniti da ECTC comprendono, tra l'altro:

- supporto in loco - invio di **squadre operative**;
- supporto **analitico** operativo;
- individuazione del **finanziamento** del terrorismo;

- supporto alle **indagini online** degli Stati membri dell'UE;
- risposta alle crisi attraverso la squadra di collegamento congiunta antiterrorismo;
- dispiegamento di agenti ospiti negli **hotspot** per la migrazione;
- accesso alle tecnologie e alle competenze del centro europeo per la criminalità informatica.

Nell'ambito dell'ECTC si ricorda, infine, l'**Unità di riferimento Internet dell'UE** ("IRU"), che si occupa di **rilevare** e **analizzare** i **contenuti terroristici** e di **estremismo violento** disponibili pubblicamente su Internet e li segnala ai fornitori di servizi online perché li valutino volontariamente. La missione dell'Unità è non solo limitare l'accesso pubblico alla propaganda terroristica, ma anche **indagare sui contenuti terroristici** per facilitare l'attribuzione e il perseguimento degli autori. L'IRU dell'UE fornisce inoltre supporto al **Centro europeo per il traffico di migranti** di Europol, segnalando i contenuti relativi alla **pubblicità** di servizi di **viaggio illegali** e ai **documenti** di viaggio **contraffatti** offerti dalle reti criminali a migranti e rifugiati.

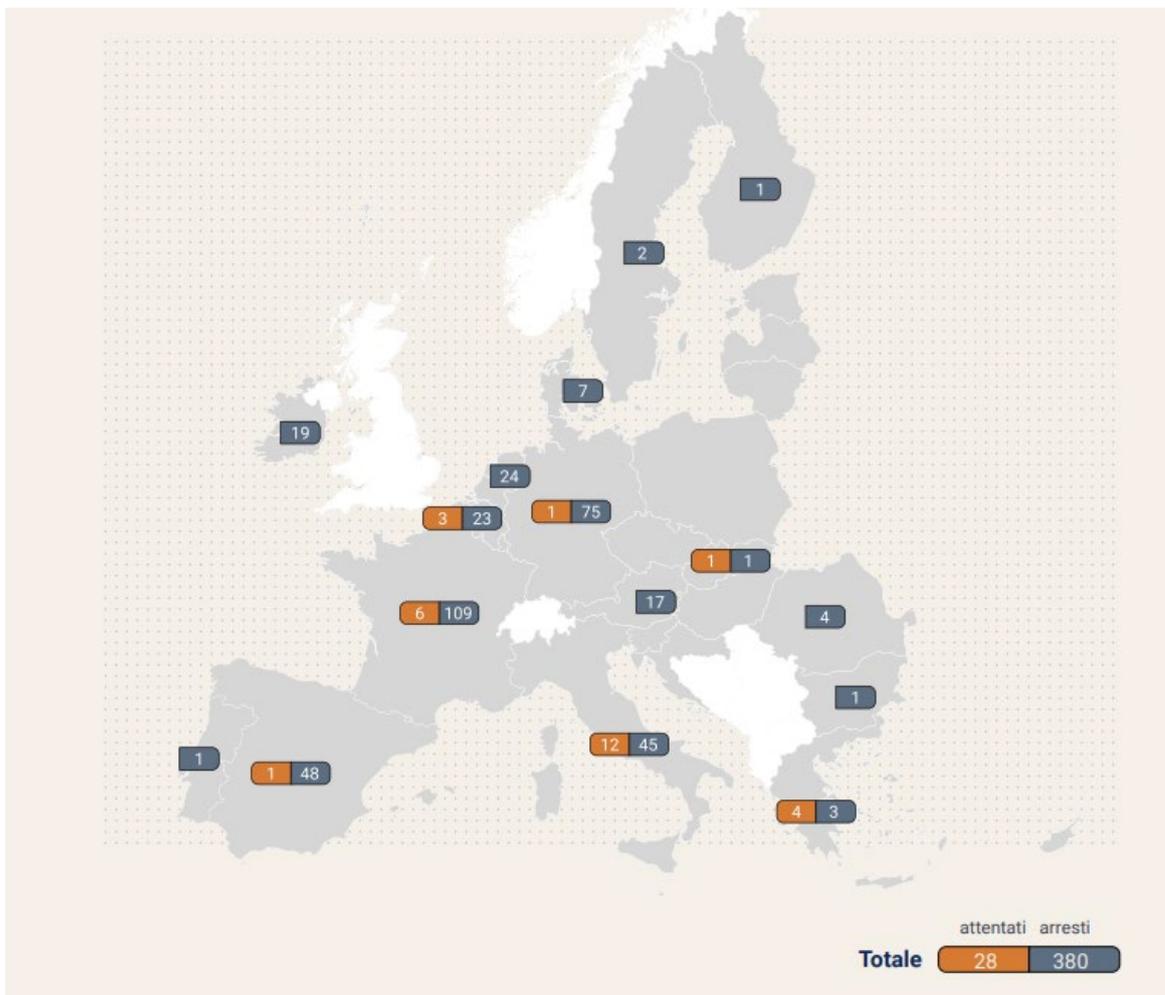
Il **Rapporto** sulla situazione e le tendenze del terrorismo nell'UE (EU Terrorism Situation and Trend Report TE-SAT), che Europol redige ogni anno dal 2007, fornisce una panoramica degli attacchi falliti, sventati e portati a termine nell'UE, nonché degli arresti, delle condanne e delle sanzioni legate al terrorismo. In particolare, il rapporto affronta:

