dossier

22 ottobre 2021

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

9a riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Videoconferenza, 25 e 26 ottobre 2021

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

9ª riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Videoconferenza, 25 e 26 ottobre 2021

SENATO DELLA REPUBBLICA

SERVIZIO STUDI
DOSSIER EUROPEI

N. 137

CAMERA DEI DEPUTATI

UFFICIO RAPPORTI CON
L'UNIONE EUROPEA

N. 69

Senato della Repubblica

Servizio Studi

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

Dossier europei n. 137

Camera dei deputati

Ufficio rapporti con l'Unione europea

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

Dossier n. 69

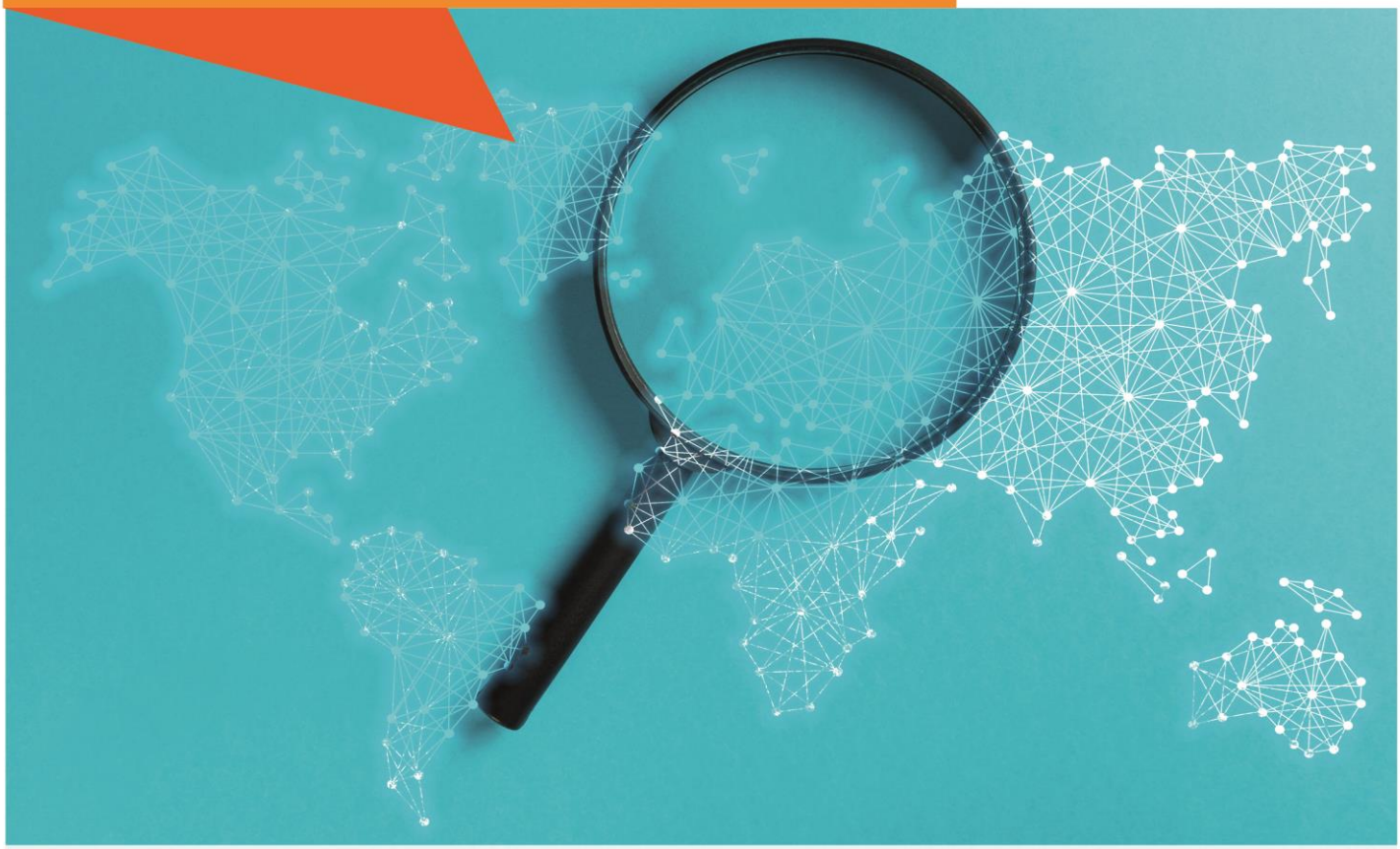
I N D I C E

9TH MEETING OF THE JOINT PARLIAMENTARY SCRUTINY GROUP (JPSG) ON THE EUROPEAN AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

25-26 OCTOBER 2021

EUROPEAN PARLIAMENT
BRUSSELS

REMOTE PARTICIPATION



JPSG on EUROPOL

CO-ORGANIZED:
by the European Parliament and
by the Sloveinan Presidency

European Parliament
National Parliaments

JOINT PARLIAMENTARY SCRUTINY GROUP (JPSG) ON THE EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

– 9TH MEETING –

EUROPEAN PARLIAMENT, BRUSSELS

MEETING BY REMOTE PARTICIPATION

AGENDA

Monday, 25 October 2021, 13.45 – 15.15

13.45 – 15.15 – Meeting of the Presidential Troika
(in camera)

Monday, 25 October 2021, 16.45 – 18.45

16.45 - 17.05 - Adoption of the agenda and opening remarks

- Mr Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the delegation of the European Parliament to the JPSG;
- Mr Nik PREBIL, Co-Chair of the JPSG and Head of the delegation of the National Assembly of the Republic of Slovenia to the JPSG;
- Ms Bojana POTOČAN, Co-Chair of the JPSG and Head of the National Council of the Republic of Slovenia Delegation to the JPSG
- Chairs' announcements reporting on the outcome on the Troika meeting (procedural points) and on the outcome of the Working Group on pending matters subject to possible further revision in the JPSG Rules of Procedure.

17.05 - 18.45 - Europol activities March - September 2021 and Presentation of the Europol Draft Multiannual Programming Document 2022-2024

- Presentation by Ms Catherine DE BOLLE, Europol Executive Director;
- Report by Mr Wojciech WIEWIÓROWSKI, Supervisor to the European Data Protection Supervisor;
- Written contribution by Mr Oliver RÜß, Chairperson of the Europol Management Board
- Written contribution by Professor Francois PELLEGRINI, Chair of the Europol Cooperation Board;
- Exchange of views;

Tuesday, 26 October 2021, 09.00 - 12.00

09.00 - 10.30 - Keynote interventions

- Ms Ylva JOHANSSON, Commissioner for Home Affairs;
- Mr Aleš HOJS, Minister of Interior, Slovenia;
- Exchange of views;

10.30 - 12.00 - Thematic debate - cybercrime in the EU, with a focus on online child abuse and the cooperation with third countries, including private persons and NGOs

- Presentation by Mr Fernando RUIZ, Head of Unit of Operations, European Cybercrime Centre, Europol;
- Presentation by Mr Olivier ONIDI, Deputy Director-General, Directoarte General for Migration and Home Affairs, European Commission;
- Presentation by Mr Robert TEKAVEC, Head of the Juvenile Crime Section, General Crime Division, Criminal Police Directorate, Police, Slovenia;
- Presentation by Mr Andrej MOTL, Safer Internet Centre, Slovenia;
- Exchange of views;

Tuesday, 26 October 2021, 13.45 - 15.45

13.45 - 15.15 - Thematic debate - Financial crime and corruption - protection of the EU financial interest

- Presentation by Mr Burkhard MUHL, Head of the European Financial and Economic Crime Centre, Europol;
- Presentation by Mr Frédéric BAAB, European Public Prosecutor, Office of the European Public Prosecutor;
- Presentation by Mr Nicholas FRANSSEN, Counsellor, Ministry of Justice and Security, The Netherlands;
- Exchange of views;

15.15 - 15.30 - Rules of procedure

- Presentation of the outcome of the Working Group and the compromise amendment;
- Possible adoption of the revised JPSG Rules of Procedure;

15.30 - 15.45 - Closing remarks by JPSG Co-Chairs:

- Mr Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the delegation of the European Parliament to the JPSG;
- Mr Nik PREBIL, Co-Chair of the JPSG and Head of the National Assembly, Slovenia;
- Ms Bojana POTOČAN, Co-Chair of the JPSG and Head of the National Council of the Republic of Slovenia Delegation to the JPSG.

Next meeting: Paris, France, February/March 2022 (TBC)

IL PROGRAMMA DELLA RIUNIONE

In base alla bozza di programma, le attività che il Gruppo di controllo parlamentare congiunto delle attività di Europol svolgerà in occasione della riunione di Bruxelles il 25 - 26 ottobre 2021 saranno precedute dall'incontro ristretto della Troika presidenziale, cui l'Italia non partecipa.

