COMMISSIONE
EUROPEA

Bruxelles, 24.6.2025
COM(2025) 349 final

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

Tabella di marcia per assicurare alle autorità di contrasto un accesso legittimo ed effettivo ai dati

Introduzione

Come indicato nella strategia europea di sicurezza interna ("ProtectEU")[1], **la sicurezza è il fondamento di tutte le nostre libertà**. La democrazia, lo Stato di diritto, i diritti fondamentali, il benessere dei cittadini europei, la competitività e la prosperità dipendono tutti dalla nostra capacità di garantire le basi della sicurezza.

L'UE e gli Stati membri hanno il dovere di garantire che i cittadini possano godere di un **elevato livello di sicurezza nella loro vita quotidiana**. A tal fine, le autorità di contrasto e giudiziarie devono disporre degli strumenti necessari per tracciare le attività illecite, identificare gli autori di reati, smantellare le reti criminali e proteggere le vittime, garantendo in ultima istanza la giustizia penale, nel pieno rispetto dei diritti fondamentali.

Terrorismo, criminalità organizzata, frodi online, traffico di droga, abuso sessuale su minori, estorsione sessuale online, ransomware e molti altri reati hanno qualcosa in comune: lasciano **tracce digitali**. Come osserva Europol nella sua valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA) per il 2025, quasi tutte le forme di criminalità grave e organizzata hanno un'impronta digitale[2]. **Circa l'85 % delle indagini penali si basa oggi su prove elettroniche**[3]. Le richieste di dati rivolte ai prestatori di servizi sono triplicate tra il 2017 e il 2022 e tali dati sono sempre più necessari[4].

Sebbene di recente siano stati osservati esempi notevoli di misure di repressione nei confronti di reti di comunicazione criminali[5] da parte delle autorità di contrasto e giudiziarie, molte altre indagini sono **ritardate o rese infruttuose dalla mancanza di un accesso tempestivo alle prove digitali[6].** Nell'ultimo decennio le autorità di contrasto e giudiziarie hanno perso terreno nei confronti dei criminali, in quanto questi ultimi si avvalgono di strumenti e prodotti offerti da prestatori di servizi che hanno messo in atto misure che impediscono la cooperazione in relazione a richieste legittime[7].

Prove di reato fondamentali rimangono inaccessibili perché[8]:

- **sono eliminate** dai prestatori di servizi entro pochi giorni, in linea con i rispettivi obblighi in materia di protezione dei dati personali e della vita privata o con le loro esigenze commerciali;
- **non possono essere ottenute** a causa di conflitti di leggi tra giurisdizioni, in quanto i diversi paesi hanno leggi e regolamenti diversi in materia di accesso ai dati, il che rende difficile ottenere dati archiviati all'estero;

---

[1] EUR-Lex - 52025DC0148 - IT - EUR-Lex.

[2] *European Union Serious and Organised Crime Threat Assessment 2025* EU-SOCTA-2025.pdf.

[3] Valutazione d'impatto della Commissione sulle proposte di regolamento sulle prove elettroniche e di direttiva sulle prove elettroniche (17 aprile 2018) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:IT:PDF.

[4] *2023 SIRIUS Report*, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, pag. 69.

[5] "Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized" | Europol
joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf/"Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" | Europol.

[6] Segnalato dal gruppo ad alto livello sull'accesso ai dati per un'efficace azione di contrasto - Commissione europea.

[7] *Concluding report of the High-Level Group on access to data for effective law enforcement* (15 novembre 2024).

[8] *Common Challenges in Cybercrime - 2024 Review by Europol and Eurojust.*

- **non possono essere recuperate dai dispositivi sequestrati nelle indagini penali** perché l'**informatica forense** è difficile, se non del tutto impraticabile;
- **non possono essere lette** perché i dati sono criptati;
- **non possono essere analizzate in modo efficace e legittimo** perché mancano tecnologie adeguate o risorse umane sufficienti per filtrare e analizzare efficacemente grandi quantità di dati sequestrati senza interferire con i quadri giuridici dell'UE e degli Stati membri.

In risposta a tali sfide, nel 2023 è stato istituito un **gruppo ad alto livello sull'accesso ai dati per un'efficace attività di contrasto** (gruppo ad alto livello), che ha formulato 42 raccomandazioni nei mesi di maggio e novembre 2024. Il **Consiglio "Giustizia e affari interni" dell'UE** ha approvato le raccomandazioni del gruppo ad alto livello[9] il 13 giugno 2024 e successivamente, nel dicembre 2024, ha adottato conclusioni in cui invitava la Commissione a redigere una tabella di marcia. La tabella di marcia doveva basarsi sui lavori del gruppo ad alto livello e sulle sue raccomandazioni per attuare misure volte ad assicurare alle autorità di contrasto l'accesso legittimo ed effettivo ai dati[10]. La presente comunicazione risponde a questa raccomandazione.

Poiché la digitalizzazione diventa più pervasiva e fornisce ai criminali un numero sempre maggiore di nuovi strumenti, è essenziale definire un quadro per l'**accesso legittimo ai dati** in modo da garantire che i criminali siano tradotti in giustizia. L'"accesso legittimo" a cui fa riferimento la tabella di marcia è l'accesso, conforme al diritto, alle informazioni digitali di cui le autorità di contrasto hanno bisogno a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

Per essere legittimo, l'accesso ai dati deve essere **necessario e proporzionato e rispettare i diritti fondamentali**, garantendo un'adeguata protezione della vita privata e dei dati personali; deve basarsi su **norme chiare, precise e accessibili stabilite dal diritto**, soggetto a **meccanismi di controllo** indipendenti e a **mezzi di ricorso efficaci** a disposizione di coloro che potrebbero essere interessati dall'accesso ai loro dati. La **sicurezza informatica** dei sistemi digitali contro l'accesso non autorizzato è una difesa altrettanto importante dalle minacce per la cibersicurezza.

I. Garantire la disponibilità di prove digitali: la conservazione dei dati[11]

In Spagna, un'indagine penale sulla scomparsa di una giovane donna è stata risolta nel 2019 grazie ai dati relativi alla localizzazione conservati da un prestatore di servizi di comunicazione secondo un obbligo giuridico nazionale. Tali dati hanno consentito agli investigatori di localizzare la donna scomparsa, di stabilire che anche il sospettato del rapimento si trovava in tale zona e di escludere altri sospettati[12]. I dati delle comunicazioni non relativi al contenuto

[9] *Recommendations of the High-Level Group on access to data for effective law enforcement.*

[10] *Conclusioni del Consiglio sull'accesso ai dati per un'efficace attività di contrasto* (12 dicembre 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/it/pdf; *Conclusioni del Consiglio sulle future priorità per rafforzare gli sforzi congiunti dell'Unione europea e dei suoi Stati membri in materia di lotta al terrorismo* (12 dicembre 2024) https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/it/pdf.