- terrorismo **jihadista**;
- terrorismo **etno-nazionalista** e **separatista**;
- terrorismo di **sinistra** e **anarchico**;
- terrorismo di **destra**;
- terrorismo **monotematico**.

Dalla **sintesi** del rapporto 2023 si apprende, tra l'altro, che:

- si sono registrati nell'UE **28 attentati in totale** (tra quelli compiuti, falliti o sventati). In particolare, sono stati compiuti 16 attentati, per la maggior parte attribuiti al terrorismo anarchico e di sinistra (13), due al terrorismo jihadista e uno a quello di destra;
- sono state **arrestate** dalle autorità di contrasto degli Stati membri dell'UE per reati connessi al terrorismo **380 persone**;
- i procedimenti giudiziari hanno portato a **427** tra **condanne** e **assoluzioni** per reati di terrorismo.

La mappa sottostante offre una panoramica degli attentati terroristici (compiuti, falliti e sventati) e degli arresti per sospetto terrorismo nell'Ue nel 2022, per un totale di **28 attentati** (i riquadri in arancione) e **380 arresti** (i riquadri in grigio). (Fonte: Europol)



Politiche dell'UE in materia di gestione delle frontiere, immigrazione irregolare, e rimpatri

Contrasto dell'immigrazione irregolare - Rafforzamento del coordinamento di Europol

A partire dal 2010, il citato Ciclo politico dell'UE per la criminalità organizzata e le forme gravi di criminalità internazionale (EMPACT) ha individuato tra i settori criminali prioritari il reato di **facilitazione dell'immigrazione clandestina (FII)**.

In tale contesto la Commissione europea ha affrontato il fenomeno mettendo in campo un ampio spettro di misure che vanno dal **rafforzamento** del mandato di **FRONTEX** per aumentarne l'efficacia alle frontiere esterne anche tramite un **corpo permanente** di guardie di frontiera e costiera, all'istituzione di un meccanismo di valutazione per verificare la corretta applicazione delle norme di **Schengen**, e a una serie strumenti nell'ambito del Nuovo patto sulla migrazione e asilo, definitivamente approvato nel maggio 2024.

In attuazione del [Piano d'azione](#) rinnovato dell'UE contro il traffico di migranti (2021-2025), nel novembre 2023, la Commissione ha presentato un pacchetto di proposte normative, tuttora all'esame delle Istituzioni legislative europee, articolato in un:

- una [proposta](#) di regolamento sul **rafforzamento** della **cooperazione** di polizia in materia di prevenzione, accertamento e indagine del traffico di migranti e della tratta di esseri umani e sul rafforzamento del **sostegno di Europol** alla prevenzione e alla lotta contro tali crimini;
- una [proposta di direttiva](#) volta ad aggiornare le disposizioni vigenti di **diritto penale** dell'UE, intervenendo in maniera più specifica sulla configurazione del **reato di favoreggiamento dell'ingresso**, del **transito** e del **soggiorno** illegali nell'Unione.

