

dossier

25 febbraio 2022

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

10^a riunione del Gruppo di controllo
parlamentare congiunto delle attività di
Europol

Videoconferenza, Parigi, 28 febbraio



Senato
della Repubblica



Camera
dei deputati

X
V
I
I
I
L
E
G
I
S
L
A
T
U
R
A



XVIII LEGISLATURA

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

10^a riunione del Gruppo di controllo parlamentare
congiunto delle attività di Europol

Videoconferenza, Parigi, 28 febbraio 2022

SENATO DELLA REPUBBLICA

SERVIZIO STUDI
DOSSIER EUROPEI

N. 157


CAMERA DEI DEPUTATI

UFFICIO RAPPORTI CON
L'UNIONE EUROPEA

N. 83



Servizio Studi

TEL. 06 6706-2451 - studi1@senato.it -  @SR_Studi

Dossier europei n. 157



Ufficio rapporti con l'Unione europea

Tel. 06-6760-2145 - cdrue@camera.it

Dossier n. 83

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.

INDICE

ORDINE DEL GIORNO

| | |
|------------------------------------|----------|
| IL PROGRAMMA DELLA RIUNIONE | 1 |
|------------------------------------|----------|

| | |
|--|----------|
| LA RIFORMA DEL MANDATO DI EUROPOL | 3 |
|--|----------|

| | |
|--|---|
| La riforma del regolamento di procedura del Gruppo di controllo parlamentare congiunto delle attività di Europol (JPSG) | 8 |
|--|---|

| | |
|--|-----------|
| IL CONTRIBUTO DI EUROPOL ALLE ATTIVITÀ DI CONTRASTO DEI TRAFFICANTI DI MIGRANTI | 11 |
|--|-----------|

| | |
|----------------|----|
| Il Centro EMSC | 13 |
|----------------|----|

| | |
|--------------------------------------|----|
| Dati statistici sui flussi migratori | 15 |
|--------------------------------------|----|

| | |
|---|-----------|
| RISCHI E OPPORTUNITÀ DELL'INTELLIGENZA ARTIFICIALE PER EUROPOL | 19 |
|---|-----------|

| | |
|----------------------------|----|
| La dimensione del fenomeno | 21 |
|----------------------------|----|

| | |
|--|----|
| L'Innovation Lab di Europol e il Polo dell'innovazione dell'UE per la sicurezza interna | 22 |
|--|----|

| | |
|--|----|
| La proposta di regolamento recante norme in materia di intelligenza artificiale | 23 |
|--|----|

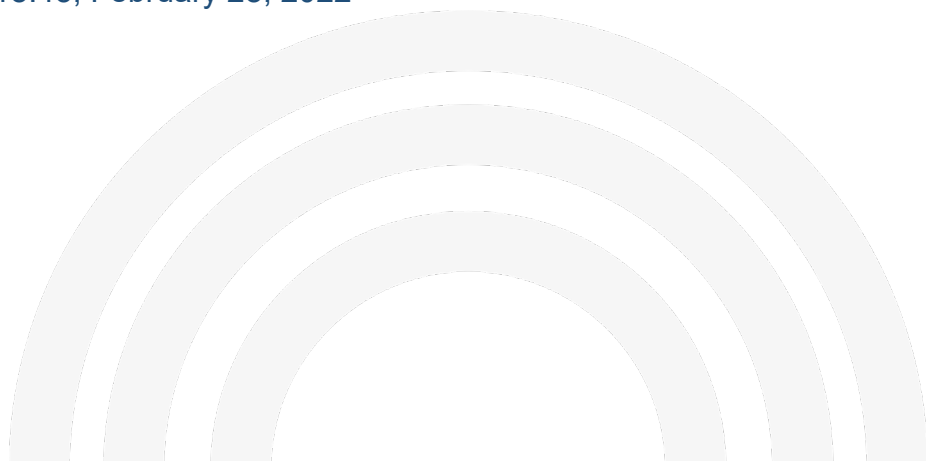


Draft Agenda

10th meeting of the Joint Parliamentary Scrutiny Group (JPSG) on the European Union Agency for Law Enforcement Cooperation (Europol)

Format: Remote, hosted at the *Assemblée nationale* of France in Paris

9:30 - 18:45, February 28, 2022



Monday February 28

- 9.30 - 10.15 **Meeting of the Presidential Troika (in camera)**
- 10:15 - 10:30 **Coffee break**
- 10:30 – 10:45 **Adoption of the agenda and introductory remarks**
- Ms. Yaël BRAUN-PIVET, JPSG Co-Chair and Head of the National Assembly of the French Republic delegation to the JPSG
 - Mr. François-Noël BUFFET, JPSG Co-Chair and Head of the Senate of the French Republic delegation to the JPSG
 - Mr. Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the European Parliament Delegation to the JPSG
 - Communications from the Chairs, summary of conclusions from the Troika meeting
- 10:45 - 12:30 **Europol activity from October 2021 to February 2022 and presentation of the state of negotiations on the proposed revision of the Europol Regulation**
- Presentation by Ms Catherine DE BOLLE, Executive Director of Europol
 - Report by Mr Wojciech WIEWIÓROWSKI, European Data Protection Supervisor
 - Report by Mr. Jérôme BONET, Chairman of the Europol Management Board
 - Written contribution from Professor François PELLEGRINI, Chairman of the Europol Cooperation Board
 - Exchange of views
- 12:30 - 14:00 **Lunch Break**

14:00 - 15:30

Thematic debate: Europol's contribution in the fight against migrant smugglers

- Jean Philippe Lecouffe
Deputy Executive Director of Europol, Operations Directorate
- Johannes Luchner
Deputy Director General, DG HOME, European Commission
- Silke Albert
Crime Prevention Expert, Human Trafficking and Migrant Smuggling Section (HTMSS), Organized Crime and Illicit Trafficking Branch (OCB), Division for Treaty Affairs (DTA), United Nations Office on Drugs and Crime
- Followed by an exchange of views

