dossier

29 gennaio 2021

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

8ª riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Videoconferenza, 1- 2 febbraio 2021

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

8ª riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

1-2 febbraio 2021

SENATO DELLA REPUBBLICA

SERVIZIO STUDI
DOSSIER EUROPEI

N. 112

CAMERA DEI DEPUTATI

UFFICIO RAPPORTI CON
L'UNIONE EUROPEA

N. 52

Senato della Repubblica

Servizio Studi

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

Dossier europei n. 112

Camera dei deputati

Ufficio rapporti con l'Unione europea

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

Dossier n. 52

INDICE

European Parliament

Assembleia da República

2021PORTUGAL.EU
Parliamentary Dimension

Joint Parliamentary Scrutiny Group on the European Union Agency for Law Enforcement Cooperation (Europol) - 8th meeting

1-2 February 2021, Lisbon

Remote participation

2021PORTUGAL.EU
Parliamentary Dimension

European Parliament

ALL TIME SPECIFICATIONS REFER TO CET

Monday | 1 February 2021

10.00 - 11.30

Troika meeting

(In camera - participation is restricted to Troika Members only)

14.00 - 14.30

Adoption of the agenda and opening remarks

Isabel ONETO, Co-Chair of the JPSG and Head of the Delegation of the Portuguese Assembleia da República to the JPSG

Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Chair of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament

Chairs' announcements reporting on the outcome on the Troika meeting (procedural points)

14.30 - 16.00

Europol activities September 2020 - February 2021

Presentation by Catherine DE BOLLE, Executive Director of Europol

Report by Wojciech WIEWIÓROWSKI, European Data Protection Supervisor

Written Contribution by Oliver RÜß, Chairperson of the Europol Management Board

Written Contribution by Professor Francois PELLEGRINI, Chair of the Europol Cooperation Board

Written report by Kris PEETERS, former Vice-Chair of the EP Delegation to the JPSG on the participation at the Management Board meeting of October 2020

Exchange of views

16.00 - 16.30 **«« Short Break »»**

16.30 - 18.00

Thematic debate I: Cybercrime and digital resilience

Edvardas ŠILERIS, Head of the European Cybercrime Centre at Europol

Pedro VERDELHO, Coordinator of the Cybercrime Office, Portuguese Prosecutor General's Office

Exchange of views

2021PORTUGAL.EU
Parliamentary Dimension

European Parliament

ALL TIME SPECIFICATIONS REFER TO CET

Tuesday | 2 February 2021

9.30 - 11.00

Keynote interventions on the revision and strengthening of the Europol mandate

Ylva JOHANSSON, EU Commissioner for Home Affairs

Eduardo CABRITA, Minister for Home Affairs of the Portuguese Government

MEP (tbd)

Exchange of views

11.15 - 12.45

Thematic debate II: The impact of COVID-19 in the EU's internal security - the role of police cooperation

Speakers:

Catherine DE BOLLE, Executive Director of Europol

Vittorio RIZZI, Deputy Director General of Public Security of Italy, and Co-Chair of the COVID-19 Chiefs of Police Working Group

Exchange of views

Closing remarks by JPSG Co-Chairs

Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Chair of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament

Isabel ONETO, Co-Chair of the JPSG and Head of the Delegation of the Portuguese Assembleia da República to the JPSG

Next meeting: European Parliament, 25-26 October 2021 (TBC)

Schede di lettura

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 Lisbona il 1° e 2 febbraio 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 settembre 2020 e febbraio 2021, con una presentazione da parte della direttrice esecutiva di Europol, Catherine De Bolle.

I lavori dovrebbero proseguire con:

- *un primo dibattito tematico sulla criminalità informatica e sulla resilienza digitale;*
- keynote interventions *di Ylva Johansson, Commissaria europea per gli Affari interni, e di Eduardo Cabrita, ministro degli Affari interni portoghese, sulla revisione e sull'ampliamento del mandato di Europol;*
- *un secondo dibattito tematico in merito all'impatto della COVID-19 sulla sicurezza interna dell'UE e sul ruolo della cooperazione di polizia.*

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

La giornata di lavoro terminerà con le conclusioni e i commenti finali dei due co-Presidenti del Gruppo, Juan Fernando Lȯpez Aguilar, presidente della Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo (LIBE), e Isabel Oneto, capo della delegazione del Parlamento portoghese presso il Gruppo.