In particolare, la proposta di regolamento, il cui iter in Parlamento europeo dovrebbe iniziare una volta terminata la fase di avvio del ciclo istituzionale, prevede, tra l'altro, l'**istituzione formale** nel quadro giuridico vigente e il rafforzamento del (già operante) [Centro europeo contro il traffico di migranti](#) nell'ambito di **Europol** e l'introduzione di un quadro di *governance* per regolamentarne e sostenerne le attività e il potenziamento della **cooperazione** e del **coordinamento** tra gli Stati membri, Europol e **altre agenzie** dell'Unione, nonché con i Paesi terzi.

Il ripristino dei controlli di frontiera alle frontiere interne dell'UE

Il [Codice frontiere Schengen](#), stabilisce norme riguardanti l'attraversamento delle frontiere esterne dell'UE e l'**assenza** di **controlli** alle **frontiere interne**, che in particolare governano:

- le **verifiche** sulle persone alle **frontiere esterne**;
- le condizioni d'ingresso;

- le condizioni per il **ripristino temporaneo** dei controlli alle **frontiere interne** nello spazio Schengen in caso di minaccia grave per l'ordine pubblico o la sicurezza interna.

Nel maggio 2024 sono state adottate [modifiche](#) alla normativa, i cui elementi chiave sono:

- l'istituzione di una **procedura** di trasferimento idonea ad affrontare i **movimenti secondari** di migranti (da uno Stato membro all'altro);
- soluzioni per contrastare il fenomeno della **strumentalizzazione** della **migrazione**;
- chiarimenti in merito alle norme relative al **ripristino** dei **controlli** di frontiera (alle frontiere interne).

In particolare, il nuovo regolamento introduce una nuova procedura di trasferimento volta a consentire agli Stati membri di trasferire i **cittadini di paesi terzi fermati** nella zona di **frontiera** (interna) il cui soggiorno nel loro territorio è **irregolare** verso lo Stato membro da cui sono arrivati direttamente. Il fermo dovrebbe avvenire nel contesto di un quadro di **cooperazione bilaterale**.

Inoltre, è chiarito il quadro vigente per il **ripristino** e la **proroga** dei controlli alle frontiere interne, che è possibile in caso di **minaccia grave** per l'**ordine pubblico** o la **sicurezza interna**. Gli Stati membri devono valutare la **necessità** e la **proporzionalità** di tale decisione e stabilire se gli obiettivi perseguiti non possano essere conseguiti con **altri mezzi**.

Viene altresì stabilita la **durata massima** durante la quale tali controlli alle frontiere interne possono essere **mantenuti**. I controlli alle frontiere interne, notificati alla Commissione, agli Stati membri e al Parlamento europeo prima di essere ripristinati, possono essere mantenuti per una **durata massima di due anni**. In gravi **circostanze eccezionali**, i controlli alle frontiere interne possono essere **prorogati** per **altri sei mesi**, proroga rinnovabile **una volta** per una durata complessiva di un **anno**.

In base al regolamento la possibilità di ricorrere a **misure alternative**, consistenti di norma in controlli di polizia e cooperazione transfrontaliera, dovrebbe **incoraggiare** gli Stati membri a **limitare** sostanzialmente il ripristino dei controlli temporanei alle frontiere; si precisa che tali misure devono essere **chiaramente distinte** dalle verifiche sistematiche sulle persone alle frontiere esterne.

Si ricorda che [misure di ripristino di controlli di frontiera](#) alle frontiere per ragioni (a seconda dei casi) di **sicurezza interna**, rischi associati alle

migrazioni secondarie, o minacce di **terrorismo**, da parte di Stati aderenti allo Spazio Schengen, sono tuttora adottate da: Norvegia, Austria, Germania, Danimarca, Francia, Svezia, **Italia**.

Prospettive di intervento negli orientamenti politici per la Commissione europea 2024-2029 e nelle lettere di conferimento del mandato ai Commissari designati

Il 18 luglio 2024, la Presidente della Commissione europea, Ursula von der Leyen, ha illustrato innanzi alla plenaria del Parlamento europeo gli orientamenti politici per il mandato della prossima Commissione europea nel periodo 2024-29, i quali, con riferimento al tema della gestione delle frontiere europee, prevedono, tra l'altro: il **rafforzamento** del ruolo di **Frontex**, portando il numero del citato corpo a **30.000 unità**; lo sviluppo di una **Strategia dell'UE** in materia di **visti**; il ripristino del **pieno funzionamento** dell'area **Schengen** mediante l'eliminazione dei rimanenti controlli alle frontiere interne e la piena estensione a Bulgaria e Romania.