15:30 - 16:45

Keynote Interventions

- Ms Ylva JOHANSSON, Commissioner for Home Affairs
- Mr. Gérald DARMANIN, Minister of the Interior of the French Republic
- Followed by an exchange of views

16:45 - 17:00

Coffee break

17:00 - 18:30

Thematic debate: Risks and opportunities of artificial intelligence for Europol

- Jürgen Ebner
Deputy Executive Director of Europol, Governance Directorate
- Olivier Onidi
Deputy Director General, DG HOME, European Commission
- Nathalie Smuha,
Lawyer and Researcher, Law and Ethics of AI/Technology Faculty of Law, KU Leuven
- Followed by an exchange of views

18:30 - 18:45

Closing remarks by the JPSG Co-Chairs

- Ms. Yaël BRAUN-PIVET, JPSG Co-Chair and Head of the National Assembly of the French Republic delegation to the JPSG
- Mr. François-Noël BUFFET, JPSG Co-Chair and Head of the Senate of the French Republic delegation to the JPSG
- Mr. Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the European Parliament Delegation to the JPSG

Next meeting: Autumn 2022, European Parliament, Brussels

IL PROGRAMMA DELLA RIUNIONE

Il 28 febbraio 2022 si svolgerà a Parigi (nel formato da remoto) la Decima Riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol (JPSG). L'evento segue la Nona Riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol, che si è svolta a Bruxelles il 25 - 26 ottobre 2021, mentre, ai sensi dell'articolo 3.4 del regolamento di procedura del Gruppo, la prossima riunione dovrebbe tenersi nel corso della seconda metà dell'anno (in data non ancora definita) presso la sede del Parlamento europeo di Bruxelles.

In base alla bozza di programma, i lavori della Decima Riunione del JPSG saranno preceduti dall'incontro ristretto della Troika presidenziale (Slovenia, Francia e Repubblica Ceca), cui l'Italia non partecipa.

Le attività inizieranno con l'adozione dell'agenda e i saluti di apertura dei co-Presidenti: Yael Braun Pivet, capo della delegazione al JPSG della Assemblea nazionale della Repubblica francese; Francois - Noel Buffet, capo della delegazione al JPSG del Senato della repubblica francese; Juan Fernando López Aguilar, Presidente della Commissione per le libertà civili, giustizia e affari interni (LIBE) del Parlamento europeo.

Successivamente, l'ordine del giorno prevede l'esame delle attività di Europol nel periodo fra ottobre 2021 e febbraio 2022, e la presentazione dello stato dei negoziati relativi alla proposta di riforma del regolamento recante il quadro giuridico di Europol.

La sessione prevede, tra l'altro, l'illustrazione delle attività di Europol da parte della direttrice esecutiva dell'Agenzia, Catherine De Bolle, e la relazione del Garante europeo per la protezione dei dati, Wojciech Wiewioroski.

L'ordine del giorno della riunione include, inoltre:

- un primo dibattito tematico sul contributo di Europol alle attività di contrasto alle reti del traffico dei migranti;*
- gli interventi della Commissaria europea agli affari interni, Ylva Johanson, e del Ministro dell'interno della Repubblica francese Gerald Darmanin;*
- un secondo dibattito tematico sui rischi e le opportunità dell'intelligenza artificiale per Europol.*

In esito a ciascuna sessione è previsto lo svolgimento da parte del Gruppo di uno scambio di punti di vista. I lavori del Gruppo si concluderanno con i commenti finali dei co-Presidenti.

Alla Riunione parteciperanno per il Senato e per la Camera dei deputati italiani, rispettivamente, il senatore Vincenzo Garruti e l'onorevole Valentina Corneli.

LA RIFORMA DEL MANDATO DI EUROPOL

Presentata dalla Commissione europea il 9 dicembre 2020, nell'ambito di un pacchetto di misure **antiterrorismo**, la [proposta di regolamento](#) volta a rafforzare il **mandato** dell'Agenzia **Europol** è tuttora in corso di approvazione da parte delle Istituzioni legislative dell'UE.

In particolare, in esito ai negoziati interistituzionali, il 20 febbraio 2022 Parlamento europeo e Consiglio dell'UE hanno raggiunto un **accordo** politico in vista dell'adozione di un testo condiviso del regolamento.

Secondo i termini dell'accordo, il nuovo quadro giuridico di Europol ne rafforza il mandato con riferimento ai seguenti profili:

- capacità di cooperazione con **parti private**, nel rispetto delle norme sulla tutela dei dati; in tale contesto, è consentita a Europol la ricezione di **dati** da parte di **soggetti privati**;
- disposizioni relative all'**analisi** dei **big data** da parte di Europol a supporto delle indagini penali, nel rispetto dei diritti fondamentali; il nuovo mandato fornisce chiarezza giuridica sulla pre-analisi dei big data da parte di Europol, tenendo conto anche delle indicazioni del **Garante europeo della protezione dei dati**. Europol ha a disposizione diciotto mesi per pre-analizzare i big data ricevuti dagli Stati membri e assegnargli una categoria, con una possibile proroga per un altro periodo di pari durata;
- l'attribuzione all'Agenzia di un ruolo di supporto per quanto riguarda la trasmissione di **allarmi informativi** sui **combattenti terroristi stranieri**; in forza di tale disposizione viene conferita ad Europol la facoltà di proporre agli Stati membri di inserire nel sistema d'informazione Schengen le informazioni ricevute da paesi terzi su sospetti e criminali, in particolare combattenti stranieri;
- poteri di **cooperazione** rafforzata con i **Paesi terzi**;
- rafforzamento della cooperazione con la **Procura europea**; è previsto che la Procura europea abbia accesso indiretto ai dati Europol in relazione ai reati nell'ambito del suo mandato, in linea con le garanzie applicabili;
- misure per consolidare il ruolo di Europol nella ricerca e nell'innovazione, per identificare le esigenze tecnologiche e gli strumenti informatici per contrastare la criminalità grave e il terrorismo;

- miglioramento del quadro giuridico in materia di **tutela dei dati personali**;
- rafforzamento del ruolo del Gruppo di controllo parlamentare congiunto (incaricato di monitorare le attività dell'agenzia), con il supporto da parte un **Forum consultivo**.