La prossima riunione è prevista per il 25 e 26 ottobre 2021 presso il Parlamento europeo.

IL RUOLO DI EUROPOL

Mandato e organizzazione

Entrata in funzione nel 1998 sulla base della Convenzione Europol del 1995 e più volte giuridicamente riformata, da ultimo, con il regolamento n. 2016/794, l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (**Europol**) assiste le autorità degli Stati membri incaricate dell'applicazione della legge fornendo una piattaforma per lo **scambio** e **l'analisi** di informazioni su una serie di attività criminali gravi e a carattere transnazionale.

Il raggio di azione dell'Agenzia, previsto dall'articolo 88, paragrafo, 1, del Trattato sul funzionamento dell'UE (TFUE), ricomprende la prevenzione e la lotta contro la criminalità grave che **interessa due** o **più Stati membri**, il **terrorismo** e le **forme** di **criminalità** che ledono un **interesse comune** oggetto di una **politica dell'Unione**. In particolare, l'allegato I del regolamento citato specifica le tipologie di reato di competenza dell'Agenzia: **terrorismo**, **criminalità organizzata**, traffico di **stupefacenti**, attività di **riciclaggio** del denaro, criminalità nel settore delle materie nucleari e radioattive, organizzazione del **traffico** di **migranti**, tratta di esseri umani, criminalità connessa al traffico di **veicoli rubati**, **omicidio** volontario e lesioni personali gravi, **traffico** illecito di **organi** e tessuti umani, **rapimento**, **sequestro** e presa di ostaggi, **razzismo** e **xenofobia**, **rapina** e **furto** aggravato, traffico illecito di beni culturali, compresi gli oggetti d'antiquariato e le opere d'arte, **truffe** e **frodi**, **reati** contro gli **interessi finanziari dell'Unione**, abuso di informazioni privilegiate e **manipolazione** del **mercato finanziario**, racket ed estorsioni, contraffazione e pirateria in materia di prodotti, **falsificazione** di atti amministrativi e traffico di documenti falsi, **falsificazione** di **monete** e di altri mezzi di **pagamento**, criminalità informatica, corruzione, **traffico** illecito di **armi**, munizioni ed esplosivi, traffico illecito di **specie animali protette**, traffico illecito di specie e di essenze vegetali protette, criminalità ambientale, compreso l'inquinamento provocato dalle navi, traffico illecito di sostanze ormonali e altri fattori di crescita, **abuso** e **sfruttamento sessuale**, compresi materiale **pedopornografico** e adescamento di minori per scopi sessuali, genocidio, crimini contro l'umanità e crimini di guerra.

Con sede a L'Aia (Paesi Bassi), l'Agenzia funge da:

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

Oltre alla raccolta, conservazione, trattamento, analisi e scambio di informazioni, l'Agenzia può sostenere e rafforzare le azioni delle autorità

competenti degli Stati membri svolgendo attività di **coordinamento, organizzazione** e svolgimento di **indagini** e **azioni** operative comuni. Tuttavia, **Europol non applica misure coercitive** nello svolgimento dei suoi compiti, trattandosi di **competenza esclusiva** delle pertinenti **autorità nazionali**.

La struttura amministrativa e di gestione di Europol comprende: un Consiglio di amministrazione; un direttore esecutivo; se del caso, altri organi consultivi istituiti dal Consiglio di amministrazione.

In particolare, il Consiglio di amministrazione è il principale organo di *governance* dell'Agenzia. Esso infatti è chiamato a stabilire gli orientamenti strategici e a verificare l'attuazione dei suoi compiti. Il Consiglio inoltre adotta i programmi di lavoro annuali e pluriennali, nonché il bilancio annuale. Il *board* è composto da un rappresentante per ciascuno Stato membro dell'UE che partecipa al regolamento Europol e da un rappresentante della Commissione europea. La Danimarca ha lo *status* di osservatore. Il Consiglio di amministrazione si riunisce in media quattro volte all'anno.