[11] La conservazione dei dati si riferisce al fatto che i prestatori di servizi conservano per un dato periodo determinati dati non relativi al contenuto, trattati nel contesto dei servizi di comunicazione da essi forniti, al fine di consentire alle autorità competenti di accedervi nel contesto delle indagini penali, nel rispetto di garanzie adeguate, e garantire la giustizia penale.

[12] "La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina | España".

(ad esempio informazioni relative agli abbonati, dati relativi alla localizzazione, data, ora, durata, mittente e destinatario e dimensioni della comunicazione) sono fondamentali nella maggior parte delle indagini e delle azioni penali e possono essere decisivi per identificare e localizzare vittime, sospettati e imputati, facendo luce su un reato commesso e aiutando ad escludere altri sospettati.

In linea con la normativa dell'UE in materia di protezione della vita privata e dei dati, i prestatori di servizi di comunicazione elettronica possono conservare i dati delle comunicazioni non relativi al contenuto che passano nei relativi sistemi solo per il tempo necessario a fini commerciali specifici, espliciti e legittimi. Gli obblighi giuridici possono tuttavia imporre loro di mantenere (o "conservare") tali dati per altri obiettivi, ad esempio qualora siano necessari a fini di prevenzione, indagine, accertamento e perseguimento di reati.

Da quando la direttiva dell'UE sulla conservazione dei dati[13] è stata dichiarata invalida nel 2014[14], il panorama legislativo dell'UE che obbliga i prestatori di servizi a conservare i dati è diventato frammentato e disomogeneo. I quadri di conservazione dei dati degli Stati membri divergono per quanto riguarda i tipi di comunicazioni elettroniche che i prestatori di servizi devono conservare, le categorie di dati che coprono e i periodi di conservazione richiesti[15]. Alcuni Stati membri non dispongono di leggi in materia di conservazione dei dati. Le autorità di contrasto e giudiziarie incontrano ostacoli giuridici e operativi nello svolgimento del proprio lavoro. I fornitori di comunicazioni elettroniche, in particolare quelli più piccoli, devono affrontare costi e ostacoli aggiuntivi quando prestano i propri servizi in tutta l'UE, in quanto sono tenuti a rispettare obblighi giuridici diversi nei diversi Stati membri.

Il gruppo ad alto livello ha pertanto raccomandato di istituire **un quadro armonizzato dell'UE sulla conservazione dei dati** al fine di garantire la disponibilità delle prove digitali necessarie per indagare e perseguire i reati. Un regime armonizzato a livello dell'UE limiterebbe la frammentazione tra gli Stati membri per quanto riguarda le norme in materia di conservazione e le garanzie relative ai diritti fondamentali, in particolare alla protezione della vita privata e dei dati e ai diritti di difesa, compreso il diritto a un processo equo. Tale quadro giuridico garantirebbe in tal modo anche la certezza del diritto per le autorità competenti, da un lato, e per i prestatori di servizi, dall'altro[16].

Azione fondamentale

- **Nel 2025 la Commissione preparerà una valutazione d'impatto al fine di aggiornare, laddove opportuno, le norme dell'UE in materia di conservazione dei dati.**

[13] https://eur-lex.europa.eu/eli/dir/2006/24/oj.

[14] Sentenza della Corte (Grande Sezione) dell'8 aprile 2014, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e altri*.

[15] Per una panoramica, cfr. *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU* | Eurojust | Agenzia dell'Unione europea per la cooperazione giudiziaria penale e *Study on the retention of electronic communications non-content data for law enforcement purposes*, Commissione europea.

[16] "Recommendation Cluster 6", *Concluding Report of the High-Level Group*.

Il gruppo ad alto livello ha individuato la necessità di **rafforzare le sinergie tra i professionisti preposti all'azione di contrasto e i prestatori di servizi**[17].

A tal fine, **l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust)** sono invitate a proseguire e intensificare l'impegno **per facilitare la cooperazione e lo scambio di informazioni e migliori pratiche tra professionisti e prestatori di servizi** attraverso il **progetto SIRIUS**[18], con il costante sostegno della Commissione. Il progetto SIRIUS è diventato la più importante fonte di informazioni **per aiutare i professionisti preposti all'azione di contrasto e le autorità giudiziarie nell'UE e nel resto del mondo ad accedere alle prove elettroniche conservate da prestatori di servizi online** con sede in paesi terzi. La piattaforma SIRIUS conta oltre 8 000 membri delle comunità di contrasto e giudiziarie, che rappresentano 47 paesi in tutto il mondo, e ha sostenuto direttamente quasi 70 operazioni di polizia.

Allo stesso scopo, Europol ed Eurojust dovrebbero utilizzare il progetto SIRIUS per sviluppare, in cooperazione con il **settore privato, un catalogo dei dati che i servizi di comunicazione elettronica trattano legittimamente per i loro fini commerciali**. Ciò aiuterà le autorità competenti a individuare i dati che possono essere disponibili per le loro richieste di accesso legittimo, a individuare i prestatori di servizi pertinenti e a orientare meglio le richieste di accesso legittimo, riducendo così tempo e costi sia per le autorità pubbliche sia per i prestatori di servizi.

Azioni fondamentali

- **Con il costante sostegno della Commissione, Europol ed Eurojust sono invitati a basarsi sul progetto SIRIUS per razionalizzare la cooperazione con i prestatori di servizi di comunicazione elettronica.**

- **Europol ed Eurojust sono invitati ad elaborare, in cooperazione con il settore privato, un catalogo dei dati che i fornitori di comunicazioni elettroniche trattano per i loro fini commerciali (l'inizio è previsto per il quarto trimestre del 2025).**

II. Acquisizione di prove tra diversi sistemi e giurisdizioni: l'intercettazione legale

L'accesso legittimo ai dati delle comunicazioni in tempo reale è essenziale per combattere i criminali online e offline. Nel 2020 una squadra investigativa comune francese e neerlandese ha smantellato EncroChat, una rete telefonica cifrata ampiamente utilizzata dai gruppi della criminalità organizzata. Tale indagine congiunta ha comportato l'intercettazione di milioni di messaggi in tempo reale tra criminali che intendevano compiere reati gravi, la condivisione dei messaggi con altre autorità e la relativa analisi. Grazie alle informazioni ottenute, le autorità di contrasto di tutta Europa e di altre parti del mondo hanno sventato attività criminali, tra cui attacchi violenti, corruzione, tentati omicidi e traffico di droga su larga scala. Alcuni messaggi rivelavano l'intenzione di commettere reati violenti nell'imminenza e hanno permesso alle

[17] "Recommendation Cluster 5", *Concluding Report of the High-Level Group*.
[18] *SIRIUS Project* | Europol.

autorità di contrasto di prevenirli[19]. L'ordine europeo di indagine (OEI) ha facilitato la condivisione efficiente di tali prove[20].