In particolare, il Parlamento europeo ha proposto di inserire una disposizione che prevede che Europol istituisca un **forum consultivo** che la assista nelle questioni legate ai diritti fondamentali fornendole, su richiesta, una consulenza indipendente. Secondo la proposta il direttore esecutivo e il consiglio di amministrazione, in coordinamento con il responsabile dei diritti fondamentali, possono consultare il forum consultivo in merito a qualsiasi questione connessa ai diritti fondamentali. Europol invita **esperti indipendenti, l'Agenzia dell'Unione europea per i diritti fondamentali** e altre **organizzazioni competenti** nel settore dei diritti fondamentali a partecipare al forum consultivo. Sulla base di una proposta del responsabile dei diritti fondamentali, presentata previa consultazione del direttore esecutivo, il consiglio di amministrazione decide in merito alla **composizione** del forum consultivo, ai suoi metodi di lavoro e alle modalità di **comunicazione** delle informazioni al forum consultivo.

La discussione in sede di Assemblea plenaria del Parlamento europeo sul testo di compromesso che rispecchia gli elementi dell'accordo politico testè illustrato dovrebbe svolgersi durante la sessione di maggio 2022.

Si ricorda che la proposta è collegata a un'altra [proposta normativa](#) (tuttora in corso di iter legislativo), che modifica il regolamento (UE) 2018/1862 sul Sistema di informazione Schengen, nel senso di conferire ad Europol il potere di inserire nel **Sistema d'informazione Schengen** (consentendo la condivisione dell'informazione con agenti in prima linea) dei dati su un sospetto coinvolgimento di un **cittadino** di un **paese terzo** in un **reato** di competenza dell'Agenzia. Le autorità dedite al contrasto del crimine degli Stati membri utilizzano il sistema d'informazione Schengen (SIS) per inserire o consultare segnalazioni relative a persone e oggetti ricercati o scomparsi. Il SIS fornisce istruzioni alle autorità sulle linee da seguire in caso di ritrovamento di persone o di oggetti, ad esempio: arresto di **persone ricercate**; protezione di persone vulnerabili **scomparse**; sequestro di oggetti **illeghi** o **rubati**.

Si ricorda che ai sensi dell'allegato I del quadro giuridico di Europol la competenza dell'Agenzia abbraccia le seguenti forme di criminalità: **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** e 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** ed 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**.

Come nelle precedenti riunioni del Gruppo, l'ordine del giorno prevede, tra l'altro, che in tale sessione intervenga il Garante europeo per la protezione dei dati (GEPD); il Garante nelle precedenti occasioni ha normalmente illustrato il quadro sul suo monitoraggio circa le attività di Europol concernenti il trattamento di dati personali.

In tale contesto, si ricorda che il 3 gennaio 2022 il Garante europeo per la protezione dei dati (GEPD), ha notificato a Europol un'[ordinanza](#) di **cancellazione** dei dati relativi a persone senza alcun legame accertato con un'attività criminale (categorizzazione degli interessati). La decisione conclude l'indagine del GEPD avviata nel 2019.

Nell'ambito delle sue indagini, nel settembre 2020 il GEPD ha chiesto a Europol di non continuare a **conservare** ingenti volumi di dati **senza categorizzare** gli interessati, pratica che rappresenta un rischio per i diritti fondamentali delle persone. Secondo il Garante, pur avendo adottato alcune misure, Europol non avrebbe soddisfatto la richiesta di definire un periodo di conservazione dei dati appropriato per filtrare ed estrarre i dati personali consentiti. Ciò significa che Europol avrebbe conservato questi dati più a lungo del necessario, contrariamente ai principi di minimizzazione dei dati e di limitazione della conservazione, sanciti dal regolamento Europol.

Il GEPD ha pertanto deciso di avvalersi dei propri poteri correttivi e di imporre un periodo di conservazione di 6 mesi (per filtrare ed estrarre i dati personali). In forza della decisione, i set di dati più vecchi di 6 mesi che non sono stati sottoposti a questa categorizzazione degli interessati devono essere **cancellati**. Il GEPD ha

concesso a Europol un periodo di **12 mesi** per conformarsi alla decisione per i set di dati già ricevuti prima che tale decisione fosse notificata a Europol.

La riforma del regolamento di procedura del Gruppo di controllo parlamentare congiunto delle attività di Europol (JPSG)

Nel corso della riunione svoltasi a Bruxelles il 25-26 ottobre 2021 il Gruppo ha adottato talune **modifiche** al proprio **regolamento di procedura**.

Tale regolamento (articolo 6.2) prevedeva che, in linea con le raccomandazioni della Conferenza dei Presidenti dei Parlamenti UE riuniti a Bratislava il 23-24 aprile 2017, il JPSG avrebbe rivisto alcune delle sue regole di procedura due anni dopo la prima riunione costitutiva e presentato le conclusioni di tale riesame alla Presidenza della Conferenza dei Presidenti dei Parlamenti dell'Unione Europea.

Il 28 settembre 2020, la Troika presidenziale del Gruppo interparlamentare di controllo delle attività di Europol ha adottato un **mandato** per il gruppo di lavoro sulle proposte di modifica di alcune regole di procedura del funzionamento del JPSG. Si tratta, in particolare, delle disposizioni rispettivamente concernenti:

1. la **nomina** del rappresentante del JPSG presso il consiglio di amministrazione di Europol (articolo 5 del regolamento di procedura del JPSG);
2. la **clausola di revisione** del regolamento interno del JPSG (articolo 6.2).