Principali attività

La funzione di analisi delle attività criminali esercitata da Europol si traduce, tra l'altro, nella pubblicazione dei seguenti documenti periodici di valutazione:

- la **valutazione** della minaccia rappresentata dalla **criminalità organizzata** e dalle forme gravi di criminalità nell'UE (**SOCTA**);
- la **relazione** sulla **situazione** e sulle **tendenze** del **terrorismo** nell'UE (**TE-SAT**), recante un resoconto dettagliato dello stato del terrorismo nell'UE;
- la **relazione annuale dell'Agenzia**, recante in linea di massima mezzi impiegati e risultati riconducibili alle attività di Europol.

L'Agenzia riveste un ruolo centrale per quanto riguarda la condivisione di informazioni tra Stati membri in materia di criminalità. Al riguardo, il quadro giuridico di Europol disciplina le modalità di **interrogazione** della **banca dati** gestita dall'Agenzia (normalmente alimentata da informazioni inserite dalle autorità di contrasto degli Stati membri).

Si ricorda che il Regno Unito, in quanto Paese terzo al di fuori dell'area Schengen, non sarà più membro di Europol, con la quale si prevedono però delle forme di cooperazione già previste per i Paesi terzi.

Nel corso degli anni sono stati costituiti, in seno all'Agenzia, una serie di centri specializzati nell'approfondimento di tipologie criminali ritenute di prioritaria importanza. Sono riconducibili a tali organismi, tra l'altro:

- il **Centro europeo per il *cybercrime*** (**EC3**), costituito nel 2013 per rafforzare la risposta di polizia alle forme di criminalità cibernetiche, con particolare riguardo alla protezione dei cittadini, delle imprese e degli apparati pubblici dai reati *online*;
- il **Centro europeo per il traffico di migranti**, istituito all'inizio del 2016 a seguito della grave crisi dei flussi migratori, concernente in particolare la rotta del Mediterraneo orientale e dei Balcani occidentali. Tale organismo sostiene gli Stati membri nelle attività di individuazione e smantellamento delle reti internazionali che gestiscono i flussi irregolari migratori;
- il **Centro europeo antiterrorismo**, istituito nel 2016, fornisce sostegno operativo richiesto alle autorità degli Stati membri nel settore delle indagini e del contrasto al fenomeno dei *foreign fighters*, delle forme di finanziamento del terrorismo, della propaganda terroristica ed estremistica *online* (avvalendosi della unità *EU Internet Referral Unit*), del traffico illegale di armi, cooperando altresì con le altre autorità antiterroristiche a livello internazionale;
- l'***Internet Referral Unit*** (**EU IRU**), costituita nel 2015 con il compito di ridurre il livello e l'impatto della propaganda *online* che inciti al terrorismo o all'estremismo violento. L'unità collabora a progetti in materia di individuazione e segnalazione di tali contenuti ai fornitori di servizi di Internet (ai fini della rapida cancellazione), sostenendo altresì gli Stati membri nelle analisi operative e strategiche concernenti di tale fenomeno.

Presso Europol sono, infine, istituite l'unità *Intellectual Property Crime Coordinated Coalition* (IPC3) e la rete *Financial Intelligence Units* – FIU.net, volte rispettivamente al contrasto al crimine contro la proprietà intellettuale, e al sostegno alle Unità di Informazione Finanziaria degli Stati membri in materia di riciclaggio e di finanziamento del terrorismo.

IL GRUPPO DI CONTROLLO PARLAMENTARE CONGIUNTO SULLE ATTIVITÀ DI EUROPOL

Dando attuazione a quanto disposto dall'articolo 88, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, con l'approvazione del regolamento (UE) 2016/794, dell'11 maggio 2016, recante il nuovo quadro giuridico di **Europol** è stato introdotto un meccanismo di **controllo** delle **attività** dell'Agenzia da parte del Parlamento europeo in associazione con i Parlamenti nazionali; tale meccanismo si è tradotto nella costituzione del **Gruppo congiunto di controllo parlamentare**, che ha avviato i suoi lavori nel 2017.

