

Argomento aperto sulla prevenzione e contrasto dell'uso improprio delle tecnologie emergenti a fini penali, inclusi temi legati all'accesso legale ai dati

Open topic on preventing and countering the misuse of emerging technologies for criminal purposes, including issues related to lawful access to data

TOPIC ID:

HORIZON-CL3-2026-01-FCT-02

Ente finanziatore:

Commissione europea
Programma Horizon europe

Obiettivi ed impatto attesi:

Risultati attesi

I risultati dei progetti dovranno contribuire a tutti i seguenti risultati attesi:

- le Police Authorities europee dispongono di strumenti, metodologie e programmi formativi moderni, accessibili e validati per anticipare e affrontare l'uso improprio delle tecnologie nuove ed emergenti a fini criminali. Tali strumenti devono facilitare la prevenzione, l'individuazione dei reati, l'accesso efficace ai dati e le attività investigative, nel pieno rispetto della legge e dei diritti fondamentali, compresi il diritto alla protezione dei dati personali e alla privacy;
- viene rafforzata la collaborazione interdisciplinare a livello europeo, attraverso partenariati tra esperti tecnologici, decisori politici e Police Authorities, favorendo una comprensione complessiva delle sfide poste dalle tecnologie emergenti e la condivisione delle migliori pratiche;
- vengono sviluppate linee guida e framework chiari, comprese procedure e regole per garantire l'accesso legittimo ai dati, assicurando un equilibrio tra le esigenze di sicurezza e il rispetto della privacy e promuovendo un approccio europeo comune alle relative sfide per le autorità di polizia e giudiziarie.

Ambito di intervento

Le tecnologie nuove ed emergenti offrono significativi vantaggi, ma determinano al tempo stesso nuove sfide per le autorità di polizia e per il sistema giudiziario.

Tra le tecnologie considerate rientrano, a titolo esemplificativo:

- nuove tecnologie di comunicazione;
- tecnologie quantistiche;
- nuove tecnologie biometriche e di identificazione;
- tecnologie di cloud computing;
- Generative AI;
- altre tecnologie nuove ed emergenti rilevanti per le attività di contrasto.

È pertanto necessario affrontare adeguatamente le nuove criticità derivanti dall'evoluzione tecnologica e garantire che l'accesso legittimo ai dati evolva parallelamente alle tecnologie, nel rispetto della normativa applicabile e dei diritti fondamentali, in particolare della protezione dei dati personali e della privacy.

Open Topic

Il topic ha natura aperta e accoglie proposte relative a tecnologie nuove ed emergenti non già adeguatamente affrontate dai progetti delle precedenti call Horizon Europe – Fighting Crime and Terrorism né dagli altri topic della Call Fighting Crime and Terrorism 2026–2027.

Le proposte devono privilegiare metodologie e framework adattivi, capaci di evolvere in risposta a nuove minacce e nuove sfide, consentendo alle Police Authorities di operare efficacemente e, al contempo, garantendo il rispetto delle disposizioni giuridiche applicabili all'accesso ai dati.

Attività di ricerca

Le attività proposte devono affrontare in maniera equilibrata due dimensioni principali:

1. Contrasto all'uso criminale delle tecnologie emergenti

Sviluppo di strumenti moderni, metodologie e materiali formativi destinati alle Police Authorities per prevenire e contrastare l'utilizzo a fini criminali delle tecnologie nuove ed emergenti oggetto del progetto.

2. Lawful access to data

Analisi e sviluppo di soluzioni relative all'accesso legittimo ai dati nel contesto delle tecnologie considerate, garantendo il rispetto della normativa applicabile, della protezione dei dati personali, della privacy e degli altri diritti fondamentali.

Dimensione di genere e intersezionale

Per il presente topic, l'integrazione della dimensione di genere e intersezionale, comprese le analisi relative a sesso e genere, nei contenuti di ricerca e innovazione non costituisce un requisito obbligatorio.

Coordinamento tra i progetti

Deve essere previsto il coordinamento tra le proposte selezionate nell'ambito del topic, al fine di:

- evitare duplicazioni;
- valorizzare le complementarità;
- individuare opportunità per aumentare l'impatto complessivo dei risultati.

Cooperazione con Europol, EU Drugs Agency e CEPOL

I progetti che affrontano tematiche rientranti nel mandato di Europol dovranno prevedere il coinvolgimento dello Europol Innovation Lab durante il ciclo di vita del progetto, compresa la validazione dei risultati, con l'obiettivo di facilitare la futura adozione delle innovazioni da parte della comunità delle autorità di contrasto.

Qualora le proposte riguardino problematiche connesse alle droghe, è previsto il coinvolgimento della EU Drugs Agency, anche ai fini della validazione dei risultati.

Per gli aspetti relativi alla formazione delle Police Authorities, è prevista la cooperazione con CEPOL, a condizione che l'Agenzia non presenti domanda di finanziamento nell'ambito della call.

Le proposte devono infine tenere conto di tutte le considerazioni applicabili indicate nell'introduzione della Destination Fighting Crime and Terrorism.