Al gruppo di lavoro hanno partecipato, oltre alla **Troika presidenziale**, le seguenti delegazioni (ciascuna delle quali rappresentata da un solo membro): Parlamento europeo; Bundestag; Parlamento portoghese; Parlamento croato; Camera dei deputati del Lussemburgo; Camera dei deputati italiana; Camera dei rappresentanti della Repubblica di Cipro; Parlamento rumeno; Parlamento greco; Assemblea nazionale di Francia; Sejm polacco; Parlamento svedese; Camera dei rappresentanti del Belgio; Assemblea nazionale di Slovenia; Eerste Kamer (Camera Alta dei Paesi bassi). **L'onorevole Valentina Corneli ha partecipato in rappresentanza della Camera dei deputati.** La riunione costitutiva del gruppo di lavoro si è svolta il 10 dicembre 2020. La prima discussione sulle proposte del gruppo di lavoro si è tenuta a livello tecnico il **21 gennaio 2021**. Il gruppo ha concluso i lavori con l'adozione di due proposte di compromesso il 25 maggio 2021.

In esito al lavoro del *working group*, l'allora **Copresidenza del JPSG (Isabel Oneto**, capo della delegazione dell'Assemblea della Repubblica portoghese, e **Fernando López Aguilar**, Presidente della Commissione LIBE del Parlamento europeo e capo della delegazione del Parlamento europeo al JPSG) ha presentato sulle questioni testé illustrate **emendamenti di compromesso**, successivamente

adottati dalle delegazioni dei Parlamenti nazionali partecipanti alla riunione del *working group* del 25 maggio 2021.

Gli emendamenti sono stati quindi discussi e **approvati** per consenso nel corso della riunione del JPSG del 25-26 ottobre 2021.

*Di seguito la nuova formulazione degli **articoli 5 e 6.2** del regolamento di procedura del Gruppo.*

Articolo 5:

Rappresentanti presso il consiglio di amministrazione di Europol

Il JPSG deve avere due membri quali rappresentanti aventi diritto a partecipare, ai sensi dell'articolo 14 del regolamento di Europol e per il tempo stabilito dal JPSG, alle riunioni del consiglio di amministrazione di Europol come osservatori non votanti.

Uno dei membri deve essere delegato dal Parlamento europeo e l'altro membro dalla delegazione al JPSG del Parlamento dello Stato membro che detiene la Presidenza di turno del Consiglio dell'UE. Solo uno di questi prende la parola al consiglio di amministrazione a nome del JPSG. Prima di ciascuna riunione cui sono invitati, i due rappresentanti si accordano su quale dei due sia designato per parlare al consiglio di amministrazione. I rappresentanti riferiscono per iscritto al JPSG dopo ogni riunione del consiglio di amministrazione sui loro principali risultati.

Articolo 6.2

Le delegazioni al JPSG possono presentare proposte per la revisione delle Regole di procedura. Tali proposte e la dichiarazione delle motivazioni sono sottoposte per iscritto alla copresidenza del JPSG e alla Troika, e inoltrate a tutte le delegazioni del JPSG, almeno quattro mesi prima di una riunione del JPSG. La Troika decide se inserire le proposte di revisione delle Regole di procedura nell'agenda della prima o della seconda riunione del JPSG a seguito della presentazione. Ogni emendamento è sottoposto a una decisione per consensus del JPSG.

Si ricorda che il 14 e 15 dicembre 2021 si è svolta la 123a riunione del **consiglio di amministrazione** di Europol, alla quale hanno partecipato come **osservatori** i Copresidenti del JPSG **Juan Fernando López Aguilar** (Presidente della Commissione libertà giustizia e affari interni - LIBE) e **Nik Prebil**, Capo della delegazione dell'Assemblea nazionale al JPSG della Slovenia, invitati al fine di assistere a taluni punti all'ordine del giorno.

In tale occasione il consiglio di amministrazione ha, tra l'altro:

- adottato il documento di programmazione 2022-2024 e il bilancio definitivo 2022 di Europol;
- aggiornato l'elenco annuale delle partner prioritari di Europol nel settore delle relazioni esterne;
- approvato il programma di lavoro sulla capacità di audit interno per il 2022.

**IL CONTRIBUTO DI EUROPOL ALLE ATTIVITÀ DI CONTRASTO
DEI TRAFFICANTI DI MIGRANTI**

Secondo i dati in possesso del Consiglio dell'UE, la dimensione della crescita del fenomeno del traffico di migranti a partire dalla crisi dei flussi del 2015 è comprovata dalla stima dei proventi ricavate dalle reti illegali: un fatturato tra i 3 e i 6 miliardi di euro su base mondiale e circa 200 milioni con riferimento alle rotte marittime nel 2019 verso l'Unione europea.

La piattaforma multidisciplinare europea di lotta alle minacce della criminalità (EMPACT) ha stabilito che la lotta al favoreggiamento dell'immigrazione irregolare rappresenta una delle priorità per il periodo 2022-2025. In particolare, nel 2020 l'azione coordinata degli Stati membri ha portato a 2.280 arresti, allo smantellamento di 14 gruppi della criminalità organizzata e al sequestro di:

- 639.900 di euro in contanti;
- 52 armi da fuoco;
- 1.166 documenti fraudolenti;
- 381 veicoli;
- 1.230 componenti di veicoli.

Il Centro EMSC

Si ricorda che nel febbraio 2016 l'UE ha istituito in seno a Europol il **Centro europeo contro il traffico di migranti (EMSC)** per aiutare gli Stati membri a combattere il fenomeno, con il compito principale di sostenere la polizia e le autorità di frontiera a coordinare operazioni antitraffico transfrontaliere complesse. Nel luglio 2019 il centro è stato integrato da una task force congiunta di collegamento sul traffico di migranti e sulla tratta di esseri umani.

Sono assegnati alla struttura 45 esperti in materia di traffico di migranti, specializzati, tra l'altro, in materia di documenti di identità fraudolenti, di informazioni sul traffico dei migranti nei social media, e su indagini finanziarie e recupero di beni criminali.