Il caso EncroChat dimostra che l'accesso in tempo reale ai dati relativi al contenuto delle comunicazioni è uno strumento essenziale per indagini e azioni penali efficaci nei confronti dei gruppi della criminalità organizzata. Rimane tuttavia uno dei pochi esempi di successo: il gruppo ad alto livello ha osservato che l'efficacia dell'intercettazione legale[21] è drasticamente diminuita in quanto la comunicazione è passata dalle chiamate telefoniche e dagli SMS tradizionali ai servizi di messaggistica "over the top" (OTT) forniti tramite applicazioni. Attualmente circa il 97 % di tutti i messaggi mobili è inviato tramite applicazioni di messaggistica, mentre i messaggi SMS e MMS tradizionali rappresentano solo il 3 % circa dei messaggi[22]. Il gruppo ad alto livello ha inoltre osservato che dal 2020, a seguito dell'interruzione di alcune delle principali reti di comunicazione criminali, molti gruppi criminali hanno deciso di tornare a servizi regolari di messaggistica OTT cifrati da punto a punto[23].

Nell'UE le norme nazionali che impongono obblighi di intercettazione legale sono frammentate[24]. Il gruppo ad alto livello ha osservato che, mentre alcuni Stati membri impongono obblighi analoghi per tutti i tipi di servizi di comunicazione elettronica, compresi gli OTT, altri li escludono. Spesso inoltre i prestatori di servizi non sono stabiliti nello Stato membro dell'autorità richiedente, il che può comportare questioni giurisdizionali complesse, conflitti di leggi e problemi di applicazione[25]. Di conseguenza, il contenuto di tali servizi di messaggistica è praticamente inaccessibile.

L'OEI e altri strumenti di cooperazione possono contribuire a superare il problema dell'intercettazione transfrontaliera in alcune parti dell'UE. Tuttavia le autorità degli Stati membri incontrano ancora difficoltà nell'utilizzarli: tali strumenti non possono aiutare l'intercettazione se il servizio è fornito da Stati membri che non partecipano allo strumento in questione o da un paese terzo. Il gruppo ad alto livello ha pertanto raccomandato una serie di misure volte a garantire che un'ampia gamma di fornitori, compresi i fornitori OTT, risponda alle richieste di intercettazione legale[26].

In risposta, la **Commissione proporrà modi per migliorare le misure volte a rafforzare la cooperazione transfrontaliera in materia di intercettazione** sia tra le autorità, sia tra queste ultime e i prestatori di servizi. A seguito delle raccomandazioni del gruppo ad alto livello, la Commissione si adopererà principalmente per migliorare gli strumenti esistenti, in particolare l'OEI, e la cooperazione volontaria (laddove non vi siano conflitti di leggi con paesi terzi o gli

---

[19] "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" | Europol; "Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée".

[20] "European Investigation Order" | Eurojust | Agenzia dell'Unione europea per la cooperazione giudiziaria penale.

[21] Nel contesto della presente comunicazione, le tecnologie di intercettazione legale attuate per ottenere l'accesso in tempo reale ai dati delle comunicazioni nelle indagini giudiziarie da parte di un operatore di comunicazione nonché le tecnologie che possono essere utilizzate autonomamente dalle autorità di contrasto.

[22] *Concluding Report of the High-Level Group*, pag. 38.

[23] *Internet Organised Crime Threat Assessment IOCTA 2024*.

[24] Cfr. Libro bianco dell'UE *Come affrontare adeguatamente le esigenze dell'Europa in termini di infrastruttura digitale?*, pag. 14; relazione Letta sul mercato interno, pag. 59 e relazione Draghi sulla competitività dell'UE, pagg. 70, 74, 76.

[25] *Concluding Report of the High-Level Group*, pag. 41.

[26] "Recommendation Cluster 8", *Concluding Report of the High-Level Group*.

stessi siano stati revocati). In ultima analisi, gli Stati membri dovrebbero poter imporre obblighi di intercettazione legale a tutti i prestatori di servizi di comunicazione che propongono servizi a livello nazionale, come previsto dalle legislazioni nazionali, indipendentemente dal fatto che si tratti di servizi di telecomunicazione tradizionali o basati su internet e a prescindere dalla loro ubicazione.

Inoltre alcuni Stati membri non dispongono delle capacità di rete necessarie per la condivisione dei dati nella cooperazione transfrontaliera. Pertanto la **Commissione individuerà le esigenze degli Stati membri** e sosterrà lo sviluppo di reti sicure con una larghezza di banda sufficiente tra gli Stati membri interessati, consentendo il trasferimento di grandi quantità di dati in tempo reale. Tale iniziativa potrebbe essere finanziata dai programmi dell'UE.

Azioni fondamentali

La Commissione intende:

- **proporre misure per migliorare l'efficienza delle richieste transfrontaliere di intercettazione legale attraverso gli strumenti esistenti, valutando fra l'altro la necessità di rafforzare ulteriormente l'ordine europeo di indagine (entro il 2027);**

- **vagliare misure volte a creare condizioni di parità per tutti i tipi di prestatori di servizi di comunicazione nell'esecuzione degli obblighi di intercettazione legale;**

- **determinare l'approccio più efficiente per far fronte ai prestatori di servizi di comunicazione non cooperativi;**

- **sostenere la diffusione di capacità di condivisione sicura delle informazioni tra gli Stati membri, Europol e altre agenzie di sicurezza (dal 2026 al 2028).**

Gli Stati membri sono incoraggiati ad attuare misure di intercettazione legale transfrontaliera, basandosi su meccanismi esistenti quali l'ordine europeo di indagine e gli accordi bilaterali e multilaterali.