A seguito dell'adozione dell'agenda e dei saluti di apertura, il Gruppo inizierà i suoi lavori esaminando le attività di Europol nel periodo fra marzo e settembre 2021 e con la presentazione della bozza del documento di programmazione pluriennale 2022-2024 dell'Agenzia. La sessione prevede, tra l'altro, l'illustrazione delle attività di Europol e del citato documento da parte della direttrice esecutiva dell'Agenzia, Catherine De Bolle.

I lavori dovrebbero proseguire con:

- i keynote interventions *di Ylva Johansson, Commissaria europea per gli Affari interni, e Aleš Hojs, Ministro dell'interno della Slovenia;*
- *un primo dibattito tematico sul* cybercrime *nell'UE, con un focus sugli abusi sui minori* online *e la cooperazione con i Paesi terzi, incluse le persone private e le ONG;*
- *un secondo dibattito tematico sui reati finanziari e la corruzione, e protezione degli interessi finanziari dell'UE;*
- *una sessione dedicata alle Regole di procedura del JPSG, durante la quale è prevista la presentazione dell'*outcome *del Gruppo di lavoro e degli emendamenti di compromesso, in esito alla quale sarà possibile adottare le regole revisionate.*

In esito a ciascuna sessione è previsto lo svolgimento da parte del Gruppo di uno scambio di punti di vista.

I lavori del JPSG si concluderanno con le conclusioni e i commenti finali dei co-Presidenti del Gruppo, Juan Fernando López Aguilar, Presidente della Commissione per le libertà civili, giustizia e affari interni (LIBE) del Parlamento europeo, Nik Prebil, Capo della delegazione della Assemblea della Repubblica di Slovenia al JPSG e Bojana Potočan, Capo della delegazione del Consiglio nazionale della Slovenia al JPSG.

DOCUMENTO DI PROGRAMMAZIONE EUROPOL 2022 – 2024

Il progetto di programmazione pluriennale di Europol definisce: la programmazione strategica globale, compresi gli obiettivi, i risultati attesi e gli indicatori di performance; la pianificazione delle risorse, incluso il bilancio pluriennale e il personale; la strategia per i rapporti con i Paesi e le organizzazioni internazionali.

Priorità strategiche

Secondo il documento per il triennio 2022 - 2024 le seguenti priorità, indicate con la Strategia di Europol 2020+, guideranno il lavoro dell'Agenzia anche negli anni 2022-2024:

a) fungere da hub dell'UE delle **informazioni**, sfruttando appieno i dati provenienti da un'ampia rete di partner;

b) fornire un agile **supporto operativo**;

c) fungere da **piattaforma** per soluzioni di polizia europea;

d) essere in prima linea nell'**innovazione** e nella **ricerca** per le forze dell'ordine;

e) essere il **modello** europeo di **organizzazione** di contrasto al crimine con solide prestazioni, buona *governance* e responsabilità, promuovendo la diversità e il coinvolgimento del personale.

Hub di informazioni

Con riferimento alla priorità sub a) Europol intende, tra l'altro, migliorare la organizzazione delle informazioni tramite il perfezionamento della **gestione dei dati**, con particolare riguardo all'efficienza dell'acquisizione delle informazioni, e liberando risorse per analisi e supporto operativo. L'Agenzia intende altresì sfruttare le opportunità rese disponibili dall'**interoperabilità** dei sistemi dell'UE, incluso un maggiore uso della **biometria**.

Supporto operativo

Le aree di miglioramento chiave in relazione all'obiettivo di rafforzare il supporto operativo indicate nel programma sono:

- l'individuazione e il rafforzamento del supporto delle **indagini prioritarie;**

- lo sviluppo di **procedure** operative standard per una risposta rapida;
- l'ampliamento degli strumenti per l'applicazione del diritto dell'UE, con particolare riguardo alle **capacità tecniche** e **forensi** di nicchia;
- la creazione e il supporto a un ambiente per **team multidisciplinari** e indagini **transnazionali**.

Piattaforma per una polizia europea

In tale area l'Agenzia mira a rafforzare la capacità di **analisi**, in particolare al fine di rilasciare prodotti di analisi e servizi con *intelligence* fruibile, riconosciuti e utilizzabili dalle **autorità giurisdizionali** degli Stati membri. A tal proposito, l'Agenzia vuole: creare una **piattaforma** di conoscenza dinamica, in grado di sfruttare le informazioni in possesso di Europol; sviluppare una metodologia comune e standard di analisi; realizzare un **inventario centrale** delle competenze disponibili tra le forze dell'ordine degli Stati membri al fine di collegare le competenze; promuovere le migliori pratiche e fornire attività di formazione; istituire una piattaforma per complesse soluzioni di polizia dell'UE, tra l'altro in materia di la **decrittazione** e **criptovalute**.

Ricerca e innovazione

In tale ambito Europol intende affrontare la sfida relativa **all'evoluzione tecnologica** della criminalità, sempre più sofisticata, con particolare riguardo al tema della crescita esponenziale dei tipi e del volume di **dati**. A tal proposito l'Agenzia mira a sviluppare sia nuovi metodi per sfruttare l'intero valore dei dati disponibili, sia modelli innovativi nell'applicazione della legge a beneficio degli Stati membri. Le misure chiave in tale ambito sono: l'individuazione delle **esigenze** di innovazione e ricerca degli Stati membri, nonché dei migliori ***partner*** per tali obiettivi; lo sviluppo di una **strategia** di innovazione che definisca i settori prioritari di **investimento**; lo sviluppo di un **laboratorio** preposto all'innovazione.

Modello di organizzazione per l'applicazione della legge dell'UE

Gli obiettivi in tale ambito attengono alla gestione delle risorse, agli standard di *governance,* e ai profili di responsabilità e trasparenza dell'Agenzia. In particolare, l'Agenzia mira: al rafforzamento della forza lavoro mediante le capacità volte a migliorare l'**organizzazione**; a una gestione delle risorse **trasparente**, **affidabile** e conforme; allo sviluppo di

nuove strategie di **comunicazione**; a una strategia sulla **diversità** e **l'inclusione**.

Risorse umane e finanziarie

Secondo il documento di programmazione pluriennale le risorse proposte nell'ambito del bilancio di Europol per il 2022 ammontano a **192, 4 milioni di euro**. L'andamento del *budget* di Europol registra un **incremento** rispetto alla dotazione di 149 milioni nel 2020 e ai circa 172 del bilancio iniziale nel 2021 (si segnala che dal sito di Europol emerge che il bilancio dell'Agenzia nell'anno corrente è stato emendato più volte raggiungendo **attualmente la cifra di 182,3 milioni di euro**).

Per i profili relativi alle spese, la proposta per il 2022 prevede: per lo staff circa 101,6 milioni di euro (rispetto ai 96,2 previsti dal bilancio 2021 emendato); per le attività operative 76,2 milioni di euro (73,5 nel 2021); per le altre spese amministrative 14,5 milioni di euro (12,6 nel 2021).

Circa le risorse umane, l'organico indicato nel **2021** si attesta a **615 posti**; il documento prevede che il numero di posti nel **2022** aumenti con **71** posti di agente temporaneo (TA). Per il **2023** e il **2024** è previsto un **ulteriore aumento** rispettivamente di 30 e 26 posti di AT.

Il numero di agenti a contratto nel periodo 2022-2024 dovrebbe rimanere allo stesso livello del 2021 (235), così come quello degli esperti nazionali distaccati, che dovrebbero attestarsi 71.

Strategia esterna di Europol 2021-2024

Obiettivi generali

La strategia esterna fa parte della programmazione pluriennale di Europol, ai sensi dell'articolo 12 del regolamento Europol. Le disposizioni per le relazioni di Europol con i partner sono stabilite nel capo V del regolamento. Il quadro politico della strategia esterna di Europol 2021-2024 comprende l'agenda strategica 2019-2024 del Consiglio europeo, la strategia globale dell'UE, gli orientamenti politici dell'attuale Commissione e le tappe che conducono all'Unione della sicurezza europea, alla quale Europol contribuisce.

Secondo il documento Europol intende **sviluppare ulteriormente le sue relazioni con Paesi terzi**, organizzazioni internazionali, gruppi regionali e altri partner esterni. L'Agenzia mira a stabilire una nuova cooperazione strategica e operativa con partner esterni, per consentire alle autorità

competenti degli Stati membri di rafforzare ulteriormente la prevenzione e il contrasto alle forme gravi di criminalità. Europol intende altresì **rafforzare ulteriormente la sua cooperazione con la Commissione europea e il Servizio europeo per l'azione esterna (SEAE)** al fine di sostenere lo sviluppo delle relazioni esterne nel settore della sicurezza, in linea con le esigenze operative degli Stati membri. Oltre alle priorità esistenti, il documento pone l'accento sullo sviluppo di ulteriori capacità nella lotta alla criminalità informatica, alla criminalità finanziaria ed economica e alla criminalità ambientale per sostenere l'attuazione degli orientamenti politici della Commissione per il periodo 2019-2024.