Il centro comprende il **Joint Operational Team (JOT) Mare**, composto da specialisti distaccati da sette Stati membri, con il compito di scambiarsi informazioni sulle reti dei trafficanti operanti in Turchia, Libia e altri Paesi nordafricani.

Nello specifico l'EMSC fornisce analisi sulle attività dei gruppi criminali organizzati, incrocia dati contenuti in varie banche dati, offre supporto

tecnico e forense. Fungendo da hub di informazioni, l'EMSC supporta le task force regionali dell'UE in Italia e in Grecia, che assistono le autorità nazionali tra l'altro nell'identificazione dei migranti e nelle procedure di asilo.

Il [sesto rapporto annuale](#) (2022) dell'EMSC illustra le attività e gli indicatori di *performance* della struttura, con un approfondimento specifico in merito ai collegamenti tra varie tipologie di crimine.

Nel 2021 l'EMSC ha scambiato sulla piattaforma Siena oltre **21 mila messaggi** relativi a circa **5 mila** casi concernenti il traffico di migranti, e redatto oltre mille rapporti.

La piattaforma **Siena (Secure Information Exchange Network Application)** è impiegata per gestire le comunicazioni delle forze dell'ordine dell'UE, consentendo lo **scambio** rapido di **informazioni** operative e strategiche relative alla criminalità tra:

- **funzionari** di collegamento, analisti ed esperti di Europol;
- **Stati membri**;
- **terze parti** che hanno stretto con Europol accordi di cooperazione o di lavoro.

La piattaforma è stata impiegata a partire dal 1° luglio 2009. Vi partecipano tra l'altro, **Eurojust**, **Frontex**, **OLAF** e **Interpol**, oltre a **Stati terzi** quali Australia, Canada, Norvegia, Liechtenstein, Moldavia, Svizzera e Stati Uniti.

In anni recenti l'accesso a SIENA è stato consentito anche a forze dell'ordine specializzate, come gli Uffici per il recupero dei beni (**ARO**), i centri di cooperazione doganale di polizia (**PCCC**), le unità di informazione ai passeggeri (**PIU**), i servizi finanziari unità di intelligence (**FIU**).

Sulla piattaforma è stato istituito un ambiente dedicato allo scambio di informazioni per le **unità antiterrorismo**. La Strategia 2020+ di Europol prevede l'ulteriore sviluppo di SIENA, per far progredire l'architettura di gestione delle informazioni di Europol e adottare rapidamente metodi e tecnologie aggiornate.

Il Centro ha sostenuto le operazioni delle forze di polizia in oltre 6 mila casi di traffico di migranti e tratta degli esseri umani; sono 55 i giorni di attività in loco di esperti di Europol; 26 i target di alto livello individuati.

Il rapporto si sofferma sul ruolo aumentato delle **tecnologie digitali** nel business del traffico di migranti e della tratta di esseri umani, con particolare riguardo all'uso di piattaforme di **social media** e di applicazioni **mobili**. In particolare secondo l'ESCM la rete della tratta degli esseri umani avrebbe

abusato dell'anonimato dell'ambiente Internet per individuare persone vulnerabili e per sfruttarle mediante siti Web e **piattaforme di incontri**.

Tra gli indicatori chiave del rapporto:

- il trend in aumento degli **attraversamenti** alle frontiere dell'UE e dei **movimenti secondari**;
- la pressione migratoria lungo la rotta orientale tramite la **Bielorussia** come fattore di aumento della presenza di reti criminali che facilitano i movimenti secondari;
- l'incremento dei **ricavi medi** per le attività di traffico di migranti verso **l'Italia**, quasi raddoppiati, da **6 mila** a circa **12 mila** euro;
- l'aumento della **policriminalità** delle reti del traffico di migranti lungo le rotte del Mediterraneo occidentale/Africa dell'ovest;
- la **digitalizzazione** del business, inclusi il reclutamento e l'organizzazione logistica, e le costanti pratiche di abusi.

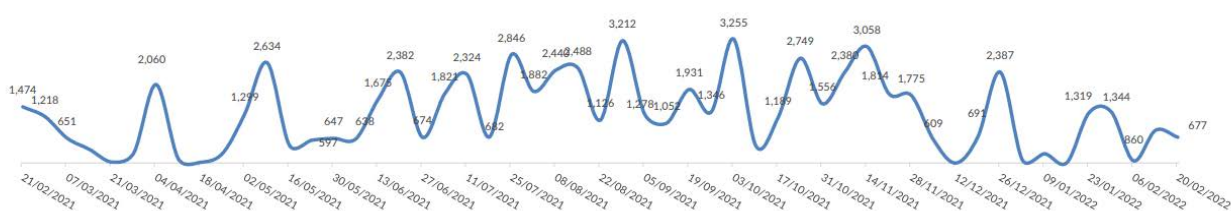
Si ricorda che il [rapporto](#) Jot mare pubblicato nel dicembre 2021 riferisce in merito ai ricavi che le reti del traffico di migranti hanno ottenuto nel 2019 anche in relazione ai flussi del Mediterraneo orientale e occidentale:

- nell'ambito della rotta orientale (principalmente verso la Grecia) le entrate dei trafficanti sono stimate in circa **90 milioni** di euro con un ricavo medio per migrante di circa **2.200** euro;
- gli introiti ottenuti dai trafficanti in relazione ai flussi nell'ambito della rotta occidentale (principalmente verso la Spagna) ammontano a circa **50 milioni**, con un'entrata media per migranti pari a **2.500** euro.