III. Recupero di prove dai dispositivi sequestrati nel corso delle indagini: l'informatica forense

Per condurre le indagini penali, le autorità di contrasto e giudiziarie devono essere in grado di accedere alle prove digitali conservate sui dispositivi elettronici, nonché di raccogliere, analizzare e conservare tali prove. Tali prove digitali possono, ad esempio, aiutare a identificare i membri di gruppi della criminalità organizzata o a escludere dalle indagini individui precedentemente sospettati[27].

Il gruppo ad alto livello ha discusso una serie di problemi che impediscono l'accesso a tali prove digitali. Le autorità nazionali risentono di una grave mancanza di risorse e capacità necessarie per condurre operazioni di informatica forense. Faticano a tenere il passo con la necessità di sviluppare costantemente nuove competenze e strumenti per tenere conto delle nuove tecnologie (ad esempio nuovi tipi di dispositivi e sistemi operativi, l'internet delle cose

[27] Un caso discusso nel gruppo ad alto livello riguardava l'analisi di un dispositivo che è risultato determinante nel dimostrare che un sospettato non era coinvolto in un omicidio; *Concluding Report of the High-Level Group*, pag. 12.

e il cloud computing). La cooperazione transfrontaliera tra gli Stati membri è compromessa dalla mancanza di capacità comparabili e dall'assenza di meccanismi per riconoscere le competenze e l'esperienza degli esperti in informatica forense. Le soluzioni commerciali esistenti diventano rapidamente obsolete, hanno prezzi proibitivi e spesso sono sviluppate al di fuori dell'UE. Possono inoltre essere poco adatte alle esigenze delle autorità degli Stati membri o non soddisfare le norme dell'UE in materia di responsabilità nel settore dell'informatica forense o altri requisiti giuridici.

Di conseguenza, per rafforzare la capacità delle autorità di contrasto europee di svolgere attività di informatica forense sui dispositivi sequestrati, il gruppo ad alto livello ha raccomandato di fornire finanziamenti mirati per progetti, sia per la ricerca e lo sviluppo di strumenti di informatica forense sia per la loro adozione. Il gruppo ad alto livello ha accolto con favore gli sforzi in corso della Commissione per sostenere tali progetti attraverso finanziamenti a titolo di determinati strumenti dell'UE (Orizzonte Europa, il programma Europa digitale e il Fondo Sicurezza interna) e dei corrispondenti strumenti nell'ambito del prossimo bilancio a lungo termine dell'UE (quadro finanziario pluriennale).

In risposta a tali raccomandazioni[28], **la Commissione, con il sostegno di Europol, coordinerà un'analisi dei divari e delle esigenze in materia di ricerca, sviluppo, manutenzione dell'implementazione e adozione di soluzioni tecniche comuni per l'informatica forense.**

L'uso delle risorse deve essere massimizzato creando sinergie tra i progetti di informatica forense, integrando anche quelli finanziati nell'ambito dei programmi degli Stati membri nei meccanismi o nelle reti esistenti. Dovrebbero essere fra l'altro finanziati partenariati pubblico-privati per la fornitura di strumenti software pienamente collaudati e pronti all'uso senza costi di licenza[29].

Nell'ambito del mandato dell'OLAF di svolgere indagini amministrative, l'Ufficio ha sviluppato una notevole esperienza nei processi e negli strumenti di informatica forense e può aiutare le autorità degli Stati membri a rafforzare le loro capacità attraverso il programma antifrode dell'Unione.

L'**archivio di strumenti di Europol** è una piattaforma online sicura, accessibile esclusivamente alle autorità di contrasto, per la condivisione di software gratuiti e non commerciali sviluppati da Europol, dalle agenzie di contrasto europee e dal mondo accademico. Le autorità investigative nazionali hanno ampiamente utilizzato gli strumenti dell'archivio per sostenere la lotta contro settori della criminalità organizzata e forme gravi di criminalità, tra cui la tratta di esseri umani, la criminalità informatica e gli abusi sessuali sui minori online. Tale archivio dovrebbe rimanere il canale di distribuzione privilegiato per gli strumenti investigativi digitali sviluppati dai progetti dell'UE e gli Stati membri, che saranno incoraggiati a condividere strumenti di informatica forense open source sviluppati a livello nazionale nell'ambito dei meccanismi o delle reti esistenti. **Europol può sviluppare e promuovere ulteriormente il proprio archivio di strumenti** per mettere a disposizione delle

[28] "Recommendation Cluster 1", *Concluding Report of the High-Level Group*.

[29] Ad esempio, l'associazione europea per lo sviluppo di tecnologie contro la criminalità informatica (EACTDA) (www.eactda.eu) fornisce strumenti software pienamente collaudati e operativamente pronti all'uso senza costi di licenza e accesso al codice sorgente per le agenzie di contrasto dell'UE. Oltre agli otto strumenti messi a punto finora, l'EACTDA sta sviluppando altri 16 strumenti di indagine digitale, da realizzare entro la metà del 2025.

autorità di contrasto dell'UE strumenti investigativi affidabili, sicuri, gratuiti, di facile installazione e scalabili.

La Commissione **sosterrà inoltre l'adozione di soluzioni innovative da parte delle autorità di contrasto degli Stati membri attraverso i meccanismi esistenti, come l'EMPACT[30] e attraverso inviti specifici del Fondo Sicurezza interna**.

Il gruppo ad alto livello ha sottolineato che le **licenze per gli strumenti di informatica forense** sono costose e talvolta insostenibili per alcune autorità di contrasto. Gli strumenti di informatica forense possono fornire dati in formati non compatibili con i sistemi utilizzati per l'ulteriore trattamento. Inoltre la fiducia è fondamentale per le attività di informatica forense, che non dovrebbero basarsi su strumenti a "scatola nera" (ossia strumenti che trattano i dati senza che autorità affidabili siano in grado di verificarne il funzionamento). La condivisione di strumenti di informatica forense dovrebbe essere sostenuta da sistemi di valutazione e, se del caso, dalla certificazione degli strumenti commerciali a livello dell'UE, per garantire che soddisfino le norme in materia di affidabilità e le norme forensi senza imporre oneri indebiti. Il sostegno dovrebbe essere fornito anche attraverso sistemi di appalti comuni, garantendo la cooperazione tra le unità operative e i punti di contatto delle autorità responsabili degli appalti[31].