Paesi prioritari

Nel documento si sottolinea l'**importanza del vicinato dell'UE** per la cooperazione esterna di Europol, nonché la necessità di instaurare **un'ottima partnership operativa con il Regno Unito**, dopo la sua uscita dall'Europa, in tutti i settori criminali che rientrano nel mandato di Europol.

La **regione dei Balcani occidentali rimane una priorità assoluta** per Europol in considerazione delle persistenti minacce alla sicurezza in termini di criminalità organizzata, terrorismo e traffico di migranti. Il documento ricorda che l'Agenzia partecipa a una cooperazione operativa consolidata con tutti i Paesi partner della regione (ad eccezione del Kosovo), dei quali ospita una comunità di ufficiali di collegamento nelle sue sedi.

Particolare attenzione dovrebbe essere prestata anche alla **cooperazione con la Turchia**, considerato che la conclusione del progetto di accordo operativo tra l'UE e la Turchia sullo scambio di dati personali tra Europol e le autorità di contrasto turche dovrebbe permettere una collaborazione più strutturata.

Con riferimento al partenariato orientale il documento indica che sarà proseguito il rafforzamento della cooperazione con l'Ucraina nella lotta contro la criminalità finanziaria ed economica in vista dell'istituzione dell'EFECC (*European financial and economic crime centre*), nonché nel contrasto alla criminalità informatica, considerato settore di interesse comune. Il documento sottolinea anche il focus sulla condivisione attiva delle informazioni con i Paesi che hanno stabilito una cooperazione con Europol e la promozione del modello di cooperazione di Europol presso i potenziali partner. La strategia ritiene prioritaria anche la **cooperazione con Stati Uniti, Canada e Australia**, e prefigura sforzi per sviluppare un'eccellente collaborazione anche con la **Nuova Zelanda**.

Nel documento Europol sottolinea la possibilità che sia necessaria ulteriore cooperazione con i Paesi asiatici a seguito della crisi da Covid-19. In particolare viene riconosciuta l'importanza di un **ulteriore impegno con la Cina**, nel quadro dell'accordo di cooperazione strategica, che dovrebbe andare di pari passo con i crescenti investimenti cinesi e l'espansione delle relazioni con alcuni Stati membri.

Si ricorda che il **30 dicembre 2020 -** su forte **impulso della Presidenza tedesca** del Consiglio dell'UE - l'**UE e la Cina** hanno raggiunto una **intesa** in **linea di principio per un accordo globale sugli investimenti (CAI)**.

L'accordo prevede, in particolare **l'impegno da parte della Cina a garantire**:

- un livello **più elevato di accesso al mercato per gli investitori dell'UE;**
- **un trattamento equo alle aziende dell'UE** in modo che possano competere in **condizioni di migliore parità in Cina**, anche in termini di disciplina per le imprese di proprietà statale, trasparenza dei sussidi e regole contro il trasferimento forzato di tecnologie;
- il **rispetto di disposizioni sullo sviluppo sostenibile**, compresi gli **impegni sul lavoro forzato** e la **ratifica** delle pertinenti **convenzioni fondamentali dell'OIL**.

La **firma dell'Accordo è al momento sospesa**. Il **Parlamento europeo** ha più volte ribadito in particolare,– da ultimo nella risoluzione del 16 settembre 2021 - **l'intenzione di non procedere alla ratifica dell'accordo fintanto che la Cina non ritirerà le controsanzioni adottate** in seguito alle sanzioni dell'UE per le violazioni dei **diritti umani nella regione autonoma uigura dello Xinjiang**.

Si ricorda che il **22 marzo 2021 l'UE ha adottato misure restrittive nei confronti di quattro persone fisiche e un'entità cinesi** direttamente responsabili di gr**avi violazioni dei diritti umani nella regione autonoma uigura dello Xinjiang**. In risposta a queste misure, la **Cina ha imposto controsanzioni** a dieci persone e a quattro entità europee, tra cui **cinque membri del Parlamento europeo e due organi istituzionali dell'UE**, la **sottocommissione per i diritti umani del Parlamento europeo** e il **comitato politico e di sicurezza del Consiglio dell'Unione europea**, oltre a due studiosi europei, due gruppi di riflessione in Germania e l'Alliance of Democracies Foundation in Danimarca

Il previsto invio di un nuovo ufficiale di collegamento di Europol a Singapore dovrebbe rafforzare le possibilità di cooperazione. La lotta alla criminalità informatica, lo sfruttamento sessuale dei minori e la cooperazione sull'innovazione sono indicate in cima all'agenda per la futura cooperazione nella regione.

Infine, la crescente domanda di droga, e in particolare potenziamento delle rotte del traffico di droga verso l'UE, nonché il tema della contraffazione dell'euro secondo la strategia giustificano la **necessità di una cooperazione**

rafforzata con i paesi dell'America latina. In tale contesto Europol annuncia l'intenzione di concentrarsi sulla cooperazione e su nuovi partenariati con la comunità andina.

Organizzazioni internazionali

Con riferimento alla cooperazione con le organizzazioni internazionali, il documento sottolinea che **Interpol** rimane il **partner chiave di Europol** grazie al suo raggio d'azione globale, agli strumenti complementari e al dialogo strategico che si è sviluppato tra i rispettivi dirigenti, poiché entrambe le organizzazioni supportano la cooperazione tra le forze dell'ordine. Secondo la strategia la cooperazione con Interpol continuerà e si svilupperà ulteriormente in linea con il regolamento e il previsto accordo di cooperazione UE-Interpol. Sono citati come partener strategici di Europol anche le organizzazioni di polizia regionali come la **Police Community of the Americas** (AMERIPOL), l'Associazione delle Nazioni del Sud-Est asiatico (ASEANAPOL) e il Meccanismo dell'Unione africana per la cooperazione di polizia (AFRIPOL).

Da ultimo, Europol annuncia l'intenzione di continuare i suoi sforzi per **rafforzare la cooperazione** con altre organizzazioni internazionali come l'Organizzazione del Trattato del Nord Atlantico (NATO), l'Organizzazione mondiale delle dogane (OMD), le entità delle Nazioni Unite (come ad esempio l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine – UNODC e *l'Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL* - UNITAD) e l'Organizzazione per la sicurezza e Cooperazione in Europa (OSCE) con particolare riguardo alla lotta al terrorismo e alle minacce ibride.

DIBATTITO TEMATICO I - LA CRIMINALITÀ INFORMATICA NELL'UE, CON PARTICOLARE ATTENZIONE AGLI ABUSI SUI MINORI *ONLINE* E LA COOPERAZIONE CON I PAESI TERZI, COMPRESI I PRIVATI E LE ONG

Con l'accelerazione della digitalizzazione, la sicurezza informatica è divenuta una delle componenti più importanti della sicurezza globale. Gli attacchi informatici e la criminalità informatica stanno aumentando in tutta Europa in termini sia di quantità che di sofisticazione; una tendenza destinata a crescere in futuro, visto che il numero dei dispositivi connessi, fra cui macchine, sensori, componenti industriali e reti che costituiscono l'internet degli oggetti (IoT), continua a crescere.

Come evidenziato nella risoluzione del **Parlamento europeo**, del **10 giugno 2021**, sulla strategia dell'Ue in materia di cibersicurezza per il decennio digitale, si prevede che, entro il 2024, in tutto il mondo i dispositivi collegati all'IoT saranno 22,3 miliardi. Inoltre, in base a stime dell'associazione internazionale dei gestori di telefonia mobile (Gsma) i dispositivi connessi superano già il numero delle persone sul pianeta, e il loro numero dovrebbe salire a 25 miliardi entro il 2025, di cui un quarto si troverà in Europa. La pandemia di Covid-19 ha d'altra parte accelerato la digitalizzazione dei modelli di lavoro.

Tutto questo ha accresciuto le vulnerabilità agli attacchi informatici, come segnalato in *"The Internet Organised Crime Threat Assessment"* (Iocta), la relazione pubblicata ogni anno dal Centro europeo per la lotta alla criminalità informatica (EC3) al fine di illustrare i principali risultati, le minacce emergenti e gli sviluppi in merito al *cybercrime*.

L'unità EC3

Operativo dal gennaio del 2013, il **Centro europeo per la lotta alla criminalità informatica** (EC3) si concentra sulle attività illegali *online*, con particolare riguardo alle frodi e agli **attacchi diretti contro l'*e-banking* e altre attività finanziarie *online*,** allo **sfruttamento sessuale dei minori *online*** e ai **reati che colpiscono i sistemi di informazione e alle infrastrutture critiche** dell'Ue[1].