Politica di rimpatrio dei migranti irregolari

La [direttiva rimpatri](#) disciplina le procedure e i criteri che gli Stati membri devono applicare per il rimpatrio di cittadini di paesi terzi in posizione irregolare.

A seguito dell'invito Consiglio europeo, nel settembre 2018 la Commissione ha [proposto](#) una **rifusione mirata** della direttiva con l'obiettivo di "ridurre la **durata** delle **procedure** di rimpatrio, garantire un migliore **collegamento** tra le **procedure** di asilo e di **rimpatrio** e assicurare un uso più efficace delle misure di **prevenzione della fuga**. L'esame della proposta è tuttora in fase di **stallo**, come sottolineato dal Parlamento europeo nel recente [dibattito](#) su possibili **nuove regole** per i rimpatri svoltosi durante la sessione plenaria dello scorso ottobre.

In base ai [dati](#) in possesso del Parlamento europeo il **tasso di rimpatrio** dei migranti irregolari dal 2016 al 2021 ha registrato un continuo **declino**, passando nel corso degli anni dal **46 al 25 per cento**. Il [2022](#), ha confermato questo trend considerato che su **422.400** decisioni di rimpatrio emesse dai paesi dell'UE solo **meno di un quarto** dei cittadini di paesi terzi sono stati rimpatriati in un paese al di fuori dell'UE.

Di seguito un grafico sul volume (in migliaia) di **rimpatri effettivi** (in arancione) dall'UE rispetto agli **ordini di rimpatrio** (in giallo) emessi dagli Stati membri (Fonte: Parlamento europeo)



Recenti misure nell'ambito del Nuovo patto sulla migrazione e l'asilo

Il miglioramento della politica di rimpatrio è uno degli obiettivi cui sono riconducibili una serie di misure adottate nell'ambito del **Nuovo patto sulla migrazione e l'asilo**, il cui corpus normativo principale è stato approvato alla fine della scorsa legislatura europea.

Le nuove regole, entrate in vigore l'11 giugno 2024, sono articolate in quattro pilastri: **sicurezza delle frontiere esterne**; **procedure** rapide ed efficaci; sistema efficace di **solidarietà**; migrazioni nel contesto delle **relazioni internazionali**.

Con riferimento al primo ambito di intervento, viene in considerazione, in primo luogo, il nuovo [regolamento sullo screening](#), volto a rafforzare i **controlli** sulle persone alle frontiere esterne, nella prospettiva di una rapida individuazione della **procedura da applicare** alla persona che entra nell'UE in violazione delle norme di ingresso.

Gli accertamenti includono l'**identificazione**, i **controlli sanitari** e di **sicurezza**, il rilevamento delle **impronte digitali** e la registrazione nella banca dati [Eurodac](#). I controlli in linea di principio devono essere effettuati in un luogo adeguato e

opportuno designato da ciascuno Stato membro, generalmente ubicato **presso le frontiere esterne** o nelle loro **vicinanze** o, in alternativa, in **altri luoghi** all'interno del suo territorio, durante un periodo massimo di **sette giorni**.

Il regolamento si applica alle persone fermate in caso di **attraversamento non autorizzato** della frontiera esterna per via terrestre, marittima o aerea, a quelle **sbarcate** a seguito di **un'operazione di ricerca e soccorso in mare** e a quelle che hanno presentato domanda di protezione internazionale presso i **valichi di frontiera esterni** o nelle zone di **transito** ma non soddisfano le condizioni d'ingresso. Il nuovo regime riguarda anche le persone fermate sul territorio dell'UE che hanno **eluso** i controlli alle frontiere esterne. Le persone soggette agli accertamenti **non sono autorizzate** ad **entrare** nel territorio di uno Stato membro, devono rimanere a disposizione delle autorità nel luogo in cui sono effettuati gli accertamenti, e possono essere poste in stato di **trattenimento** conformemente alle condizioni e alle garanzie previste dal diritto dell'UE

Nell'ambito dello stesso pilastro merita ricordare altresì il [regolamento](#) volto ad aggiornare la **banca dati** Eurodac delle **impronte digitali**, tra l'altro prevedendo la registrazione dei **singoli richiedenti** asilo anziché delle domande, al fine di consentire alle autorità nazionali di identificare più facilmente le persone che presentano **domande multiple**, di individuare lo **Stato membro competente** per il trattamento di una domanda di asilo, e di tracciare i **movimenti secondari**. La banca dati è ampliata con ulteriori dati biometrici, come le **immagini del volto**. Eurodac include i dati delle persone il cui soggiorno è **irregolare**, delle persone entrate nell'UE in **maniera irregolare** e delle persone sbarcate a seguito di operazioni di **ricerca e soccorso**.