Pertanto **la Commissione sosterrà le unità operative degli Stati membri e le loro autorità responsabili degli appalti nella realizzazione di acquisti congiunti di licenze per strumenti di informatica forense, iniziando con una fase pilota.**

Azioni fondamentali

La Commissione, con il sostegno di Europol, intende:

- **coordinare un'analisi dei divari e delle esigenze in materia di ricerca, sviluppo, manutenzione dell'implementazione e adozione di soluzioni tecniche comuni per l'informatica forense entro il secondo trimestre del 2026;**

- **continuare a sostenere lo sviluppo di soluzioni tecniche per l'informatica forense attraverso adeguati meccanismi di finanziamento e coordinamento;**

- **sostenere gli Stati membri e le autorità responsabili degli appalti nella realizzazione di acquisti congiunti di licenze per strumenti di informatica forense (entro il secondo trimestre del 2027), iniziando con una fase pilota.**

Europol è invitata a sviluppare e promuovere ulteriormente il proprio archivio di strumenti al fine di consentire alle autorità di contrasto di accedere a strumenti digitali non commerciali (a partire dal terzo trimestre del 2025).

Gli Stati membri sono invitati a partecipare, sostenere e orientare lo sviluppo, la convalida e l'adozione di strumenti di informatica forense.

[30] L'EMPACT (piattaforma multidisciplinare europea di lotta alle minacce della criminalità) è un'iniziativa in materia di sicurezza portata avanti dagli Stati membri dell'UE e tesa a individuare, classificare in ordine di priorità e affrontare le minacce poste dalla criminalità organizzata e dalle forme gravi di criminalità internazionale.

[31] Basandosi sul progetto iProcureNet (www.iprocurenet.eu/), che, finanziato nell'ambito del programma Orizzonte Europa dell'UE per la ricerca e l'innovazione, ha elaborato una metodologia per gli appalti congiunti nel settore della sicurezza, nonché una rete di autorità responsabili degli appalti negli Stati membri.

L'Agenzia dell'UE per la formazione delle autorità di contrasto (CEPOL) impartisce formazione agli investigatori di informatica forense, anche in materia di analisi forense dei dispositivi mobili e dei dati attualizzati. A seguito della raccomandazione[32] del gruppo ad alto livello, la **Commissione dovrebbe continuare a sostenere la creazione di materiali e risorse di formazione** attraverso i meccanismi esistenti che coinvolgono i professionisti del settore e il mondo accademico[33]. CEPOL e gli Stati membri dovrebbero inoltre **dare priorità all'offerta di formazione in materia di informatica forense.**

Il gruppo ad alto livello ha inoltre sottolineato che potrebbe essere creato un sistema di certificazione a livello dell'UE per gli esperti di informatica forense. Tale sistema garantirebbe la qualità del lavoro di informatica forense, contribuirebbe a rendere più trasparenti i procedimenti giudiziari e aumenterebbe la fiducia tra le autorità di contrasto a livello transfrontaliero.

In linea con le raccomandazioni del gruppo ad alto livello[34], CEPOL **potrebbe sostenere i professionisti del settore e il mondo accademico, sfruttando appieno le reti e i meccanismi esistenti[35], nella creazione di un sistema di certificazione a livello dell'UE per gli esperti di informatica forense**.

Azioni fondamentali

La <u>Commissione</u> intende:

- **continuare a sostenere la creazione di materiali e risorse di formazione.**

<u>CEPOL e gli Stati membri</u> sono incoraggiati a:

- **dare priorità all'offerta di formazione in materia di informatica forense (dal terzo trimestre del 2025);**
- **sostenere lo sviluppo e l'attuazione di un sistema di certificazione a livello dell'UE per gli esperti di informatica forense (da preparare tra il primo trimestre del 2026 e il quarto trimestre del 2028).**

Il gruppo ad alto livello ha formulato raccomandazioni sull'agevolazione della condivisione di soluzioni e strumenti di informatica forense tra gli Stati membri in un contesto di fiducia[36]. In risposta, **<u>Europol dovrebbe sviluppare ulteriormente il proprio ruolo di centro di eccellenza delle attività di contrasto dell'UE per le competenze operative digitali nel settore dell'informatica forense</u>**. Ciò potrebbe includere l'istituzione di un progetto simile a SIRIUS[37] per facilitare la condivisione di conoscenze, competenze, soluzioni tecniche, strumenti di informatica forense e migliori pratiche in un contesto di fiducia. Europol dovrebbe

[32] "Recommendation Cluster 3", *Concluding Report of the High-Level Group*.

[33] Ad esempio, il Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG) (www.ecteg.eu) è un'associazione che lavora in stretta collaborazione con Europol e CEPOL con l'obiettivo di fornire risorse di formazione gratuite alle autorità di contrasto nel settore delle indagini digitali. Attualmente è finanziato dal Fondo Sicurezza interna dell'UE.

[34] "Recommendation Cluster 3", *Concluding Report of the High-Level Group*.

[35] In particolare l'ECTEG.

[36] "Recommendation Cluster 1", *Concluding Report of the High-Level Group*.

[37] Il progetto SIRIUS, guidato da Europol ed Eurojust, sostiene le autorità di contrasto e giudiziarie dell'UE agevolando un accesso transfrontaliero efficiente alle prove elettroniche conservate dai prestatori di servizi online. Fornisce strumenti pratici, formazione e risorse a oltre 9 000 professionisti, promuove la cooperazione tra i prestatori di servizi online e promuove la condivisione delle conoscenze attraverso eventi e partenariati internazionali.

inoltre rafforzare il proprio ruolo di coordinamento nella creazione di conoscenze nel campo dell'informatica forense a livello dell'UE, sulla base dei meccanismi creati negli ultimi anni[38]. Europol può avviare alcune di tali azioni nell'ambito del suo attuale mandato. Europol avrà tuttavia bisogno di un mandato rafforzato e di risorse aggiuntive per sviluppare appieno dette azioni e soddisfare efficacemente le esigenze operative degli Stati membri.

Dando seguito all'impegno assunto negli orientamenti politici della Commissione europea per il periodo 2024-2029 e come annunciato nella strategia europea di sicurezza interna, **la Commissione proporrà una revisione ambiziosa del mandato di Europol**. A tal fine, in stretta cooperazione con gli Stati membri, la Commissione vaglierà le modalità per rafforzare le competenze tecnologiche e la capacità di Europol di sostenere le autorità di contrasto nazionali nello spazio digitale. In tale contesto sarà fondamentale rafforzare le capacità di Europol in materia di informatica forense, conferendo all'agenzia un mandato rafforzato e risorse aggiuntive.