[1] Tali ambiti di intervento corrispondono alle priorità individuate dal Consiglio dell'Ue nel maggio del 2017 nell'ambito del cosiddetto Ciclo programmatico 2018-2021 per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale.

Il centro sostiene le autorità nazionali di contrasto alla criminalità sul piano **operativo**, **investigativo** e **forense**. La struttura funge da *hub* centrale per informazioni e *intelligence* criminali; sostiene le operazioni e le indagini degli Stati membri offrendo analisi operative e coordinamento; fornisce, inoltre, prodotti di analisi strategica e svolge attività di sensibilizzazione che colleghi le autorità di contrasto che affrontano la criminalità informatica con il settore privato, il mondo accademico e altri partner; la cellula sostiene infine la formazione e il rafforzamento delle capacità, in particolare per le autorità competenti negli Stati membri, e fornisce capacità di supporto tecnico legale e digitale.

Le attività dell'EC3 sono supportate dal ***Cyber Intelligence Team*** **(Cit)**, i cui analisti raccolgono ed elaborano le informazioni relative al crimine informatico da fonti pubbliche, private e aperte e identificano le minacce e i modelli emergenti, e dalla ***Task Force*** congiunta di azione sulla criminalità informatica (J-Cat), che lavora sui più importanti casi internazionali di criminalità informatica che colpiscono gli Stati membri dell'Ue e i loro cittadini.

Il rapporto Europol Iocta, pubblicato annualmente, offre una **valutazione della minaccia rappresentata dalla criminalità organizzata su internet.** È considerato il prodotto strategico di punta di Europol in quanto pone in evidenzia quelle che sono le minacce dinamiche e in continua evoluzione della criminalità informatica. Secondo l'ultimo *Internet Organized Crime Threat Assessment (Iocta),* del 5 ottobre 2020, il *cybercrime* sta diventando sempre più aggressivo, come si può riscontrare nelle varie forme di criminalità informatica. La relazione fa riferimento in particolare ai crimini ad alta tecnologia e alle violazioni dei dati.

La raccolta dei dati per la stesura del rapporto 2020 è avvenuta durante la pandemia di Covid-19, la quale ha provocato cambiamenti significativi e introdotto diverse forme di criminalità informatica. I criminali hanno ideato nuovi *modus operandi* e adattato quelli esistenti per sfruttare la situazione, utilizzato nuovi "vettori di attacco" e individuato nuovi gruppi di potenziali vittime.

Il rapporto evidenzia in particolare che:

- l'**ingegneria sociale** rimane una delle principali minacce, in quanto può facilitare altri tipi di criminalità informatica;
- le **criptovalute** agevolano i pagamenti per varie forme di criminalità informatica, mentre si assiste a un'evoluzione nella *privacy* per quanto riguarda *crypto coins* e servizi;

- il ***ransomware*** continua a essere uno dei principali rischi (i criminali aumentano le pressioni minacciando la pubblicazione dei dati nel caso le vittime non paghino);
- il ***ransomware* sui *providers* di parti terze** crea danni potenziali e ingenti per le altre società della catena di approvvigionamento e delle infrastrutture critiche;
- **Emotet** è ritenuta una delle *cyber* minacce più pericolose al mondo, data la versatilità del suo utilizzo, e punto di riferimento del moderno *malware*[2];
- il **potenziale della minaccia degli attacchi DDoS** (*Distributed Denial of Service*) è maggiore rispetto all'impatto attuale nell'Ue.

Iniziative dell'Unione europea volte a contrastare la criminalità informatica

L'Unione europea ha progressivamente rafforzato le misure volte a contrastare la criminalità informatica, articolando il proprio intervento con riferimento a tre principali categorie di illeciti:

1. gli **attacchi alle reti e ai sistemi informatici**;
2. la perpetrazione di **reati di tipo comune** (ad esempio, crimini essenzialmente predatori) tramite l'uso di sistemi informatici;
3. la **diffusione di contenuti illeciti** (ed esempio, **pedopornografia**, propaganda terroristica, *hate speech*/discorso di odio, etc.) per mezzo di sistemi informatici.

Le politiche di contrasto alle attività illecite e dolose di natura informatica e basate sull'uso di sistemi informatici (comprese le iniziative in materia di disinformazione) sono state trattate in occasione dei vari Consigli europei, in occasione dei quali i leader dell'Ue hanno, fra l'altro, chiesto la conclusione dei procedimenti legislativi dei principali strumenti normativi proposti dalla Commissione europea, e dato impulso a nuove iniziative nel campo della cibersicurezza.

[2] A gennaio 2021 un'operazione coordinata fra le forze di polizia internazionali - Europol, Fbi, National Crime Agency britannica e forze dell'ordine di Paesi Bassi, Germania, Francia, Lituania, Canada e Ucraina - hanno concluso un'operazione di contrasto, riuscendo infine ad assumere il controllo dell'infrastruttura che gestisce e coordina Emotet. L'attività internazionale è stata coordinata da Europol ed Eurojust e l'operazione è stata svolta nel quadro della Piattaforma multidisciplinare europea di lotta alle minacce della criminalità (Empact).

1. Le minacce alle reti e ai sistemi informatici

La prima categoria di illeciti è considerata di particolare rilievo, attesa la vitale importanza delle reti e dei sistemi informatici rispetto al funzionamento delle **infrastrutture critiche** (fra tutte, il sistema dei trasporti, le strutture ospedaliere, quelle energetiche), la cui sicurezza attiene peraltro al normale **svolgimento della vita democratica di un paese**. L'intervento dell'Ue al riguardo si è sviluppato su diversi piani, inclusa la politica estera, di sicurezza e di difesa europea, stante la natura di vera e propria **minaccia ibrida** di alcune tipologie di attacchi informatici.

Per **minacce ibride** – nozione per la quale non esiste una definizione sul piano giuridico universalmente accettata – la Commissione europea intende una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali pur senza oltrepassare la soglia di guerra formalmente dichiarata. Il loro obiettivo non consiste soltanto nel provocare danni diretti e nello sfruttare le vulnerabilità, ma anche nel destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

In particolare, con la direttiva 2016/1148, sulla **sicurezza delle reti e dell'informazione - direttiva Nis** (recepita in Italia con il Decreto legislativo 18 maggio 2018, n. 65), l'Unione europea ha posto le basi per un miglioramento della cooperazione operativa fra Stati membri in caso di incidenti di cibersicurezza e della condivisione delle informazioni sui rischi. La direttiva definisce obblighi di sicurezza per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, l'assistenza sanitaria e la finanza) e i fornitori di servizi digitali (mercati *online*, motori di ricerca e servizi di *cloud*); inoltre, ogni paese dell'Ue è tenuto a designare una o più autorità nazionali con il compito, fra l'altro, di monitorare l'applicazione della direttiva, nonché a elaborare una strategia per affrontare le minacce informatiche.

L'Ue ha consolidato tale quadro mediante l'adozione del regolamento (UE) n. 2019/881 sulla **cibersicurezza** (cd. ***cybersecurity act***), recante una serie di disposizioni per:

- il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (**Enisa**);
- l'introduzione nell'Unione di **sistemi europei di certificazione** della cibersicurezza dei prodotti e dei servizi delle tecnologie

dell'informazione e della comunicazione - TIC (che consisterebbero in una serie di norme, requisiti tecnici e procedure).

Il **20 maggio 2021** è stato inoltre adottato il regolamento (UE) 2021/887 che istituisce il **Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento**. La creazione del Centro europeo di competenza per la cibersicurezza dovrebbe contribuire ad aumentare la sicurezza delle reti e dei sistemi informativi, fra cui **internet** e altre **infrastrutture critiche** per il funzionamento della società, come i **trasporti, la sanità, l'energia, le infrastrutture digitali, l'acqua, il mercato finanziario e i sistemi bancari**.

Disposizioni volte alla sicurezza delle reti sono altresì contenute nel Codice delle comunicazioni elettroniche.

2. L'uso dei sistemi informatici a fini criminali

L'intervento normativo in tale settore comprende la direttiva n. 2019/713 relativa alla **lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.** Gli elementi chiave della direttiva, sostitutiva della precedente decisione quadro 2001/413/GAI del Consiglio, sono: l'ampliamento della portata dei reati, che secondo il nuovo regime include, fra l'altro, le transazioni mediante valute virtuali; l'armonizzazione delle definizioni di alcuni reati *online*, quali la pirateria informatica o il *phishing*; l'introduzione di livelli minimi per le sanzioni più elevate per le persone fisiche; norme in materia di competenza giurisdizionale riguardo le frodi transfrontaliere; il miglioramento della cooperazione in materia di giustizia penale; la prevenzione e le attività di sensibilizzazione per ridurre i rischi di frodi.