Infine, si ricorda il [regolamento](#) recante una **procedura comune** che gli Stati membri devono seguire quando ricevono una **richiesta di protezione internazionale**, il quale tra gli **elementi qualificanti** prevede l'introduzione di una **procedura di frontiera obbligatoria** tesa a valutare rapidamente alle frontiere esterne dell'UE l'eventuale **infondatezza** o **inammissibilità** delle domande di asilo.

Le persone soggette alla procedura di asilo alla frontiera **non sono autorizzate a entrare** nel territorio dello Stato membro e devono soggiornare alla **frontiera esterna** o in **prossimità della stessa**, oppure in una **zona di transito** o in altri luoghi designati sul territorio di un paese (nel rispetto delle garanzie e delle condizioni previste dalla direttiva sulle condizioni di accoglienza). Per coloro che non hanno diritto alla protezione

e a rimanere nell'UE, si attua la procedura di **rimpatrio** con supporto per la **reintegrazione** nei loro paesi d'origine.

Nell'ambito delle misure collaterali al Nuovo patto, +nel marzo del 2022 la Commissione europea ha per la prima volta nominato un [Coordinatore dell'UE per i rimpatri](#) (la finlandese **Mari Anneli Juritsch**), il cui mandato prevede di riunire i diversi filoni della politica di rimpatrio dell'UE, sostenendone l'attuazione coerente, e istituire un sistema comune dell'UE per i rimpatri.

Il Coordinatore coopera con la **Rete di alto livello per i rimpatri**, composta da rappresentanti delle istituzioni responsabili della materia negli Stati membri e nei Paesi associati Schengen, dell'Agenzia europea della guardia costiera e di frontiera (Frontex) e dell'Agenzia dell'Unione europea per l'asilo (EUAA). La rete si concentra sul **supporto pratico e operativo** agli Stati membri per aumentare l'efficacia del processo di rimpatrio complessivo.

Prospettive di intervento negli orientamenti politici per la Commissione europea 2024-2029

Nei citati orientamenti politici per il mandato della prossima Commissione europea, la Presidente von der Leyen, si è impegnata a sostenere l'attuazione di tutte le parti del nuovo Patto, stabilendo una serie di nuovi obiettivi, tra i quali:

- l'adozione di **nuovo approccio comune sui rimpatri** che comprenda un **nuovo quadro legislativo** volto ad accelerare e semplificare il processo, a garantire che i rimpatri avvengano in modo dignitoso, a digitalizzare la gestione dei fascicoli e a fare sì che le decisioni di rimpatrio siano riconosciute in tutta Europa;
- lo sviluppo di **relazioni strategiche in materia di migrazione e sicurezza con i Paesi terzi**, in particolare con i Paesi di origine e di transito;
- un nuovo **Patto per il Mediterraneo**, che comprenda una cooperazione complessiva su **investimenti**, stabilità economica, lavoro, energia, trasporti, sicurezza, migrazione e altre aree di interesse comune.

Merita ricordare che la Presidente von der Leyen oltre a designare il Commissario Magnus Brunner (Austria) per gli affari interni e la migrazione, che avrà tra l'altro la supervisione sull'attuazione del Patto, ha istituito la nuova figura del Commissario al Mediterraneo, attribuendo tale nuovo

incarico a Dubravka Šuica (Croazia). Al Commissario, sotto la guida dell'Altro Rappresentante per gli affari esteri e la politica di sicurezza, spetterà, tra l'altro, la competenza relativa alla **definizione** del citato **Patto** per il **Mediterraneo**, nonché quella relativa alla **dimensione estera** della **politica migratoria**, con particolare riguardo ai **controlli** alle frontiere e alla lotta ai **trafficienti**.

**SESSIONE DI CONTROLLO II – LA LOTTA ALLA CRIMINALITÀ
INFORMATICA, IN PARTICOLARE AI CRIMINI COMMESSI MEDIANTE
L’INTELLIGENZA ARTIFICIALE; POSSIBILITÀ DI SCAMBIO DI
CONOSCENZE CON IL COINVOLGIMENTO DI CEPOL**

Strumenti di diritto derivato dell’UE per il contrasto alla criminalità informatica

Il contesto

L’UE si sta adoperando su più fronti per promuovere la **ciberresilienza**, **combattere la criminalità informatica**, e **rafforzare la diplomazia informatica** e la **ciberdifesa**, considerato che secondo le stime rese note dalla relativa [pagina web](#) del Consiglio dell’UE, il **costo annuo globale** della criminalità informatica ammonta a circa **5.500 miliardi di euro**.