Il gruppo ad alto livello ha raccomandato il miglioramento dell'accesso alle conoscenze per gli esperti attraverso meccanismi appositi e la collaborazione degli esperti con i produttori e gli sviluppatori di strumenti di informatica forense[39]. A partire dal 2026 **Europol, utilizzando le proprie risorse, dovrebbe promuovere la cooperazione tra le autorità nazionali competenti e gli esperti per facilitare la cooperazione pubblico-privato in materia di informatica forense**. Dovrebbe sostenere gli Stati membri nello sviluppo di strumenti digitali e procedure comuni, compresa la definizione di formati comuni di dati per finalità di informatica forense[40].

Azioni fondamentali

Europol è invitata a:

- **diventare un centro di eccellenza per le competenze operative in materia di informatica forense e rafforzare il proprio ruolo nel coordinare la creazione di conoscenze in tale settore a livello dell'UE (a partire dal 2026);**

- **agevolare la cooperazione tra le autorità di contrasto e i privati, compresi i prestatori di servizi, in materia di informatica forense e contribuire alla definizione di formati comuni di dati a fini di informatica forense (a partire dal 2026).**

IV. Garantire la lettura delle prove: la decifrazione dei dati

La cifratura e altre misure di cibersicurezza svolgono un ruolo importante nel proteggere i sistemi di informazione dallo spionaggio e dalle perturbazioni e nel garantire la sicurezza delle comunicazioni, della vita privata e dei dati personali. Tra il 60 % e l'80 % delle applicazioni di messaggistica è cifrato da punto a punto, compresi i prestatori tradizionali come WhatsApp,

[38] Comunità dedicate sulla piattaforma Europol per esperti (https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); "Forensic Experts Forum" (https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference); "Europol Industry and Research Days" (https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] "Recommendation Cluster 1", *Concluding Report of the High-Level Group*.

[40] Tali sforzi dovrebbero essere sostenuti da un'adeguata fonte di finanziamento dell'UE (programmi di ricerca o sviluppo, a seconda del livello di maturità dei sistemi previsti).

Messenger, Signal e iMessage, mentre l'uso degli SMS e delle chiamate telefoniche tradizionali è in drastico calo a livello mondiale[41].

Il gruppo ad alto livello ha sottolineato che tali sviluppi incidono sulla capacità delle autorità di contrasto e giudiziarie di raccogliere prove nelle indagini e nelle azioni penali, in quanto la maggior parte delle intercettazioni legali di comunicazioni diventa inutilizzabile. Il gruppo ad alto livello ha sottolineato che gli Stati membri dispongono di competenze e capacità limitate per decifrare i dati a riposo, con notevoli differenze nei tassi di successo, che vanno dal 15-20 % in alcuni Stati membri a oltre il 66 % in altri.

Le apparecchiature di decrittazione sono costose e altamente specializzate e l'hardware consuma molte risorse. La maggior parte dei dipartimenti di informatica forense delle autorità di contrasto si basa su soluzioni commerciali per accedere ai dati sui dispositivi. Tali soluzioni faticano a tenere il passo con gli sviluppi tecnologici e diventano rapidamente obsolete; il costo elevato delle licenze riduce notevolmente il numero di utenti autorizzati; le soluzioni sono spesso sviluppate al di fuori dell'UE e potrebbero pertanto non soddisfare le esigenze delle autorità dell'UE o le norme in materia di informatica forense. Di conseguenza, solo in un numero molto limitato di indagini si riesce a usarle.

Il ricorso a tali strumenti presenta inoltre altri svantaggi. Nel corso delle indagini le autorità sfruttano spesso le vulnerabilità per ottenere l'accesso alle chiavi di decrittazione sui dispositivi, il che potrebbe in alcuni casi creare tensioni con l'obiettivo strategico di garantire la cibersicurezza per impostazione predefinita. Inoltre l'accesso ai dati criptati sta diventando sempre più complesso. Il gruppo ad alto livello ha osservato che le autorità non possono accedere ai dati conservati su determinati tipi di dispositivi moderni, protetti da chip crittografici o algoritmi di cifratura robusti e password complesse, anche utilizzando le piattaforme di decrittazione più potenti.

È necessario sviluppare e introdurre una **crittografia a prova di computer quantistici** per proteggere i dati da futuri attacchi informatici quantistici che renderebbero le comunicazioni sensibili, le transazioni finanziarie e i segreti di Stato vulnerabili alla decrittazione e allo sfruttamento. Come indicato nella raccomandazione della Commissione relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la **crittografia post-quantistica**[42] e nella strategia europea di sicurezza interna (ProtectEU), l'impiego di soluzioni di crittografia post-quantistica e lo sviluppo di una distribuzione quantistica delle chiavi saranno fondamentali per salvaguardare i dati nella nuova era quantistica. Tuttavia, come sottolineato da Europol, ciò renderà più difficile nei prossimi anni l'accesso legittimo alle prove digitali e le agenzie di contrasto devono investire per tenere il passo con il rapido sviluppo tecnologico[43].

Il gruppo ad alto livello[44] ha raccomandato di elaborare una tabella di marcia tecnologica per attuare, se del caso, un accesso legittimo mirato fin dalla progettazione, garantendo nel contempo una forte sicurezza e cibersicurezza e rispettando appieno gli obblighi giuridici in materia di accesso legittimo. In risposta, **la Commissione sta incaricando un gruppo di esperti di fornire sostegno nella preparazione di una tabella di marcia tecnologica sulla**

[41] La percentuale cui si fa riferimento riguarda la cifratura da punto a punto durante la trasmissione.
[42] Raccomandazione relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica.
[43] "The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement" | Europol.
[44] "Recommendation Cluster 10", *Concluding Report of the High-Level Group*.

cifratura. Il gruppo individuerà e valuterà soluzioni tecnologiche che permettano alle autorità di contrasto di accedere legalmente ai dati cifrati, salvaguardando nel contempo la cibersicurezza e i diritti fondamentali. Il gruppo comprenderà esperti in materia di contrasto, cibersicurezza, cifratura, tecnologie della comunicazione, normazione e diritti fondamentali. Gli studi tecnologici e la dimostrazione di concetti sosterranno tale lavoro. Lo scopo di detto lavoro consiste nell'individuare:

- **strumenti di cui le autorità di contrasto hanno attualmente bisogno e avranno bisogno in futuro** per trovare, recuperare e analizzare legalmente i dati cifrati; tali strumenti devono facilitare l'informatica forense, la decrittazione, la raccolta di dati a distanza e le attività di analisi dei reati;
- **tecnologie che garantiscano che le future tecnologie dell'informazione e della comunicazione**, come la sesta generazione di reti cellulari (6G) e la crittografia post-quantistica, non pregiudichino la capacità delle autorità di contrasto di accedere legalmente ai dati, garantendo nel contempo il rispetto dei diritti fondamentali e la cibersicurezza.