In particolare, il Gruppo esercita un **monitoraggio politico** delle attività di Europol nell'adempimento della sua missione, anche per quanto riguarda l'impatto di tali attività sui **diritti** e sulle **libertà fondamentali** delle persone fisiche.

Circa la costituzione del Gruppo:

- ciascun **Parlamento nazionale** (limitatamente agli Stati membri che abbiano aderito al regolamento Europol) deve essere rappresentato da un numero di **membri fino a 4**. Nel caso di Parlamenti bicamerali, ciascuna Camera può nominare fino a **due membri**. Il Parlamento europeo deve essere rappresentato con un numero massimo di **16 membri**;
- il Gruppo è **presieduto congiuntamente** dal Parlamento del Paese che detiene la Presidenza di turno del Consiglio dell'Unione europea e dal Parlamento europeo.

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

Il regolamento Europol disciplina una serie di attività nell'ambito del monitoraggio del Gruppo. In particolare:

a) il **presidente** del Consiglio di amministrazione dell'Agenzia, il **direttore esecutivo** o i loro supplenti compaiono dinanzi al Gruppo, su richiesta di quest'ultimo, per discutere questioni riguardanti le attività dell'Agenzia, compresi gli aspetti di **bilancio** di tali attività, l'**organizzazione strutturale** e l'eventuale istituzione di **nuove unità**

e **centri specializzati**, tenendo conto degli obblighi di segreto e riservatezza. Il Gruppo può decidere di invitare alle sue riunioni altre persone interessate, se del caso;

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

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

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

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

Il Gruppo di controllo parlamentare congiunto può redigere **conclusioni sintetiche** sul monitoraggio politico delle attività di Europol e presentarle al Parlamento europeo e ai Parlamenti nazionali. Il Parlamento europeo le trasmette, a titolo informativo, al Consiglio, alla Commissione e a Europol.

LE ATTIVITÀ DI EUROPOL NEL PERIODO DA SETTEMBRE 2020 A FEBBRAIO 2021

Catherine De Bolle, direttrice esecutiva di Europol, dovrebbe procedere alla presentazione della **Relazione sulle attività di Europol per il periodo settembre 2020 - febbraio 2021**.

In base ai documenti preparatori alla riunione del Gruppo interparlamentare di controllo congiunto, la relazione evidenzia che, nonostante la pandemia di COVID-19 e le relative restrizioni, Europol ha mantenuto un elevato livello di attività. In particolare, nel 2020 il **numero di messaggi scambiati** attraverso l'applicazione di rete per lo scambio sicuro di informazioni (SIENA) - piattaforma per le esigenze di comunicazione delle autorità incaricate dell'applicazione della legge dell'UE - è **aumentato dell'1,8%** e il numero di **nuovi casi avviati**, sempre nello stesso anno, è **aumentato del 4,7%**. Europol è inoltre stata in grado di adattarsi alla pandemia dotando i propri analisti e specialisti con mezzi (i cosiddetti ***Mobile Offices***) finalizzati ad assicurare il flusso di informazioni e l'erogazione di servizi di analisi operativa e strategica. Europol ha introdotto un'applicazione per videoconferenze sicure, che consente lo scambio di dati operativi, accessibile agli Ufficiali di collegamento degli Stati membri. Ciò ha consentito a Europol e alle forze dell'ordine dell'UE di passare, durante la pandemia, a modalità virtuali di cooperazione.

Europol sta pertanto proseguendo le proprie attività di monitoraggio della criminalità organizzata, con particolare riferimento all'impatto della pandemia, negli Stati membri dell'UE, sulla criminalità e sul terrorismo. Viene in proposito segnalato che il 12 novembre 2020 Europol ha co-diretto, insieme alle autorità italiane, la **terza riunione del gruppo di lavoro sulle minacce alla sicurezza dalla diffusione di COVID-19**.