Nell'ambito degli strumenti per la cibersicurezza, la Commissione europea ha altresì presentato **proposte legislative volte a migliorare l'acquisizione transfrontaliera di prove elettroniche per i procedimenti penali**. Si tratta di una proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali, e di una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali. Le proposte sono tuttora all'esame delle Istituzioni legislative europee.

La materia è stata trattata dall'Ue anche per i profili di politica estera. A tal proposito, il 6 giugno 2019, il Consiglio dell'Ue ha conferito alla Commissione europea due mandati per svolgere negoziati internazionali intesi a migliorare l'**accesso transfrontaliero alle prove elettroniche** nelle indagini penali, da un lato, con gli Stati Uniti, dall'altro con particolare riguardo al secondo protocollo aggiuntivo alla **Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica**. I mandati includono disposizioni recanti garanzie a tutela dei diritti fondamentali in materia di protezione dei dati, *privacy* e diritti procedurali delle persone.

Si segnalano infine:

- l'esperienza acquisita nel quadro degli sforzi di autoregolamentazione sostenuti dalla Commissione, come l'impegno per la sicurezza dei prodotti (*Product Safety Pledge*);
- il protocollo d'intesa sulla vendita di merci contraffatte;
- il codice di condotta per lottare contro le forme illegali di **incitamento all'odio *online*** (su cui, da ultimo, il **7 ottobre 2021** la Commissione ha presentato la 6a valutazione);
- il Forum dell'Ue su internet avviato nel dicembre 2015 nel quadro dell'Agenda europea sulla sicurezza;
- il regolamento (UE) 2021/784, del **29 aprile 2021**, relativo al **contrasto della diffusione di contenuti terroristici *online*.** Forum dell'Ue su internet per quanto riguarda i contenuti terroristici.

3. L'impiego dei sistemi informatici per la diffusione di contenuti illegali.

Il contrasto alle attività di disinformazione

Dal 2015, l'Ue è sistematicamente impegnata nel contrasto alle attività di **disinformazione**, cui sono riconducibili - secondo la definizione impiegata dalla Commissione europea - informazioni verificate come **false** o **fuorvianti** create, presentate e diffuse a scopo di **lucro** o al fine di **ingannare** intenzionalmente il **pubblico**, compreso l'obiettivo di **falsare** il **dibattito pubblico**, minare la **fiducia** dei cittadini nelle istituzioni e nei media e **destabilizzare** i **processi democratici** come le **elezioni**.

Fra i primi strumenti per contrastare la propaganda di enti e organismi situati in **Stati terzi** volta a diffondere informazioni fuorvianti o palesemente false (in particolare, da parte della Russia), la *Task force East StratCom*, istituita nel 2015 con il compito di sviluppare prodotti e campagne di

comunicazione incentrate sulla spiegazione delle politiche dell'Ue nella regione del **partenariato orientale**. Sono incentrate su aree geografiche diverse: la *Task Force* ***StratCom*** **per i Balcani occidentali** e la ***Task Force South Med Stratcom*** per il mondo di lingua araba.

Fra le iniziative più significative per il contrasto alla disinformazione si ricordano:

- la comunicazione dell'aprile 2018, con la quale la Commissione europea ha delineato un approccio comune alla materia e previsto quale misura chiave l'elaborazione da parte dei rappresentanti delle piattaforme *online*, dell'industria della pubblicità e dei principali inserzionisti di un codice di condotta per lottare contro le forme illegali di **incitamento all'odio *online*** (su cui, da ultimo, il **7 ottobre 2021** la Commissione ha presentato la 6a valutazione);

Il codice è stato adottato nell'ottobre del 2018 dalle principali piattaforme *online* (fra le quali Facebook, Google, Twitter, YouTube Instagram, Snapchat, Dailymotion, Jeuxvideo.com e TikTok a settembre), dalle società di *software* (in particolare, nel maggio 2019, ha aderito al codice la Microsoft) e dalle organizzazioni che rappresentano il settore della pubblicità. Il codice prevede una serie di impegni, che comprendono la garanzia della trasparenza dei messaggi pubblicitari di natura politica, la chiusura dei profili falsi, l'etichettatura dei messaggi diffusi dai "bot" e il miglioramento della visibilità dei contenuti sottoposti a verifica dei fatti.

- il **pacchetto elezioni** (presentato dalla Commissione europea in occasione del discorso sullo Stato dell'Unione del settembre 2018), recante una serie di misure per garantire elezioni libere ed eque;

Si tratta, in particolare, di: una comunicazione della Commissione europea "Assicurare elezioni europee libere e corrette (COM(2018)637); la Raccomandazione (UE) 2018/334 della Commissione, del 1º marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali *online*; orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di protezione dei dati nel contesto elettorale; una serie di modifiche (entrate in vigore nel marzo del 2019) al regolamento relativo al finanziamento dei partiti politici europei, che introducono in particolare sanzioni finanziarie ai partiti politici europei e alle fondazioni politiche europee che influenzano deliberatamente, o tentano di influenzare, i risultati delle elezioni del Parlamento europeo approfittando di violazioni delle norme in materia di protezione dei dati.

- il Piano d'azione contro la disinformazione, presentato dalla Commissione europea e dall'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza nel dicembre 2018, articolato in quattro settori chiave.

I settori sono: capacità di individuazione dei casi di disinformazione, in particolare tramite il rafforzamento delle *task force* di comunicazione strategica e della cellula dell'Ue per l'analisi delle minacce ibride del Servizio europeo per l'azione esterna (Seae); risposta coordinata, dotando istituzioni Ue e Stati membri di un sistema di allarme rapido per la condivisione e valutazione delle campagne di disinformazione; attuazione efficace da parte delle piattaforme *online* e delle industrie firmatarie degli impegni nell'ambito del codice di buone pratiche; campagne di sensibilizzazione e di responsabilizzazione dei cittadini in particolare mediante l'alfabetizzazione mediatica. Il 14 giugno 2019, è stata pubblicata una relazione sullo stato dell'arte dell'attuazione del piano.

Con particolare riferimento alla **pandemia di Covid-19**, il 10 giugno 2020 la Commissione e l'Alto rappresentante hanno pubblicato la comunicazione congiunta "Contrastare la disinformazione sulla Covid-19 – Guardare ai fatti".

Come evidenziato nella sua comunicazione dal titolo "Plasmare il futuro digitale dell'Europa", del 19 febbraio 2020, la Commissione si è impegnata ad aggiornare le norme orizzontali che definiscono **le responsabilità e gli obblighi dei prestatori di servizi digitali**, in particolare delle piattaforme *online*, dichiarando che "le persone hanno diritto a tecnologie di cui possono fidarsi" e che "**ciò che è illecito *offline* deve esserlo anche *online***".

Di particolare rilievo in tal senso è la proposta di regolamento relativo a un mercato unico dei servizi digitali (cd. **"legge sui servizi digitali"**), adottata dalla Commissione europea il 15 dicembre 2020 e all'esame dei colegislatori, che rappresenta una delle misure chiave nell'ambito della Strategia europea per il digitale. La proposta intende modificare la direttiva 2000/31/CE sul commercio elettronico in quanto, dalla sua adozione, si sono affermati nuovi e innovativi servizi digitali della società dell'informazione che - sottolinea la Commissione nella relazione illustrativa - "hanno cambiato la vita quotidiana dei cittadini dell'Unione plasmando e trasformando il loro modo di comunicare, connettersi, consumare e svolgere attività economiche (...). Allo stesso tempo, dall'uso di questi servizi sono scaturiti nuovi rischi e

nuove sfide, che interessano sia la società nel suo complesso, sia le singole persone che si avvalgono di tali servizi".

Abusi sessuali online sui minori

Come sopra ricordato, secondo i dati dell'Europol, la pandemia di Covid-19 ha contribuito all'aumento del già alto numero di casi riguardanti abusi sessuali di minori su internet. Le misure di confinamento hanno infatti portato a un aumento del tempo trascorso su internet da parte dei minori, spesso senza supervisione e questo li ha resi più esposti alle pratiche di sfruttamento. Gli autori di abusi sessuali hanno quindi tratto profitto dalla situazione pandemica per adescare le potenziali vittime fra i minori.

Anche il rapporto annuale della Internet Watch Foundation (Iwf) indica che i fornitori di servizi internet in Europa sono diventati la più vasta fonte di materiale contenente abusi sessuali infantili al mondo.