Dati statistici sui flussi migratori

Si ricorda che, secondo **l'UNHCR**, nel 2021 sono stati oltre **65 mila** i rifugiati e migranti sbarcati in Italia, il numero più alto nel periodo degli ultimi 4 anni e circa il doppio degli arrivi registrati lo scorso anno (**34.154**). Circa **50 mila** persone sono sbarcate in **Sicilia**, di cui oltre 35 mila migranti giunti a **Lampedusa**. In **Calabria** sono stati registrati oltre 11.500 migranti. Nei primi mesi del 2022 (dati UNHCR aggiornati al 20 febbraio 2022) sono circa 4.600 i migranti sbarcati sulle coste italiane.

Di seguito un grafico sul trend settimanale degli sbarchi in Italia a partire dal febbraio 2021 (UNHCR)

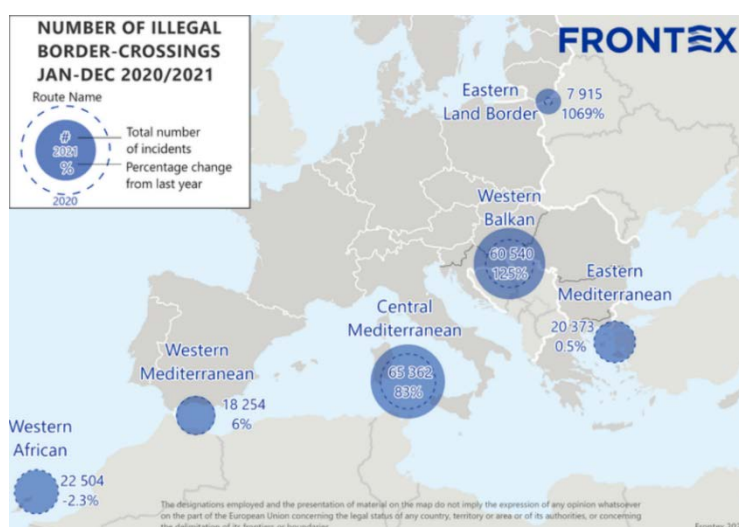


Sulle coste dell'Unione europea sono giunte complessivamente circa 11.400 persone, di cui 325 sbarchi in Grecia e oltre 6.300 in Spagna.

Di seguito il trend annuale dei flussi migratori (compresa la componente via terra) verso i Paesi UE del Mediterraneo (in azzurro gli sbarchi, in verde gli arrivi via terra, in rosso il numero delle persone scomparse o decedute) (fonte UNHCR)

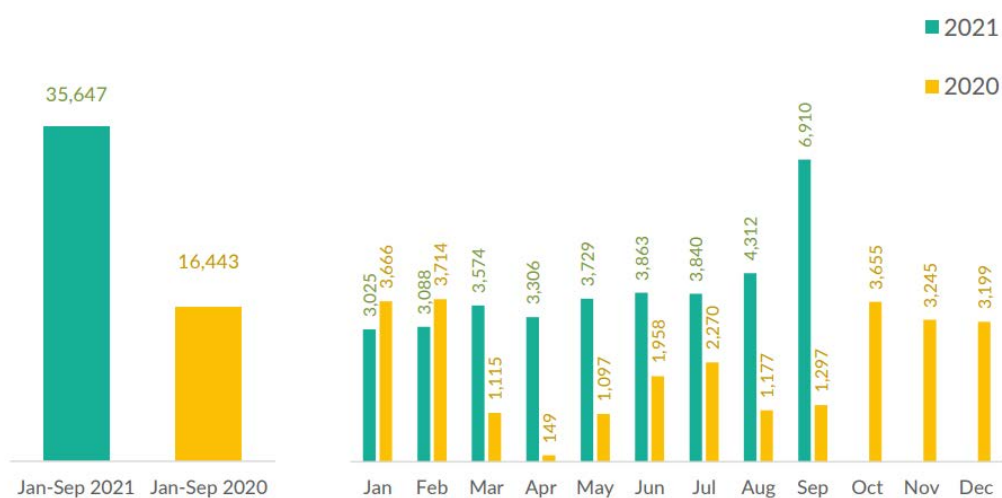
| Year | Arrivals via land (Green) | Landings (Blue) | Disappeared/Deceased (Red) |
|------|---------------------------|-----------------|----------------------------|
| 2021 | 1,218 | 41,979 | 428 |
| 2020 | 1,535 | 40,326 | 329 |
| 2019 | 6,345 | 26,168 | 510 |
| 2018 | 6,814 | 58,569 | 811 |
| 2017 | 6,246 | 22,103 | 202 |
| 2016 | 6,443 | 8,162 | 77 |
| 2015 | 11,624 | 5,312 | 59 |

Di seguito la mappa recante il numero degli attraversamenti illegali alle frontiere dell'UE nel 2021 comprensiva della variazione percentuale sul 2020 (fonte Frontex)



L’Agenzia per l’asilo dell’UE (EUAA) riferisce che secondo i dati aggiornati a novembre 2021 sono pendenti complessivamente nell’UE **431 mila** domande di protezione internazionale presentate per la **prima volta**, mentre alla fine di settembre 2021 i procedimenti di asilo in corso (sia di **prima istanza**, sia avviati con **domande non nuove**) negli Stati membri ammontano a **818 mila**.

Di seguito un grafico dell’UNHCR sul trend mensile delle domande di asilo registrate in Italia nel biennio 2020 – 2021



**RISCHI E OPPORTUNITÀ DELL'INTELLIGENZA ARTIFICIALE
PER EUROPOL**

La dimensione del fenomeno

Il [rapporto](#) *Malicious Uses and Abuses of Artificial Intelligence*, predisposto dall'unità EC3 (Centro europeo di Europol per la cibercriminalità) in collaborazione con Trend Micro Research e l'Istituto interregionale delle Nazioni Unite per la ricerca sul crimine e la giustizia (UNICRI) definisce intelligenza artificiale i sistemi di software (ed eventualmente di hardware) progettati in modo tale che, dato un obiettivo complesso, possono agire nello spazio fisico o digitale percependo il loro ambiente attraverso l'acquisizione e l'elaborazione dei dati, e prendere le decisioni sulle azioni migliori da intraprendere per raggiungere l'obiettivo prefissato.