Hanno partecipato alla riunione capi e alti dirigenti della polizia di Austria, Belgio, Francia, Germania, Italia, Paesi Bassi, Polonia, Spagna, Svizzera, Regno Unito, Interpol ed Europol. Basandosi sul lavoro passato, Europol e Italia, copresidenti del gruppo, hanno identificato le due aree di criminalità che destano preoccupazione alla maggior parte dei membri durante la pandemia, vale a dire: 1) lo **sfruttamento sessuale minorile *online***; 2) l'individuazione e il monitoraggio degli indicatori relativi all'infiltrazione di **gruppi criminali organizzati nell'economia legale**.

La quarta riunione del gruppo di lavoro dovrebbe tenersi il **12 febbraio 2021 a Roma**.

PRIMO DIBATTITO TEMATICO: LA CRIMINALITÀ INFORMATICA E LA RESILIENZA DIGITALE

Sono disponibili sul sito di Europol rapporti tematici sull'impatto della COVID-19 sulla criminalità organizzata.

Per quanto concerne in particolare la criminalità informatica, il 3 aprile 2020 è stata pubblicata da Europol la relazione *"Catching the virus cybercrime, disinformation and the COVID-19 pandemic"*.

Europol sta registrando un significativo aumento di casi di illeciti tipicamente connessi alla criminalità informatica. Questi riguardano in particolare:

- le **frodi** negli **acquisti** *online*. Tale tendenza si è manifestata in particolare per quanto riguarda i falsi annunci relativamente a prodotti specifici quali **medicine**, prodotti per l'igiene, *kit* per effettuare i **test** del virus. La COVID-19 ha determinato, in particolare, un rafforzamento dei traffici internazionali per quanto concerne medicine e **mascherine contraffatte**;
- ***phishing*** *(*mail o sms contraffatti, che richiedono di cliccare su un link al fine di raggiungere una pagina web, simile a quella originale, con lo scopo di rubare dati sensibili)***, *smishing*** (falsi messaggi fraudolenti volti a installare file che catturano i dati) e ***ransomware*** (virus volti a criptare dati contenuti in un dispositivo rendendo quasi impossibile il loro recupero). Quest'ultima forma è particolarmente aumentata con riferimento ai dispositivi mobili;
- attacchi a **reti** e sistemi e **violazione di dati.** Europol registra un aumento delle violazioni dei sistemi informatici derivante dall'aumento di vulnerabilità per via del diffondersi del **telelavoro**;
- **la pedopornografia** *online*. Europol ha collegato in particolare l'aumento di attività *online* della rete della pedopornografia (ad esempio, tramite l'invio di messaggi in *forum* e bacheche) alla maggiore vulnerabilità dei minori in situazioni di **isolamento domestico**, di aumento dell'esposizione *online* e di **minor supervisione** da parte degli adulti. In particolare Europol ha registrato un aumento della diffusione in vari Stati membri del materiale pedopornografico (CSAM) mediante le reti *peer to peer* (P2P), già ritenute le piattaforme più usate per tale forma di criminalità. I dati

forniti dalla *Child Rescue Coalition* rilevano un aumento significativo di CSAM in particolare sulle reti P2P in **Italia** e **Spagna**;

- ***streaming* illegale.** Secondo Europol le organizzazioni criminali stanno cercando di trarre vantaggio dalla attuale pandemia espandendo le loro attività nel settore dei **reati** contro la **proprietà intellettuale (PI)**. Ciò sarebbe particolarmente evidente per quanto riguarda le violazioni della proprietà intellettuale legate all'uso illegale della *Internet Protocol Television* (IPTV, il sistema per ricevere segnali televisivi tramite Internet). Secondo Europol, per la natura transnazionale di questa tipologia di crimine, i *server* si trovano spesso in Paesi distinti dagli Stati in cui gli abbonamenti vengono commercializzati, rendendo più difficile per le autorità di contrasto l'individuazione degli effettivi autori del reato. Alcuni gruppi criminali sono riconducibili a reti globali che distribuiscono illecitamente interi pacchetti di contenuti IPTV.

© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

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 i **crimini ad alta tecnologia** e alle **violazioni dei dati**.

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.

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 una delle *cyber* minacce più pericolose al mondo, data la versatilità del suo utilizzo, e punto di riferimento del moderno *malware*;

*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).*

- il **potenziale della minaccia degli attacchi DDoS** (*Distributed Denial of Service*) è maggiore rispetto all'impatto attuale nell'UE.

Politiche dell'UE in materia di *cybersicurezza*

La politica dell'UE volta al contrasto della **criminalità informatica** si concentra su tre principali categorie di illeciti:

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

La prima categoria di illeciti è considerata dall'UE di particolare rilievo, attesa la vitale importanza delle reti e dei sistemi informatici rispetto al funzionamento **delle infrastrutture critiche** (categoria in via di ampliamento, che include il sistema dei **trasporti**, quello **energetico**, le strutture **sanitarie**), 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. In tal senso le sfide in materia di cibersicurezza si estendono al di là delle frontiere nazionali e dell'UE e abbracciano diversi rami del diritto dell'Unione.

Dati statistici

Dai dati in possesso della Commissione europea (illustrati da ultimo nella "Strategia dell'UE in materia di cibersicurezza per il decennio digitale" - JOIN(2020)18) emerge che i dispositivi connessi superano già il numero delle persone sul pianeta e si prevede che il loro numero salirà a **25 miliardi** entro il **2025** di cui **un quarto in Europa**. La digitalizzazione dei modelli di lavoro è stata accelerata dalla pandemia di COVID-19, durante la quale si è registrato un **aumento del 60 per cento** del traffico Internet mentre il 40 per cento dei lavoratori all'interno dell'Unione sarebbe passato al telelavoro, il che si è tradotto, tra l'altro, in un **aumento delle vulnerabilità agli attacchi informatici**.

Secondo la Commissione europea, circa i **due quinti** degli utenti UE avrebbero sperimentato problemi riguardanti la sicurezza, mentre negli ultimi tre anni **un terzo** degli utenti avrebbe ricevuto **e-mail o telefonate fraudolente** in cui si richiedevano dati personali. Secondo quanto riportato dall'ENISA (*European Union Agency for Cybersecurity*), nel terzo trimestre del 2019 si è riscontrato un **aumento** del **241 per cento** del numero totale di **attacchi** distribuiti di negazione di un servizio (DDos) rispetto al terzo trimestre del 2018. Inoltre un'impresa su otto sarebbe stata oggetto di attacchi

informatici. La Commissione europea precisa che oltre la metà dei personal computer aziendali e di consumo, che sono stati infettati da *malware* una volta, vengono reinfettati entro lo stesso anno. Infine centinaia di milioni di *record* di dati vengono persi ogni anno a causa di violazioni dei dati; nel 2018 il costo medio di una violazione nei confronti di una singola impresa è aumentato fino a superare i **3,5 milioni di euro**.

Nel 2019 il numero di incidenti segnalati su base annuale sarebbe triplicato. Si stima che vi siano **700 milioni** di nuovi esemplari di *malware*, il mezzo utilizzato più di frequente per agevolare un attacco informatico. Si stima altresì che nel 2020 il **costo annuale** della criminalità informatica per l'economia mondiale sia stato pari a **5.500 miliardi di euro**, il doppio rispetto al 2015. Esso rappresenterebbe il più ingente trasferimento di ricchezza economica della storia, maggiore anche di quello risultante dal commercio mondiale di sostanze stupefacenti. Per un incidente grave come l'attacco *ransomware WannaCry* del 2017 si stima che il costo per l'economia mondiale sia stato di oltre **6,5 miliardi di euro**.