Sul piano definitorio, la **cibersicurezza** comprende l’insieme delle attività necessarie per **proteggere la rete** e i **sistemi informativi**, gli **utenti** di tali sistemi e altre persone interessate dalle **minacce informatiche**.

Tra i casi più diffusi di criminalità informatica si ricordano:

- l'**utilizzo di botnet**, ossia reti di dispositivi infettati da malware all’insaputa degli utenti, per trasmettere virus che consentono di ottenere il controllo remoto dei dispositivi, rubare le password e disattivare la protezione antivirus;
- la creazione di “**back door**” su dispositivi compromessi, per consentire il furto di denaro e dati o l’accesso remoto ai dispositivi per creare botnet;
- la **creazione di forum online** per lo scambio di competenze in materia di *hacking*;
- il **riciclaggio di valute** (tradizionali e virtuali);
- le **frodi online**, ad esempio attraverso **sistemi di pagamento online**;
- varie forme di **sfruttamento sessuale dei minori online**, tra cui la distribuzione online di materiale pedopornografico e il live-streaming di abusi sessuali su minori;
- l'**hosting online** di operazioni di **vendita di armi, passaporti falsi, carte di credito contraffatte e clonate, droghe e servizi di hacking**.

Il regolamento sulla cibersecurity

Nell'ambito delle politiche UE per contrastare il cybercrime occupa un posto centrale il [regolamento UE sulla cibersecurity](#), entrato in vigore nel **giugno 2019**, che ha introdotto:

- un **sistema europeo di certificazione per prodotti e servizi**, finalizzato a fornire un quadro unico di certificazione in tutta l'UE che possa aumentare la crescita del mercato della cibersecurity ed agevolare il commercio in tutta l'UE. Il quadro fornisce quindi un insieme completo di **norme, requisiti tecnici, standard e procedure**;
- un **nuovo e più forte mandato per l'Agenzia dell'UE per la cibersecurity** (“ENISA”), basata sulle strutture della precedente Agenzia europea per la sicurezza delle reti e dell'informazione, il cui compito è sostenere **gli Stati membri**, le istituzioni dell'UE e altre parti interessate nella **gestione degli attacchi informatici**.

Nel **dicembre 2020** la Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una **nuova strategia** dell'UE in materia di cibersecurity, il cui **obiettivo è rafforzare la resilienza** dell'Europa a fronte delle **minacce informatiche** e garantire che tutti i cittadini e le imprese possano beneficiare **pienamente di servizi e strumenti digitali affidabili e attendibili**. La nuova strategia include proposte concrete per l'introduzione di strumenti normativi, strategici e di investimento.

La nuova strategia costituisce una componente fondamentale del [futuro digitale dell'Europa](#), del [piano di ripresa](#) della Commissione [per l'Europa](#) e della [strategia dell'Unione per la sicurezza 2020-2025](#).

La direttiva NIS

La **direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS)**, è stata introdotta nel 2016 quale prima misura legislativa UE in materia, poi sostituita nel 2022 dalla [direttiva NIS riveduta \(NIS2\)](#). Le nuove norme garantiscono un **livello comune elevato di cibersecurity nell'UE**, rispondendo al panorama di minacce in evoluzione e tenendo in considerazione la trasformazione digitale, accelerata dalla pandemia di COVID-19. La disciplina, entrata **in vigore il 16 gennaio 2023**:

- stabilisce **nuove norme minime** per un quadro normativo;
- definisce **meccanismi per una cooperazione** efficace tra le autorità competenti di ciascun paese dell'UE;
- aggiorna l'**elenco dei settori** e delle attività soggetti agli obblighi in materia di cibersecurity.