I dati mostrano un aumento dei casi di estorsioni a sfondo sessuale e di *cyber-grooming*, la pratica consistente nel simulare un legame di amicizia con un minore, allo scopo di commettere abusi sessuali ai suoi danni. Inoltre, le **tecnologie digitali** da un lato hanno consentito ai criminali di raggiungere più facilmente i minori tramite l'uso di *webcam*, dispositivi connessi e *chat room* sui social media e nei videogiochi; dall'altro ne hanno garantito l'anonimato grazie all'uso di tecnologie come il *cloud computing* e il *dark web*.

Fra le iniziative della Commissione europea si ricorda l'adozione, il 14 luglio 2021, del regolamento (UE) 2021/1232 relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda **l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali *online* sui minori.**

Il regolamento stabilisce norme temporanee che derogano a determinati obblighi previsti dalla direttiva 2002/58/CE (**direttiva *e-privacy***), con l'obiettivo di consentire ai fornitori di servizi di comunicazione interpersonale indipendenti dal numero di continuare a utilizzare tecnologie per il trattamento di dati personali e di altro tipo nella misura necessaria a individuare e segnalare gli abusi sessuali sui minori *online* e a rimuovere il materiale pedopornografico nell'ambito dei loro servizi.

La direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche stabilisce le norme volte a garantire la sicurezza nel trattamento dei dati personali, la notifica delle violazioni dei dati personali e la riservatezza delle comunicazioni. Vieta inoltre le comunicazioni indesiderate qualora l'utente non abbia fornito il proprio consenso. La direttiva attua nel diritto derivato dell'Unione gli articoli 7 (sul rispetto della vita privata e della vita familiare) e 8 (sulla protezione dei dati di carattere personale) della Carta dei diritti fondamentali dell'Unione europea.

Con l'applicazione del **Codice europeo delle comunicazioni elettroniche**, istituito dalla sopra citata direttiva (UE) 2018/1972, la definizione di "servizi di comunicazione elettronica" sarà sostituita da una nuova definizione, che comprenderà i servizi di comunicazione interpersonale indipendenti dal numero. I servizi di comunicazione interpersonale indipendenti dal numero rientreranno pertanto nell'ambito di applicazione della direttiva *e-privacy*. Il cambiamento riguarderà i servizi di comunicazione quali i servizi di messaggistica e di posta elettronica basati sul *web* nonché la telefonia via internet.

Il Codice europeo delle comunicazioni elettroniche definisce **"servizi di comunicazione elettronica"** i servizi forniti di norma a pagamento su reti di comunicazioni elettroniche, che comprendono, con l'eccezione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti, i seguenti tipi di servizi: il "servizio di accesso a internet" quale definito all'articolo 2, comma 2, punto 2), del regolamento (UE) 2015/2120 che stabilisce misure riguardanti l'accesso a un'Internet aperta[3]; il "servizio di comunicazione interpersonale"; i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali, come i servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina e per la diffusione circolare radiotelevisiva. In particolare, il codice definisce **"servizio di comunicazione interpersonale indipendente dal numero"** un servizio di comunicazione interpersonale che non si connette a risorse di numerazione assegnate pubblicamente — ossia uno o più numeri che figurano in un piano di numerazione nazionale o internazionale — o che non consente la

[3] Il regolamento (UE) 2015/2020 definisce "servizio di accesso a Internet" un servizio di comunicazione elettronica a disposizione del pubblico che fornisce accesso a Internet, ovvero connettività a praticamente tutti i punti finali di Internet, a prescindere dalla tecnologia di rete e dalle apparecchiature terminali utilizzate.

comunicazione con uno o più numeri che figurano in un piano di numerazione nazionale o internazionale.

La lotta contro gli abusi sessuali sui minori è una delle **priorità dell'Unione europea**.

Il 24 luglio 2020 la Commissione europea ha adottato una **Strategia dell'Ue per una lotta più efficace contro gli abusi sessuali su minori** (COM(2020)607), che mira a fornire una risposta efficace a livello di Ue al reato di abuso sessuale sui minori.

La strategia sottolinea fra l'altro che occorrerà innanzitutto garantire **la piena attuazione della legislazione vigente**, rappresentata dalla direttiva 2011/93/UE relativa alla **lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile**, primo strumento giuridico dell'Ue con un approccio globale che istituisce norme minime relative alla definizione dei reati e delle sanzioni in materia di abuso e sfruttamento sessuale dei minori e di materiale pedopornografico, e che comprende la prevenzione, l'indagine e il perseguimento dei reati, nonché l'assistenza e la protezione delle vittime. I reati riguardano situazioni *offline* e *online*, quali la visione e la diffusione di materiale pedopornografico *online*, l'adescamento (ossia la creazione di un legame emotivo *online* con un minore a scopo di abusi sessuali) e gli abusi sessuali tramite *webcam*.

La Commissione ritiene che la lotta contro gli abusi sessuali su minori *online* richieda chiari obblighi imperativi che impongano di individuare e segnalare gli abusi sessuali su minori *online*, al fine di apportare maggiore chiarezza e certezza al lavoro sia delle autorità di contrasto che dei soggetti pertinenti del settore privato per contrastare gli abusi *online*. La Commissione intende a tal fine preparare una **legislazione settoriale volta a contrastare in modo più efficace gli abusi sessuali su minori *online***, nel pieno rispetto dei diritti fondamentali, in particolare il diritto alla libertà di espressione, la protezione dei dati personali e il rispetto della vita privata.

La strategia dell'Ue in materia di cibersicurezza per il decennio digitale

Nella comunicazione congiunta - presentata il 16 dicembre 2020 dalla Commissione europea e dall'Alto rappresentante per gli affari esteri - dal titolo "La strategia dell'Ue in materia di cibersicurezza per il decennio digitale", la Commissione europea afferma che la cibersicurezza è fondamentale per creare un'Europa digitale, verde e resiliente.

L'Unione europea intende rispondere alle sfide **in materia di cibersicurezza** attraverso una serie di meccanismi e misure, che coinvolgono i seguenti sei settori chiave:

1) accrescere la ciberresilienza;

2) proteggere le infrastrutture critiche;

3) combattere la criminalità informatica;

4) rafforzare la diplomazia informatica;

5) intensificare la ciberdifesa;

6) promuovere la ricerca e l'innovazione nella sicurezza informatica.

Come evidenziato nella comunicazione, la strategia rappresenta una "componente chiave" del documento "Plasmare il futuro digitale dell'Europa" (COM(2020)67), del piano per la ripresa europea della Commissione ("Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione" - COM(2020)456), della strategia dell'Ue per l'Unione della sicurezza 2020-2025 (COM(2020)605), della strategia globale per la politica estera e di sicurezza dell'Unione europea e dell'agenda strategica del Consiglio europeo 2019-2024.

La strategia definisce in che modo l'Ue intende proteggere i cittadini, le imprese e le istituzioni dalle **minacce informatiche**, promuovere la cooperazione internazionale e contribuire a garantire un'internet globale e aperta. A tal fine, facendo seguito ai progressi conseguiti con le strategie precedenti, la comunicazione delinea proposte concrete per l'attuazione di tre strumenti principali - normativi, di investimento e politici - per tre settori di intervento dell'Ue:

1. **resilienza, sovranità tecnologica e *leadership;***
2. **sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta:**
3. **promozione di un ciberspazio globale e aperto**.

Con riferimento a quest'ultimo punto, la strategia evidenzia che l'Ue dovrebbe continuare a **collaborare con i partner internazionali** per promuovere un modello politico e una visione del ciberspazio fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici che generino sviluppo sociale, economico e politico a livello globale e contribuiscano a un'Unione della sicurezza. A tal fine, l'Ue dovrebbe lavorare con i Paesi terzi, le organizzazioni internazionali e la comunità multipartecipativa per sviluppare e attuare una politica

internazionale in materia di ciberspazio coerente e olistica che tenga conto della crescente interconnessione fra gli aspetti economici delle nuove tecnologie, la sicurezza interna e le politiche estere, di sicurezza e di difesa.

Si dovrebbe pertanto estendere il dialogo dell'Ue in materia di ciberspazio con paesi terzi, organizzazioni internazionali e regionali, anche attraverso una **rete informale della diplomazia informatica dell'Ue**.