Da ultimo la Commissione europea ha sottolineato che nel 2019 si sono verificati quasi **450 incidenti** connessi alla cibersicurezza che hanno coinvolto **infrastrutture essenziali** europee come il settore della **finanza** e dell'**energia**, e le **organizzazioni sanitarie.**

La strategia europea in materia di cibersicurezza

L'UE ha recentemente elaborato il nuovo **programma** per rafforzare la politica di contrasto al crimine informatico. In particolare, con la sopra citata comunicazione del 16 dicembre 2020 "La strategia dell'UE in materia di cibersicurezza per il decennio digitale" (JOIN(2020)18) la Commissione europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato un'agenda recante le prossime misure nel settore, che si articolano nei seguenti obiettivi:

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**.

Resilienza e sovranità tecnologica

Tra i punti qualificanti nel primo ambito di intervento, la Commissione:

- propone di rafforzare il regime contenuto nella **direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS) -** direttiva (UE) 2016/1148 **-** per aumentare il livello di ciberresilienza di tutti i settori pertinenti, pubblici e privati, che svolgono una funzione significativa per l'economia e la società;

La direttiva (NIS) è stata introdotta per accrescere la **cooperazione** tra Stati membri sulla questione della cibersicurezza. Essa ha definito **obblighi di sicurezza** per gli **operatori** di **servizi essenziali** (in settori critici come l'energia, i trasporti, la sanità e la finanza) e i **fornitori di servizi digitali** (mercati *online*, motori di ricerca e servizi di *cloud*). Conformemente alla direttiva NIS, ogni Paese dell'UE è tenuto a designare una o più **autorità nazionali**, nonché a elaborare una **strategia** per affrontare le minacce informatiche. La revisione prefigurata nella Strategia è volta a ridurre le incoerenze nel mercato interno **allineando** i requisiti riguardanti l'**ambito di applicazione**, la sicurezza e la **segnalazione** degli incidenti nonché la **vigilanza** e l'applicazione a livello nazionale e le capacità delle **autorità competenti**.

*Il **16 dicembre 2020** la Commissione ha presentato la **proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148** (COM(2020)823).*

*La Commissione ritiene che la direttiva NIS mostri ormai i suoi limiti, e che questi siano stati accentuati dalla rapida trasformazione digitale della società, intensificatasi in seguito alla pandemia. Gli **obiettivi generali del riesame della NIS** sono tre: 1) aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea in tutti i settori rilevanti per economia e società civile; 2) ridurre le incongruenze in termini di resilienza sul mercato interno nei settori già disciplinati dalla direttiva, attraverso un ulteriore allineamento a) dell'ambito di applicazione de facto, b) dei requisiti di sicurezza e segnalazione degli incidenti, c) delle disposizioni che disciplinano la vigilanza e l'attuazione nazionali e d) delle capacità delle autorità competenti negli Stati membri; 3) migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta, adottando misure atte ad aumentare il livello di fiducia tra le autorità competenti, condividendo maggiori informazioni e definendo regole e procedure in caso di incidenti o crisi su vasta scala.*

*La Commissione riferisce che la maggioranza dell'autorità competenti e delle imprese si è mostrata favorevole a una revisione della direttiva NIS. le stime effettuate indicano che l'opzione prescelta può portare a una riduzione pari a **11,3 miliardi di euro** dei costi degli incidenti di cibersicurezza.*

- per assicurare la continuità dei servizi essenziali e il controllo strategico delle **infrastrutture energetiche critiche,** ha

preannunciato l'adozione, entro la fine del 2022, di un "**codice di rete**" volto a stabilire regole per la cibersicurezza dei flussi transfrontalieri di energia elettrica. Inoltre, per la sicurezza delle infrastrutture e dei servizi nell'ambito del futuro programma spaziale, la Commissione europea si è impegnata ad approfondire la strategia per la **cibersicurezza di Galileo** per la prossima generazione di servizi del sistema globale di **navigazione satellitare** e altre nuove componenti del **programma spaziale**;

- propone la creazione di uno **scudo di cibersicurezza** per l'UE, rappresentato da una **rete** di **torri** di **controllo** in grado di rilevare potenziali minacce prima che queste ultime possano causare danni su larga scala. L'infrastruttura dovrebbe poggiare sui preesistenti **centri operativi di sicurezza SOC**.