Il regolamento sulla ciberresilienza

Il **10 ottobre 2024** è stato adottato il [regolamento dell'UE sulla ciberresilienza](#), recante norme sui **requisiti di cibersecurity** per i **prodotti con elementi digitali**, al fine di garantire che prodotti quali fotocamere domestiche connesse, frigoriferi, televisori e giocattoli siano sicuri prima della loro immissione sul mercato. Il nuovo regolamento mira a colmare le lacune, chiarire i collegamenti e rendere **più coerente il quadro normativo in vigore** in materia di **cibersecurity**, garantendo che i prodotti con componenti digitali, ad esempio i prodotti dell'internet delle cose, siano resi sicuri lungo l'intera catena di approvvigionamento e per tutto il ciclo di vita.

In particolare, il nuovo regolamento introduce requisiti di cibersecurity a livello di UE per la **progettazione**, lo **sviluppo**, la **produzione** e la **messa a disposizione** sul mercato di **prodotti hardware** e **software** al fine di evitare la sovrapposizione di requisiti derivanti da diversi atti legislativi negli Stati membri dell'UE. Ad esempio, i prodotti software e hardware riceveranno la marcatura CE per indicare che sono conformi ai requisiti del regolamento. Inoltre, il regolamento si applicherà a tutti i prodotti connessi direttamente o indirettamente a un altro dispositivo o a una rete. Infine, il nuovo regolamento consentirà ai **consumatori** di tener conto della cibersecurity quando **selezionano e utilizzano prodotti** contenenti elementi digitali, rendendo più facile individuare prodotti hardware e software con caratteristiche di cibersecurity adeguate.

Allo scopo di conseguire il **ravvicinamento delle disposizioni di diritto penale** degli Stati membri nel settore degli attacchi contro i sistemi di informazione, nel **2013** è stata adottata la [direttiva \(UE\) 2013/40](#) recante norme atte ad armonizzare la criminalizzazione e le sanzioni penali per una serie di reati contro i sistemi informatici.

Il ruolo di Europol nella lotta alla criminalità informatica

Nel 2013 Europol ha istituito il [Centro europeo per la criminalità informatica \(EC3\)](#), per rafforzare la risposta delle forze dell'ordine alla

criminalità informatica nell'UE e contribuire a proteggere i cittadini, le imprese e i governi europei.

Il **Centro europeo** si concentra sui seguenti tipi di crimini informatici: crimini dipendenti dal cyberspazio, sfruttamento sessuale dei minori e frode nei pagamenti.

Offre tra l'altro **supporto operativo, strategico, analitico e forense** alle indagini degli Stati membri, fungendo da **hub centrale** per le **informazioni e l'intelligence** sul questo settore criminale. Esso fornisce, inoltre, **supporto** alle autorità, 24 ore su 24, 7 giorni su 7, per reagire immediatamente a incidenti informatici urgenti e/o crisi informatiche tramite il servizio di stand-by e il protocollo di risposta di emergenza dell'UE per le forze dell'ordine. Ulteriori compiti del centro riguardano, tra l'altro, la **formazione e lo sviluppo di capacità**, una **serie di prodotti di analisi strategica, la preparazione e attuazione di campagne e attività standardizzate** di prevenzione e sensibilizzazione nelle aree di competenza della criminalità informatica.

Inoltre, ogni anno il Centro pubblica la [Valutazione della minaccia della criminalità organizzata su Internet](#) (“IOCTA”), che stabilisce le priorità per il Piano d'azione operativo EMPACT nelle aree della criminalità informatica che sono al centro dell'attenzione per quell'anno.

Il Centro ospita anche la [Task Force congiunta d'azione contro la criminalità informatica](#) (“J-CAT”), il cui obiettivo è, tra l'altro, guidare un'azione coordinata dall'intelligence contro le principali minacce alla criminalità informatica attraverso indagini e operazioni transfrontaliere dei suoi partner.

L'uso dell'intelligenza artificiale per finalità criminali

Come sottolinea la apposita [scheda tematica](#) del servizio di ricerca del Parlamento europeo, la **crescente integrazione dell'intelligenza artificiale** (“IA”) nella vita quotidiana richiede una **particolare attenzione alla protezione dei modelli, dei dati, della formazione e delle implementazioni** legate al suo utilizzo. La cybersicurezza è, quindi, il presupposto per modelli e algoritmi di IA affidabili, sicuri e resilienti.