Criteri di eleggibilità:

Qualsiasi soggetto giuridico, indipendentemente dal luogo in cui è stabilito, compresi i soggetti giuridici di Paesi terzi non associati o le organizzazioni internazionali (incluse le organizzazioni internazionali europee di ricerca), è ammissibile a partecipare, indipendentemente dal fatto che sia o meno ammissibile al finanziamento, a condizione che siano rispettate le condizioni stabilite dal Regolamento Horizon Europe, nonché ogni altra condizione prevista dallo specifico invito a presentare proposte/topic.

Per «soggetto giuridico» si intende qualsiasi persona fisica o giuridica costituita e riconosciuta come tale ai sensi del diritto nazionale, del diritto dell'Unione europea o del diritto internazionale, dotata di personalità giuridica e che, agendo in nome proprio, possa esercitare diritti ed essere soggetta a obblighi, oppure un'entità priva di personalità giuridica.

I beneficiari e le entità affiliate devono registrarsi nel Registro dei partecipanti (Participant Register) prima della presentazione della domanda, al fine di ottenere un codice di identificazione del partecipante (PIC), e devono essere convalidati dal Servizio centrale di convalida (Central Validation Service) prima della firma della convenzione di sovvenzione.

Ai fini della convalida, durante la fase di preparazione della convenzione di sovvenzione sarà richiesto di caricare la documentazione necessaria attestante lo status giuridico e il Paese di stabilimento.

Il possesso di un PIC già convalidato non costituisce un requisito preliminare per la presentazione della domanda.

Per ulteriori informazioni, si vedano le norme relative alla convalida dei soggetti giuridici, alla nomina del LEAR e alla valutazione della capacità finanziaria.

Utilizzo dei sistemi spaziali europei

Qualora i progetti utilizzino dati o servizi satellitari relativi all'osservazione della Terra, al posizionamento, alla navigazione e/o ai relativi servizi di temporizzazione, i beneficiari devono utilizzare:

Copernicus e/o Galileo/EGNOS.

È consentito l'utilizzo aggiuntivo di altri dati e servizi.

Technology Readiness Level – TRL

Le attività devono raggiungere, entro la conclusione del progetto:

TRL 5 – Technology Readiness Level 5.

Configurazione giuridica e finanziaria del Grant Agreement

Si applicano le disposizioni previste dal General Annex G di Horizon Europe, con specifiche eccezioni.

L'autorità concedente può, fino a 4 anni dopo la conclusione dell'azione, opporsi al trasferimento della proprietà dei risultati o alla concessione di licenze esclusive sugli stessi, secondo quanto previsto dalle specifiche disposizioni dell'Annex 5 del Grant Agreement.

Condizioni di ammissibilità

Si applicano le condizioni stabilite nel General Annex B di Horizon Europe, con i seguenti criteri aggiuntivi di ammissibilità.

Il topic richiede il coinvolgimento attivo, in qualità di beneficiari, di almeno 2 Police Authorities appartenenti ad almeno 2 diversi Stati membri dell'UE o Paesi associati.

Ai fini del presente topic, per Police Authorities si intendono le autorità pubbliche espressamente designate dalla legislazione nazionale, oppure altri soggetti legalmente incaricati dall'autorità nazionale

competente, per la prevenzione, l'individuazione e/o l'investigazione di reati di terrorismo o di altri reati. Sono espressamente esclusi dalla definizione di Police Authorities:

- accademie di polizia;
- istituti forensi;
- strutture di formazione;
- autorità di frontiera;
- autorità doganali.

Per le Police Authorities partecipanti, i richiedenti devono compilare nell'Application Form la tabella "Information about security practitioners", fornendo tutte le informazioni richieste secondo il modello disponibile nel sistema informatico di presentazione della proposta.

Protezione delle reti europee di comunicazione

Il topic è soggetto a restrizioni finalizzate alla protezione delle reti europee di comunicazione.

Contributo finanziario:

Contributo UE per progetto

La Commissione stima che un contributo UE di circa 4,5 milioni di EUR per progetto sia adeguato a conseguire i risultati previsti dal topic.

È comunque possibile presentare e selezionare proposte che richiedano importi differenti.

Budget indicativo

Il budget indicativo complessivo disponibile per il topic è pari a:

9 milioni di EUR.

Tipologia di azione

Research and Innovation Action (RIA) – Azione di ricerca e innovazione.

Forma del finanziamento

I costi ammissibili saranno finanziati mediante lump sum, ossia attraverso un contributo forfettario, secondo le disposizioni applicabili nell'ambito di Horizon Europe.

Security Sensitive

Alcune attività derivanti dal topic possono comportare l'utilizzo di background classificato e/o la produzione di risultati sensibili sotto il profilo della sicurezza, comprese:

- EU Classified Information (EUCI);
- Sensitive Information (SEN).

Si applicano pertanto le specifiche disposizioni in materia di Security – EU classified and sensitive information previste dai General Annexes di Horizon Europe.

Scadenza:

05 Novembre 2026 17:00:00 Brussels time

Ulteriori informazioni:

[Civil Security for Society](#)