Il documento offre una panoramica sulle modalità con le quali le reti criminali possono utilizzare l'IA per facilitare e potenziare le loro attività massimizzando le opportunità a scopo di lucro in tempi più brevi, individuando nuove vittime, e riducendo le possibilità di contrasto delle forze di polizia e delle autorità giudiziarie. Nel rapporto si distingue tra:

- “usi dannosi dell'IA” (*malicious use*) come nel caso di impiego di sistemi di apprendimento per automatizzare gli attacchi informatici e migliorare i malware;
- “abusi dannosi dell'IA” (*malicious abuse*) nei casi in cui i criminali tentano di attaccare e sfruttare i **sistemi di intelligenza artificiale esistenti** per violarli o aggirarli —ad esempio, hackerando gli assistenti domestici intelligenti.

Le forme più frequenti di impiego di IA in attività illecite e criminali riguardano le pratiche dei malware, l'abuso degli strumenti di assistenza intelligente (es. Amazon Alexa or Google Home), l'individuazione delle password supportata dall'IA, l'uso dell'IA per violare i sistemi CAPTCHA utilizzati per determinare se l'utente sia un umano o un *bot* (programma informatico creato per diversi scopi tra cui raccogliere informazioni dai siti internet e catalogarle); sistemi intelligenti in grado di replicare il comportamento umano per ingannare sistemi di rilevamento dei *bot* su piattaforme di social media; hackeraggio; attività illecite nel mercato delle criptomonete; crittografia assistita dall'intelligenza artificiale; attacchi di ingegneria sociale tra i quali ad esempio il *phishing*.

L’Innovation Lab di Europol e il Polo dell’innovazione dell’UE per la sicurezza interna

Il Laboratorio di Europol per l’innovazione gestisce progetti, avviati da Europol e/o dagli Stati membri dell’UE, per l’impiego di nuove tecnologie volte a soddisfare le esigenze operative della comunità delle forze dell’ordine dell’UE. In particolare, in collaborazione con il Centro comune di ricerca (JRC) della Commissione europea e l’Interpol Innovation Centre, il Lab monitora gli sviluppi tecnologici in materia di individuazione e analisi dei rischi nelle attività di polizia. Il Lab mantiene collegamenti con reti di esperti nel mondo dell’**industria**, del mondo **accademico**, della **società civile**, con **organizzazioni internazionali**, e con le forze dell’ordine.

Le attività del Lab includono:

- lo sviluppo di **partenariati strategici** per fornire nuove soluzioni tecnologiche agli Stati membri dell’UE;
- la definizione di **standard etici** nello sviluppo di soluzioni tecniche e *governance* dei dati;
- la promozione della **cultura** dell’innovazione tra le forze dell’ordine dell’UE;
- il miglioramento della capacità delle forze dell’ordine dell’UE di rilevare **distorsione** e **manipolazione dei dati**;
- la promozione di **standard** legislativi, regolamentari e di conformità per facilitare l’uso delle nuove tecnologie.

Di più ampia portata il **Polo** dell’innovazione (Innovation Hub) dell’UE per la sicurezza interna, costituito da una **rete di laboratori** per l’innovazione cui aderiscono altre Agenzie dell’UE. Partecipano all’Hub Stati membri europei, Europol, Frontex, eu-LISA (Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia), Eurojust, Agenzia per i diritti fondamentali (FRA), l’Osservatorio europeo delle droghe e delle tossicodipendenze (OEDT), l’Istituto per la parità di genere (EIGE), l’Ufficio europeo per l’asilo (EASO), l’Accademia di polizia dell’UE (CEPOL), Segretariato generale del Consiglio dell’Unione europea e Commissione europea.

Europol ospita il segretariato del **Polo** e un gruppo di funzionari provenienti dalle Agenzie UE per la gestione delle **operazioni quotidiane**. L’Hub coordina progetti nel campo della sicurezza interna con riferimento a

diversi settori di intervento: gestione delle frontiere, migrazione e dogane, giustizia penale.

I progetti dell'Hub riguardano, tra l'altro:

- l'impiego dei sistemi di **intelligenza artificiale**, con particolare riguardo a temi della responsabilità e dell'**etica**;
- i sistemi per la **biometrica**;
- le soluzioni per **comunicazioni** sicure;
- le tecnologie di crittografia/decrittografia;
- lo sviluppo di *open source*;
- le tecnologie **blockchain** e le sue applicazioni;
- nuove soluzioni per sensori e tecnologie per la **sorveglianza di frontiera**.

La proposta di regolamento recante norme in materia di intelligenza artificiale

Preannunciata in una serie di documenti programmatici della Commissione europea (tra i quali, il Libro Bianco sull'Intelligenza artificiale - un approccio europeo all'eccellenza e alla fiducia [COM\(2020\)65](#)), e pubblicata contestualmente alla comunicazione Promuovere un approccio europeo all'intelligenza artificiale [COM\(2021\)205](#)), la proposta di regolamento [COM\(2021\)206](#) reca una serie di norme armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad **alto rischio**, così come **restrizioni** in relazione a determinati usi, tra i quali in particolare i sistemi di identificazione biometrica remota.

La proposta è all'esame congiunto delle Commissioni **IMCO** (Mercato interno e protezione dei consumatori) e **LIBE** (Libertà, giustizia e affari interni) del **Parlamento europeo**; il **termine** per gli **emendamenti** alla proposta è stato fissato al **26 aprile 2022**. In sede di **Consiglio dell'UE**, la proposta è all'esame del Working party in materia di telecomunicazioni, che sta portando avanti i negoziati su un testo di compromesso predisposto dalla Presidenza.

L'intelligenza artificiale (IA) consiste in una famiglia di tecnologie in grado di generare **output** quali contenuti, **previsioni**, raccomandazioni o **decisioni** che influenzano gli ambienti con cui interagiscono.