L'Ue dovrebbe inoltre: intensificare il suo impegno e la sua *leadership* nei **processi di normazione internazionale**[4], nonché rafforzare la propria rappresentanza negli organismi di normazione internazionali ed europei e in altre organizzazioni per lo sviluppo di norme; promuovere la sicurezza e la stabilità internazionali nel ciberspazio, in particolare attraverso la proposta dell'Ue e dei suoi Stati membri di un programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio (PoA) in seno alle **Nazioni Unite**; rafforzare ed espandere i dialoghi in materia di ciberspazio con i paesi terzi per promuovere i suoi valori e la sua visione del ciberspazio, condividendo le migliori pratiche e cercando di cooperare in modo più efficace, e avviare scambi strutturati con organizzazioni regionali come l'Unione africana, il Forum regionale dell'Associazione delle Nazioni del Sud-est asiatico (Asean), l'Organizzazione degli Stati americani e l'Organizzazione per la sicurezza e la cooperazione in Europa; sulla base delle dichiarazioni congiunte dell'8 luglio 2016 e del 10 luglio 2018, continuare a far progredire la cooperazione Ue-Nato, in particolare per quanto riguarda i requisiti di interoperabilità della ciberdifesa; sviluppare un'agenda dell'Ue per lo sviluppo delle capacità informatiche esterne al fine di orientare gli sforzi in linea con i suoi orientamenti per lo sviluppo delle capacità informatiche esterne e con l'Agenda 2030 per lo sviluppo sostenibile.

[4] Ad esempio, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardization (CENELEC), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP) e Institute of Electrical and Electronics Engineers (IEEE).

DIBATTITO TEMATICO II - CRIMINALITÀ FINANZIARIA E CORRUZIONE: LA TUTELA DEGLI INTERESSI FINANZIARI DELL'UE

Il **20 luglio 2021** la Commissione europea ha presentato un pacchetto di quattro proposte legislative volto a consolidare le **norme dell'Ue per contrastare il riciclaggio di denaro e il finanziamento del terrorismo** (*Anti-money laundering and countering the financing of terrorism* - Aml/Cft).

Il pacchetto fa parte dell'impegno della Commissione a proteggere i cittadini e il sistema finanziario dell'Ue dal riciclaggio di denaro e dal finanziamento del terrorismo. Obiettivo è migliorare l'individuazione delle operazioni e delle attività sospette e colmare le lacune sfruttate dai criminali per riciclare proventi illeciti o finanziare attività terroristiche attraverso il sistema finanziario.

Come si sottolinea nella strategia dell'Ue per l'Unione della sicurezza per il **periodo 2020-2025**, il consolidamento del quadro normativo dell'Ue in materia di lotta al riciclaggio e al finanziamento del terrorismo contribuirà anche a proteggere i cittadini europei dal **terrorismo** e dalla **criminalità organizzata**.

Il quadro normativo in cui si inseriscono le proposte è costituito da:

- il **Piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo** (C(2020)2800), adottato dalla Commissione nel maggio 2020;
- la **Strategia dell'Ue per l'Unione della sicurezza** (COM(2020)605), del luglio 2020;
- la **Strategia dell'Ue per la lotta alla criminalità organizzata 2021-2025** (COM(2021)170);
- il regolamento (UE) 2018/1805 relativo al **riconoscimento reciproco dei provvedimenti di congelamento e di confisca**;
- la direttiva (UE) 2018/1673 sulla **lotta al riciclaggio mediante il diritto penale**;
- la direttiva (UE) 2019/1153 che reca disposizioni per **agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati**;

- la Procura europea;

La **Procura europea** è stata istituita con il regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»).

L'Eppo ha sede in Lussemburgo (il Procuratore capo è Laura Codruța Kövesi) ed è competente a indagare e a perseguire dinanzi alle ordinarie giurisdizioni nazionali degli Stati partecipanti, e secondo le rispettive regole processuali, i reati che ledono gli interessi finanziari dell'Unione - come definiti dalla direttiva (UE) 2017/1371 relativa alla **lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale** (cd. direttiva PIF) - quali:

- frodi;
- corruzione;
- riciclaggio;
- frodi IVA transfrontaliere.

L'Eppo **è diventata operativa il 1° giugno 2021**. Le istituzioni e gli organi dell'Ue, nonché le autorità competenti dei 22 Stati membri che hanno aderito all'Eppo[5], devono segnalare a quest'ultima qualsiasi condotta criminosa a danno del bilancio dell'Ue (anche le persone fisiche possono segnalare presunti casi di frode e altri reati).

- il Sistema europeo di vigilanza finanziaria.

Il pacchetto di misure proposto dalla Commissione si compone di:

1. un regolamento che istituisce una **nuova autorità dell'Ue in materia di Aml/Cft** (COM(2021)421), che dovrebbe trasformare la vigilanza Aml/Cft nell'Ue e rafforzare la cooperazione fra le Unità di informazione finanziaria (Uif);

La nuova **Autorità antiriciclaggio a livello dell'Ue (Amla)** dovrà fungere da centro di coordinamento delle autorità nazionali, e garantire che il settore privato applichi in modo corretto e coerente le norme dell'Ue. L'Amla dovrà inoltre sostenere le Uif nel loro lavoro per migliorarne la capacità analitica

[5] Austria, Belgio, Bulgaria, Cipro, Croazia, Estonia, Finlandia, Francia, Germania, Grecia, **Italia**, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Repubblica ceca, Romania, Slovacchia, Slovenia e Spagna.

dei flussi illeciti e fare dell'*intelligenc*e finanziaria una fonte di informazioni fondamentale per i servizi di contrasto.

L'Amla dovrà in particolare:

- istituire un unico sistema integrato di vigilanza Aml/Cft in tutta l'Ue, basato su metodologie di vigilanza comuni e sulla convergenza verso standard di vigilanza elevati;
- vigilare direttamente su alcuni degli enti finanziari più rischiosi che operano in un gran numero di Stati membri o richiedono un'azione immediata per far fronte a rischi imminenti;
- monitorare e coordinare gli organismi di vigilanza nazionali responsabili di altri soggetti finanziari e coordinare gli organismi di vigilanza dei soggetti non finanziari;
- sostenere la cooperazione fra le Unità di informazione finanziaria nazionali e facilitare il coordinamento e le analisi congiunte fra di esse, al fine di individuare meglio i flussi finanziari illeciti di natura transfrontaliera.

2. un **regolamento in materia di Aml/Cft** (COM(2021)420), contenente norme direttamente applicabili, anche in relazione all'adeguata verifica della clientela e alla "titolarità effettiva";

La proposta intende istituire **un codice unico dell'Ue in materia di antiriciclaggio e contrasto del finanziamento del terrorismo.** Verranno in tal modo armonizzate le norme Aml/Cft in tutta l'Ue, incluse, ad esempio, disposizioni più specifiche in materia di adeguata verifica della clientela, titolarità effettiva e competenze e compiti delle Unità di informazione finanziaria (Uif). I registri nazionali dei conti bancari saranno collegati, consentendo alle Uif di accedere più rapidamente alle informazioni sui conti bancari e sulle cassette di sicurezza.

La Commissione intende fornire anche alle **autorità di contrasto** l'**accesso a questo sistema**, accelerando le indagini finanziarie e il recupero dei proventi di reato nei casi transfrontalieri. L'accesso alle informazioni finanziarie sarà soggetto alle garanzie della direttiva (UE) 2019/1153 sullo **scambio di informazioni finanziarie**.

3. una **sesta direttiva in materia di Aml/Cft** (COM(2021)423), che intende sostituire la direttiva (UE) 2015/849 (quarta direttiva antiriciclaggio, a sua volta modificata dalla quinta), contenente disposizioni sugli **organismi di**

vigilanza nazionali e le **Unità di informazione finanziaria** negli Stati membri;

4. una revisione del regolamento (UE) 2015/847 sui trasferimenti di fondi ai fini del **tracciamento dei trasferimenti di cripto-attività** (COM(2021)422).

Per quanto concerne il **settore delle cripto-attività** in **materia di Aml/Cft,** la Commissione ricorda che, attualmente, solo alcune categorie di prestatori di servizi per le cripto-attività sono soggette alle norme dell'Ue in materia di Aml/Cft. La riforma proposta intende estendere l'ambito di applicazione di tali norme all'intero settore delle cripto-attività, obbligando tutti i prestatori di servizi all'adeguata verifica della clientela. Le nuove modifiche dovrebbero garantire **la piena tracciabilità dei trasferimenti di cripto-attività, come i Bitcoin**, e consentire di prevenire e individuare il loro possibile impiego a fini di riciclaggio/finanziamento del terrorismo. Saranno inoltre vietati i portafogli anonimi di cripto-attività.

Per la lotta al riciclaggio di denaro, in quanto **fenomeno globale**, la Commissione collabora con i suoi partner internazionali.

Il **Gruppo di azione finanziaria internazionale** (Gafi), garante a livello mondiale della lotta al riciclaggio di denaro e al finanziamento del terrorismo, formula raccomandazioni ai vari paesi. Un paese inserito negli elenchi del Gafi sarà incluso anche in quelli dell'Ue e vi saranno due elenchi dell'Ue - una "lista nera" e una "lista grigia" - che rifletteranno quelli del Gafi. Per ogni paese aggiunto agli elenchi, l'Ue applicherà misure proporzionate ai rischi posti da quel paese. Sulla base di una valutazione autonoma, l'Ue potrà inserire anche paesi non riportati dal Gafi, ma che rappresentino una minaccia per il proprio sistema finanziario.