Laddove attualmente non esistono strumenti, la tabella di marcia tecnologica dovrebbe fornire raccomandazioni sul loro sviluppo e su come garantirne sia la compatibilità con il quadro giuridico dell'UE sia la cibersicurezza. I risultati della tabella di marcia tecnologica possono inoltre orientare azioni specifiche al fine di promuovere un approccio coordinato alla normazione.

La piattaforma di decrittografia di Europol si è dimostrata determinante nel sostenere casi penali di rilievo, compresi quelli provenienti da Sky ECC[45] ed EncroChat. Sono necessarie capacità di decrittazione rafforzate, guidate anche da ulteriori investimenti nell'intelligenza artificiale (IA) e nel calcolo ad alte prestazioni per garantire che le autorità di contrasto abbiano la capacità di decifrare algoritmi sempre più complessi.

Il gruppo ad alto livello ha raccomandato[46] di aumentare i finanziamenti per sostenere l'innovazione in materia di accesso ai dati. In risposta, **la Commissione sosterrà la ricerca e lo sviluppo di nuove capacità di decrittazione** per garantire che Europol disponga degli strumenti necessari dopo il 2030 per sostenere gli Stati membri, alla luce dei nuovi sviluppi tecnologici e della ricerca più avanzata nel settore. Tale iniziativa potrebbe comportare un aumento dei finanziamenti a sostegno della ricerca sulla decrittazione, nonché lo sviluppo e l'attuazione di strumenti da parte degli Stati membri. Gli Stati membri saranno strettamente coinvolti per condividere le proprie esigenze specifiche, al fine di migliorare le rispettive capacità, competenze e risorse tecniche, basandosi sulle tecnologie progettate a livello dell'UE ed eventualmente valutando la possibilità di appalti congiunti.

Azioni fondamentali

La Commissione intende:

- **elaborare una tabella di marcia tecnologica in materia di cifratura (nel secondo trimestre del 2026);**

[45] "New major interventions to block encrypted communications of criminal networks" | Europol.
[46] "Recommendation Cluster 10", *Concluding Report of the High-Level Group*.

- **sostenere la ricerca e lo sviluppo di nuove capacità di decrittazione per dotare Europol di capacità di decrittazione di prossima generazione (dal 2030).**

V. Conciliazione di tecnologia e accesso legittimo: normazione

Le norme sono essenziali nelle comunicazioni digitali. Sviluppate da una vasta serie di attori, principalmente dall'industria, esse garantiscono l'interoperabilità tra sistemi e dispositivi sviluppati da fornitori di tecnologie e favoriscono il rispetto degli obblighi giuridici da parte delle tecnologie, anche per quanto riguarda l'accesso legittimo a fini di contrasto. L'Istituto europeo per le norme di telecomunicazione (ETSI) ha elaborato diverse norme in materia di intercettazione legale e di divulgazione lecita. Esistono tuttavia lacune, ad esempio con la quinta generazione di reti cellulari (5G): la mancanza di un'adeguata considerazione dell'accesso legittimo nel suo sviluppo ha ostacolato la capacità delle autorità di contrasto e giudiziarie di accedere alle prove necessarie per identificare e perseguire i criminali[47].

Il gruppo ad alto livello ha raccomandato di adottare un approccio prudente nella progettazione di soluzioni per l'accesso legittimo ai sistemi, in base al quale l'industria non dovrebbe essere invitata a integrare sistemi che potrebbero indebolire la cifratura in modo generalizzato o sistemico per tutti gli utenti di un servizio. L'accesso legittimo ai dati deve rimanere mirato e limitato a comunicazioni specifiche caso per caso.

Come regola generale, qualsiasi soluzione dovrebbe essere attuata sulla base di norme chiare elaborate con il contributo di tutti i portatori di interessi, compresi i rappresentanti del settore, gli esperti in materia di protezione dei dati, vita privata e cibersicurezza e i professionisti preposti all'azione di contrasto. Come sottolineato dal gruppo ad alto livello, è tuttavia necessaria cautela per quanto riguarda la cifratura. Sulla base delle soluzioni individuate nella tabella di marcia tecnologica, saranno previste misure specifiche per promuovere un approccio coordinato alla normazione.

Qualsiasi normazione dovrebbe riflettere i requisiti giuridici applicabili ed essere basata su soluzioni valutate. Deve garantire che l'accesso legittimo non sia in conflitto con le norme applicabili in materia di cibersicurezza, come quelle elaborate ai sensi del regolamento sulla ciberresilienza, o con le norme a sostegno dell'attuazione della direttiva NIS 2, né comprometta in altro modo la sicurezza di prodotti e servizi.

Per quanto riguarda le raccomandazioni del gruppo ad alto livello[48], **la Commissione svilupperà e razionalizzerà un approccio dell'UE in materia di normazione per la sicurezza interna, con particolare attenzione all'informatica forense, alla divulgazione lecita e all'intercettazione legale.** L'approccio si baserà su un'analisi continua del panorama condotta dai professionisti preposti all'azione di contrasto, in particolare attraverso il gruppo di lavoro europeo sulla normazione in materia di sicurezza interna guidato da Europol. Tale azione aumenterà inoltre le risorse e la portata del gruppo di lavoro e comporterà un'ulteriore collaborazione con altre iniziative in materia di normazione, in particolare per quanto riguarda l'IA e l'informatica forense. L'obiettivo è garantire che la normazione tenga conto delle questioni attinenti alla sicurezza. L'iniziativa comprenderà inoltre lo sviluppo e l'organizzazione di corsi di formazione sulla normazione nel settore della sicurezza e l'erogazione di sostegno finanziario, attraverso il Fondo Sicurezza interna, agli esperti che

[47] Cfr. *First report on Encryption from the EU Innovation Hub on Internal Security*, 11 giugno 2024.
[48] "Recommendation Cluster 10", *Concluding Report of the High-Level Group*.

partecipano ai pertinenti forum di normazione. Integrerà altresì i meccanismi di governance pertinenti.