La nuova disciplina mira a **ridurre al minimo** i rischi per la **sicurezza** e i **diritti fondamentali** che potrebbero essere generati dai sistemi di IA prima della loro immissione sul mercato dell'UE. A tal fine, l'approccio della

Commissione si basa su una "**piramide di rischio**" ascendente (che va dal **rischio basso/medio** a quello **elevato**, fino al rischio **inaccettabile**) per classificare, nell'ambito dell'IA, una serie di casi di pratiche generali e di impieghi specifici in determinati settori, cui la Commissione ricollega rispettive **misure di attenuazione**, o addirittura i **divieti** di alcune pratiche di IA.

Tali **divieti** riguardano una serie limitata di utilizzi dell'IA ritenuti **incompatibili** con i valori dell'Unione europea, in particolare quelli che si sostanziano nei diritti fondamentali contenuti nella Carta europea.

Si tratta in particolare di: divieti concernenti i sistemi di IA che **distorcono** il **comportamento** di una persona attraverso tecniche subliminali o sfruttando **vulnerabilità specifiche** in modi che causano o sono suscettibili di causare **danni fisici** o **psicologici**; divieti concernenti l'attribuzione di un **punteggio sociale** (*social scoring*) con finalità generali mediante sistemi di IA da parte di autorità pubbliche.

Il regime specifico di divieto si estende a determinati sistemi di **identificazione biometrica remota** (ad esempio strumenti di riconoscimento facciale per controllare i passanti in spazi pubblici), salvo casi eccezionalmente autorizzati dalla legge riconducibili in linea di massima ad attività di prevenzione e contrasto del crimine, in ogni caso soggetti a garanzie specifiche.

Una seconda categoria di sistemi di IA, pur consentiti ma classificati ad **alto rischio**, deve rispettare un insieme di **requisiti** specificamente progettati, che comprendono l'utilizzo di **set di dati** di alta **qualità**, l'istituzione di una **documentazione** adeguata per migliorare la tracciabilità, la condivisione di **informazioni** adeguate con l'utente, la progettazione e l'attuazione di misure adeguate di **sorveglianza** umana e il conseguimento degli standard più elevati in termini di **robustezza**, sicurezza, cibersicurezza e precisione. La proposta delinea un **sistema di valutazione di conformità** dei sistemi di IA ad alto rischio a tali requisiti, attivato prima che vengano immessi sul mercato o messi in servizio.

Per integrarsi agevolmente con i quadri giuridici esistenti la proposta tiene conto, ove opportuno, delle **regole settoriali** per la sicurezza, assicurando la **coerenza** tra gli atti giuridici e la semplificazione per gli operatori economici.

Per una serie di sistemi di IA considerati a basso rischio sono previsti soltanto **requisiti minimi di trasparenza**: è il caso di *chatbot* (programmi in grado di simulare **conversazioni umane**), sistemi di riconoscimento delle

emozioni o "deep fake" (foto, video e audio creati grazie a software di intelligenza artificiale che, partendo da contenuti reali, riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce).

Sono previste norme per promuovere il ricorso a **spazi di sperimentazione normativa**, che creano un ambiente controllato per testare tecnologie innovative per un periodo limitato, e l'accesso ai **poli** dell'innovazione digitale e a **strutture** di prova e sperimentazione, con l'obiettivo di sostenere le imprese innovative, le PMI e le *start-up*.

Per i profili attinenti a questioni di **sicurezza** si ricorda che l'articolo 5 della proposta (nell'ambito del titolo II sul regime delle **pratiche** di IA **vietate**), tra l'altro, vieta l'uso di sistemi di **identificazione biometrica** remota "in **tempo reale**" in **spazi accessibili al pubblico** a fini di attività di contrasto, **a meno che** e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

- i. la ricerca mirata di potenziali **vittime** specifiche di reato, compresi i minori scomparsi;
- ii. la **prevenzione** di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;
- iii. il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un **autore** o un **sospettato** di un **reato** contemplato dal regime in materia di **mandato d'arresto europeo**, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni.

Sono inclusi in tale categoria di reati, tra l'altro: la partecipazione a un'**organizzazione criminale**, il **terrorismo**, la **frode** e il **riciclaggio**, il traffico di **droga** e di armi, la **corruzione** e la criminalità informatica.

La proposta precisa inoltre che l'uso di sistemi di identificazione biometrica remota in **tempo reale** in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi citati debba tener conto:

- della natura della **situazione** che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del **danno causato** dal mancato uso del sistema;

- delle conseguenze dell'uso del sistema per i **diritti** e le **libertà** di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

Tale impiego deve altresì rispettare le tutele e le condizioni necessarie e **proporzionate** in relazione all'uso, in particolare per quanto riguarda le **limitazioni temporali, geografiche e personali**; inoltre ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto deve essere subordinato a un'**autorizzazione preventiva** rilasciata da un'**autorità giudiziaria** o da un'**autorità amministrativa indipendente** dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale.

Tuttavia, in una situazione di **urgenza debitamente giustificata**, è **possibile** iniziare a **usare** il sistema **senza autorizzazione** e richiedere l'autorizzazione **solo durante o dopo l'uso**. L'autorità giudiziaria o amministrativa competente, tenendo conto di una serie di elementi, rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è **necessario e proporzionato**.

Infine, uno Stato membro può decidere di prevedere la possibilità di **autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni sopra descritte**. Tale Stato membro stabilisce nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni, nonché per le attività di controllo ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati, compresi i reati per i quali si impiega la tecnica di rilevazione biometrica, le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto.

Da ultimo, con i riferimenti ad altre forme di IA che pongono **rischi** ritenuti nella proposta **inaccettabili**, si ricorda che l'**articolo 5** vieta, tra l'altro, l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che:

- utilizzano **tecniche subliminali** che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il

comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un **danno fisico o psicologico**;

- sfruttano le **vulnerabilità** di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di **distorcere materialmente il comportamento** di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un **danno fisico o psicologico**.