In particolare, il rapporto tra IA e cybersicurezza ha **tre dimensioni**: la cybersicurezza dell'IA, che riguarda la standardizzazione dell'IA; l'uso dell'IA per supportare la cybersicurezza; **l'uso dell'IA per scopi criminali**,

foriero di nuove minacce. Mentre gli aspetti di cybersecurity dell'IA ricevono molta attenzione, i dati dimostrano che l'uso dell'IA a favore e contro la cybersecurity si sta sviluppando rapidamente. In particolare, l'intelligenza artificiale può essere utilizzata **anche** per gli **attacchi informatici**, come le **campagne di disinformazione** e la **codifica di malware** (ossia un software dannoso progettato per compromettere o sfruttare qualsiasi tipo di dispositivo, servizio o rete programmabile). Secondo l'ENISA, i sistemi di intelligenza artificiale stanno diventando particolarmente potenti nelle **tecniche di ingegneria sociale** grazie alla loro **capacità di imitare l'interazione umana**.

Microsoft ha recentemente riferito che gli attori delle minacce utilizzano attivamente i modelli linguistici di grandi dimensioni (LLM) disponibili per progettare i loro attacchi. Sebbene i sistemi di intelligenza sulle minacce di Microsoft e Open AI non abbiano finora identificato “nuove o uniche tecniche di attacco o di abuso abilitate dall'IA e derivanti dall'uso dell'IA da parte degli attori delle minacce”, essi sottolineano l'importanza di un **monitoraggio continuo** e ravvicinato per **rilevare eventuali tentativi incrementali** e **rimanere al passo con l'evoluzione** delle minacce.

L'IA può essere quindi sfruttata per creare **nuovi potenti tipi di attacchi**. I ricercatori di Google hanno dimostrato come l'IA possa essere utilizzata per **comprendere modelli crittografici avanzati** e **prevedere informazioni** che possono essere sfruttate. Hanno pubblicato un **documento di ricerca** che presenta un potente strumento di intelligenza artificiale in grado di **attaccare diversi algoritmi crittografici**. Il documento conclude sottolineando la “pressante necessità di concepire **nuove protezioni** che siano resistenti agli **attacchi di deep-learning**”.

Il coinvolgimento di CEPOL nel contrasto al cyber crime

Istituita con [regolamento \(UE\) 2015/2219](#), l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto ([CEPOL](#)) sostiene, sviluppa, realizza e coordina **attività di formazione** per i **funzionari** delle autorità di contrasto, ponendo un accento particolare sulla **tutela dei diritti umani** e delle **libertà fondamentali** nell'ambito delle attività di contrasto, in particolare, nel settore della **prevenzione** e della **lotta** contro la **criminalità grave** che interessa due o più Stati membri e il terrorismo, del mantenimento dell'ordine pubblico, in particolare le **operazioni di polizia internazionali** in occasione di eventi di primo piano, e della programmazione e del comando

di missioni dell'Unione, che possono includere anche la formazione sul comando delle attività di contrasto e le competenze linguistiche.

Alla guida di CEPOL vi è un **direttore esecutivo**, il quale riferisce al **consiglio di amministrazione**, composto da **rappresentanti** degli **Stati membri** dell'UE e della **Commissione europea**. Il presidente del consiglio di amministrazione è il rappresentante di uno dei tre Stati membri che hanno preparato congiuntamente il programma di 18 mesi del Consiglio dell'UE. Il consiglio di amministrazione si riunisce almeno **due volte all'anno**. Inoltre, CEPOL ha **unità nazionali** dedicate in ogni Stato membro per fornire informazioni e assistenza ai funzionari delle autorità di contrasto che desiderano partecipare alle attività di CEPOL. Le unità nazionali sostengono le operazioni di CEPOL.

Il programma di lavoro annuale dell'agenzia è stilato con il contributo di tale rete e di altre parti interessate in modo da prevedere attività localizzate e mirate, intese a soddisfare i bisogni degli Stati membri nelle aree prioritarie derivanti dalla strategia dell'UE in materia di sicurezza interna. Inoltre, CEPOL valuta il fabbisogno formativo per far fronte alle priorità dell'UE in materia di sicurezza.

L'offerta di CEPOL comprende attività **formative residenziali**, **apprendimento online** (cioè webinar, moduli online, corsi online, ecc.), programmi di scambio, piani formativi comuni, ricerca e scienza.

La CEPOL contribuisce allo sviluppo delle competenze e delle conoscenze in materia di **criminalità informatica** e di attività illecite ad essa collegate attraverso la sua **Cybercrime Academy**, un centro di formazione specializzato a **Budapest** che ospita regolarmente funzionari delle forze dell'ordine provenienti da tutta l'UE.