Azioni fondamentali

- **La <u>Commissione</u>, in stretta collaborazione con Europol, svilupperà e razionalizzerà le attività di normazione per l'accesso legittimo, con il sostegno di meccanismi di governance adeguati (dal secondo trimestre del 2025 al secondo trimestre del 2027).**

- **Gli <u>Stati membri</u> sono incoraggiati a destinare risorse sufficienti per garantire che gli operatori del settore della sicurezza partecipino ai pertinenti forum di normazione sull'accesso legittimo.**

VI. <u>Analisi delle prove in modo efficace e legittimo: l'IA</u>

Europol ed Eurojust hanno recentemente osservato che un numero crescente di indagini contiene ingenti quantità di dati[49]. In un caso standard di abuso sessuale su minori, le indagini richiedono spesso l'analisi di 1-3 terabyte di dati, che possono includere da 1 a 10 milioni di immagini e migliaia di ore di filmati[50]. Nel 2023 sono stati scambiati 1 553 822 file di grandi dimensioni tramite il server di scambio di file di grandi dimensioni di Europol[51]. Nel caso EncroChat sono stati intercettati oltre 115 milioni di conversazioni tra persone sospettate di partecipazione a gruppi di criminalità organizzata. Nei mesi successivi, attraverso tecniche e mezzi analitici avanzati, come l'apprendimento automatico, Europol e le agenzie di contrasto sono stati in grado di individuare modelli, connessioni e "zone calde", portando all'arresto di 6 558 sospettati. Le autorità neerlandesi e francesi hanno condiviso tali informazioni con i loro omologhi negli Stati membri dell'UE e nei paesi terzi, il che ha permesso di sventare più di 200 complotti di omicidio solo nel Regno Unito[52].

Il continuo aumento dei dati trattati nel corso delle indagini rende difficile conservare, gestire e analizzare in modo efficace i dati senza disporre di competenze significative, risorse computazionali e strumenti specializzati. Europol ed Eurojust hanno confermato che il volume dei dati può essere eccessivo per gli investigatori e comportare tempi di trattamento più elevati e problemi di capacità di conservazione. Gli Stati membri spesso non dispongono dei meccanismi e delle infrastrutture necessari per gestire il trasferimento di grandi quantità di dati ad altri Stati membri e a Europol.

L'uso dell'IA è pertanto essenziale affinché le autorità di contrasto possano prevenire e individuare i reati e indagare su di essi, e di conseguenza proteggere le nostre società nell'era digitale. Le soluzioni basate sull'IA possono permettere di eseguire compiti semplici, come la traduzione automatica o la conversione dal parlato allo scritto, o compiti più complessi, come il filtraggio dei dati, la correlazione tra prove da ingenti quantità di dati o la lotta contro l'uso malevolo dell'IA. Gli strumenti delle autorità di contrasto basati sull'IA devono essere accurati,

[49] *Common Challenges in Cybercrime - 2024 Review by Europol and Eurojust.*
[50] IOCTA di Europol.
[51] Relazione annuale di attività consolidata di Europol per il 2023.
[52] "Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée"; "Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized" | Europol. EncroChat.

trasparenti e pienamente conformi al quadro giuridico dell'UE in materia di IA, protezione dei dati e tutela della vita privata, al fine di garantire indagini affidabili ed etiche basate sui dati. L'IA e il calcolo ad alte prestazioni sono di fondamentale importanza per ottenere l'accesso ai dati cifrati e sostenere le indagini e l'analisi forense.

A seguito delle raccomandazioni del gruppo ad alto livello volte ad aumentare i finanziamenti per la ricerca e lo sviluppo di strumenti per l'analisi dei dati basati sull'IA e a definire risultati chiari[53], **la Commissione promuoverà lo sviluppo e l'adozione di soluzioni di IA.** Saranno necessari investimenti mirati nello sviluppo di capacità fondamentali, quali soluzioni per individuare indizi investigativi da ingenti quantità di dati, nel pieno rispetto dei principi in materia di protezione dei dati e della vita privata, o miglioramenti nel tracciamento delle transazioni in criptovalute. Potrebbe inoltre essere possibile sfruttare le opportunità di formazione, prova e valutazione degli strumenti di IA in uno spazio di sperimentazione normativa per l'IA, come previsto dalla legge sull'IA[54], con il sostegno e l'orientamento delle autorità di controllo competenti. Le fabbriche di IA e le future gigafabbriche potrebbero sostenere lo sviluppo di strumenti e servizi basati sull'IA per le attività di contrasto. La Commissione dovrebbe agevolare tali sforzi, sulla base di un'analisi delle esigenze svolta con i portatori di interessi, compresi il laboratorio per l'innovazione di Europol e il polo di innovazione per la sicurezza interna delle agenzie dell'UE competenti in materia di giustizia e affari interni.

Gli Stati membri possono avere accesso a capacità pertinenti a costi ridotti o nulli, garantendo la compatibilità con i requisiti della legge sull'IA. È fondamentale un approccio globale all'IA che comprenda la creazione di formati di dati standardizzati per qualsiasi scambio e l'elaborazione di orientamenti sull'uso di tali sistemi in linea con la legge sull'IA e le normative dell'UE applicabili in materia di protezione dei dati. Tale azione potrebbe essere sostenuta da finanziamenti del Fondo Sicurezza interna, del programma Europa digitale e di Orizzonte Europa. Sarà necessario fornire sostegno a Europol e alla comunità EMPACT al fine di garantire un'adeguata corrispondenza con le esigenze operative e promuovere l'adozione e l'integrazione da parte dei professionisti del settore.

Azioni fondamentali

La Commissione intende:

- **promuovere la creazione e l'adozione di nuove soluzioni di IA e migliorare quelle esistenti per filtrare e analizzare le prove digitali, anche attraverso il pieno utilizzo degli spazi di sperimentazione normativa per l'IA per lo sviluppo, le prove e la valutazione, in linea con la legge sull'IA (dal 2025 al 2028);**

- **avviare un dialogo con le autorità di contrasto e altri portatori di interessi per individuarne le esigenze, sulla base del lavoro del laboratorio per l'innovazione di Europol e del polo delle agenzie dell'UE competenti in materia di giustizia e affari interni;**

- **sostenere la creazione di orientamenti chiari per l'uso dell'IA nelle attività di contrasto;**

[53] Raccomandazione 4, *High Level Group Recommendations*.
[54] Cfr. articolo 57 della legge sull'IA.

- **sostenere progetti pilota volti a sviluppare e formare soluzioni di IA giuridicamente e tecnicamente valide per l'informatica forense, l'analisi dei dati e altri strumenti investigativi a uso delle autorità di contrasto.**