Costituito nel 1989 in occasione del G7 di Parigi, Gafi è un organismo intergovernativo che ha per scopo l'elaborazione e lo sviluppo di strategie di lotta al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo. Nel 2008, il mandato del Gafi è stato esteso anche al contrasto del finanziamento della proliferazione di armi di distruzione di massa.

Del Gruppo fanno parte 39 membri in rappresentanza di Stati e organizzazioni regionali che corrispondono ai principali centri finanziari internazionali, nonché, come osservatori, i più rilevanti organismi finanziari internazionali e del settore (fra i quali Fmi, Banca mondiale, Ecb, Nazioni Unite, Europol, Egmont).

Nelle relazioni introduttive alle proposte, la Commissione afferma che queste sono coerenti con le modifiche apportate alle raccomandazioni del Gafi, in particolare per quanto riguarda **l'estensione dell'ambito di applicazione delle prescrizioni in materia di Aml/Cft ai fornitori di servizi di attività virtuali** e all'attenuazione dei rischi derivanti dalla loro attività.

Il pacchetto legislativo è al vaglio delle Istituzioni europee. La Commissione spera che l'*iter* legislativo si completi tempestivamente. La futura autorità antiriciclaggio dovrebbe entrare in funzione nel 2024 e iniziare il proprio lavoro di vigilanza diretta poco dopo, quando la direttiva sarà stata recepita e verrà applicato il nuovo quadro normativo.

LA REVISIONE DELLE REGOLE DI PROCEDURA DEL GRUPPO DI CONTROLLO PARLAMENTARE CONGIUNTO DELLE ATTIVITÀ DI EUROPOL (JPSG)

Ai sensi dell'articolo 6.2. delle Regole di procedura del Gruppo di controllo parlamentare congiunto delle attività di Europol (JPSG), e in linea con le raccomandazioni della Conferenza dei Presidenti dei Parlamenti UE riuniti a Bratislava il 23-24 aprile 2017, il JPSG ha il compito di rivedere alcune delle sue regole di procedura **due anni dopo** la prima riunione costitutiva e di presentare le conclusioni di tale riesame alla Presidenza della **Conferenza dei Presidenti** dei Parlamenti dell'Unione Europea.

In particolare, a seguito del processo di revisione avviato nella quarta riunione del JPSG che si è svolta a Bucarest nel febbraio 2019, i Copresidenti del JPSG hanno dichiarato di proporre alla Troika presidenziale del medesimo gruppo l'istituzione di un ***working group*** sulla nomina del rappresentante del Gruppo parlamentare congiunto di controllo della attività di Europol alle riunioni del consiglio di amministrazione di Europol.

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).

Le regole di funzionamento del gruppo di lavoro prevedevano il principio dell'adozione della proposta emendativa per ***consensus***. Il termine del mandato del gruppo di lavoro è stato esteso per consentire la discussione di tali proposte in occasione della riunione del JPSG prevista a Bruxelles nella **seconda metà del 2021**. 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.

La discussione si è incentrata in primo luogo sull'applicazione dell'articolo 14, paragrafo 4, del regolamento (UE) 2016/794[6] istitutivo di Europol, ai sensi del quale il consiglio di amministrazione dell'Agenzia **può invitare** a partecipare alle sue riunioni, in veste di **osservatore** senza diritto di voto, **ogni persona** il cui parere possa essere **rilevante** per le discussioni, compreso, se del caso, un **rappresentante** del Gruppo di controllo parlamentare congiunto.

Allo stato, la disposizione è stata finora attuata per mezzo dell'articolo 5 del regolamento del JSPG che prevede che tale organismo nomini, tra i suoi membri effettivi, **un rappresentante** che ha diritto a partecipare, ai sensi dell'articolo 14, paragrafo 4, del regolamento di Europol e per una **durata determinata** dal JPSG, alle riunioni del consiglio di amministrazione dell'Agenzia in qualità di osservatore senza diritto di voto. Il rappresentante deve riferire al JPSG dopo ogni riunione del consiglio di amministrazione.

La questione è stata oggetto di particolare attenzione del gruppo di lavoro poiché è stata condivisa l'esigenza che, anche nel contesto della partecipazione alle riunioni del Management Board, fosse garantita la ***doppia rappresentanza****, connaturata alla composizione mista del JPSG, mediante il coinvolgimento sia della componente espressione dei* ***Parlamenti nazionali,*** *sia di quella relativa alla delegazione del* ***Parlamento europeo****.*

[6] Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI.

Il *working group* ha altresì affrontato la questione della **clausola di revisione** del regolamento del JPSG.

In particolare, l'opportunità di una previsione che disciplini il **procedimento** di **revisione** del regolamento del JPSG è sorta dall'evidenza che il meccanismo previsto dall'attuale disposizione appare **superato** in quanto è scaduto il termine di due anni in essa contenuto, che si riferiva ad una verifica del primo biennio di attività del Gruppo da sottoporre alla Conferenza dei Presidenti dei Parlamenti dell'UE.

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

Di seguito il testo degli articoli vigenti e le rispettive proposte emendative della Copresidenza, oggetto di discussione alla riunione del JPSG del 25-26 ottobre 2021.

In carattere barrato le parti eliminate dal testo originario, in grassetto le parti aggiunte

Articolo 5:

Rappresentante presso il consiglio di amministrazione di Europol

Il JPSG deve nominare, tra i suoi membri effettivi, un rappresentante che avrà il diritto di partecipare, ai sensi dell'articolo 14 del regolamento Europol e per una durata determinata dal JPSG, alle riunioni del consiglio di amministrazione di Europol in qualità di osservatore senza diritto di voto. Il rappresentante deve riferire per iscritto al JPSG dopo ogni riunione del consiglio di amministrazione sui suoi principali risultati.

Emendamento di compromesso proposto dalla Copresidenza all'articolo 5:

***Rappresentanti* presso il consiglio di amministrazione di Europol**

Il JPSG deve ~~nominare, tra tutti i sui membri, un rappresentante~~ **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 ~~osservatore~~ ***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

Revisione

In linea con le raccomandazioni della Conferenza dei Presidenti dell'UE svoltasi a Bratislava il 23-24 April 2017, il JPSG deve rivedere le sue regole di procedura, due anni dopo la sua riunione costitutiva, e sottoporre le conclusioni di tale revisione alla Presidenza della Conferenza dei Presidenti dei Parlamenti dell'Unione Europea.

Emendamento di compromesso proposto dalla Copresidenza all'articolo 6.2

Revisione

~~In linea con le raccomandazioni della Conferenza dei Presidenti dell'UE svoltasi a Bratislava il 23-24 aprile 2017, il JPSG deve rivedere le sue regole di procedura due anni dopo la sua riunione costitutiva, e sottoporre le conclusioni di tale revisione alla Presidenza della Conferenza dei Presidenti dei Parlamenti dell'Unione Europea~~.

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.

Con **lettera del 20 ottobre 2021**, la **Copresidenza del JPSG**, nella persona di Juan Fernando López Aguilar, Presidente della Commissione per le libertà civili, giustizia e affari interni (LIBE) del Parlamento europeo, Nik Prebil, Capo della delegazione della Assemblea della Repubblica di Slovenia al JPSG e Bojana Potočan, Capo della delegazione del Consiglio nazionale della Slovenia al JPSG, ha comunicato alle delegazioni degli Stati membri che la decisione dell'assemblea plenaria del JPSG segnerebbe la fine delle questioni procedurali in sospeso. **In caso di adozione per consenso** e ai sensi dell'articolo 6.1 del regolamento interno del JPSG, in base al quale il regolamento interno entra in vigore alla data della sua adozione, dopo l'annuncio dei Presidenti gli **emendamenti adottati avrebbero effetto immediato.**

La proposta emendativa di compromesso all'articolo 6 introdurrebbe una nuova disciplina per la revisione delle regole procedurali che, a differenza della precedente, non prevedrebbe un coinvolgimento della Conferenza dei Presidenti dei Parlamenti che pure era stato raccomandato in via provvisoria (ossia per la revisione delle regole dopo due anni dalla prima riunione) dalla Conferenza stessa. Si segnala che nelle regole di procedura delle altre riunioni nell'ambito della cooperazione parlamentare permanente dell'UE (PESC, Governance economica) si prevede che le proposte emendative, oltre a essere adottate per consenso, debbano essere conformi al quadro (framework) definito dalla Conferenza dei Presidenti dei Parlamenti. Si valuti l'opportunità di inserire tale richiamo anche nel nuovo meccanismo di revisione delle regole procedurali del JPSG.