Si ricorda che un insieme di imprese private, organizzazioni pubbliche e autorità nazionali hanno istituito **gruppi di intervento per la sicurezza informatica** in caso di incidente (CSIRT) e **centri operativi di sicurezza SOC**. Questi ultimi isolano gli eventi sospetti che si verificano sulle reti di comunicazione mediante l'identificazione di segnali e modelli nonché l'estrazione di conoscenza delle minacce da grandi quantità di dati da valutare.

La Commissione intende, da un lato, creare una **rete** di centri operativi per la sicurezza all'interno dell'UE, dall'altro, sostenere la **formazione** e lo **sviluppo** di **competenze** dei lavoratori impegnati in tali ambiti. In particolare essa ha prefigurato uno stanziamento di oltre **300 milioni** di euro a sostegno della cooperazione pubblico-privata e transfrontaliera al fine di creare reti nazionali settoriali che coinvolgano anche le PMI, basate su una *governance* comune e sulla condivisione dei dati e sicurezza. L'obiettivo è migliorare la **velocità** di **rilevamento** degli incidenti, di analisi e di risposta attraverso l'**intelligenza artificiale** e l'apprendimento automatico, integrato da **un'infrastruttura di supercalcolo** sviluppata nell'UE dall'impresa comune per il calcolo ad alte prestazioni europeo.

- ritiene parte significativa della strategia il consolidamento della sicurezza della rete 5G. Si tratta in particolare di completare il processo di rafforzamento che è stato avviato con l'adozione del **pacchetto di strumenti per il 5G**. La Commissione europea ritiene che l'attuale processo debba essere sostenuto garantendo un'ulteriore convergenza negli approcci di attenuazione dei rischi in tutta l'UE, agevolando lo scambio continuo di conoscenze e lo sviluppo di capacità e promuovendo la **resilienza della catena di**

approvvigionamento. Prevede il completamento dell'attuazione del pacchetto di strumenti per il 5G entro il **secondo trimestre del 2021.**

Nel gennaio del 2020 gli Stati membri, tramite il gruppo di cooperazione NIS, hanno adottato un pacchetto di strumenti volti ad affrontare i rischi individuati nella valutazione coordinata a livello dell'UE, compresi i rischi relativi a **fattori non tecnici**, come il rischio di **interferenza da parte di un Paese terzo** o di **soggetti sostenuti da Governi di Paesi terzi** attraverso la catena di approvvigionamento del 5G. In base a tali strumenti gli Stati membri dovrebbero: rafforzare i requisiti di sicurezza per gli operatori delle reti mobili; valutare il **profilo di rischio dei fornitori; applicare restrizioni** ai fornitori considerati ad alto rischio, comprese le necessarie **esclusioni per gli *asset* critici**; garantire che ogni operatore disponga di un'adeguata strategia multifornitore per limitare la dipendenza da un unico fornitore ed evitare la dipendenza da fornitori considerati ad alto rischio.

Nell'ambito degli **obiettivi della resilienza e della sovranità tecnologica** la Strategia prevede anche:

- un'**infrastruttura di comunicazione quantistica** volta ad offrire alle autorità pubbliche una modalità sicura di trasmissione di informazioni, creata con tecnologia europea;
- nuove norme volte a migliorare la cibersicurezza di tutti i prodotti connessi e servizi associati presenti nel mercato interno (compresa la sicurezza informatica dei **veicoli a motore** per tutti i nuovi tipi di veicolo, a decorrere dal luglio 2022). Tali norme potrebbero includere un nuovo obbligo di diligenza da parte dei produttori di dispositivi connessi volto ad affrontare le vulnerabilità del software, compresa la **prosecuzione** degli **aggiornamenti software** e di **sicurezza**, nonché la **garanzia**, alla fine del ciclo di vita, della **cancellazione dei dati personali** e di altri **dati sensibili**;
- lo sviluppo di un **piano di emergenza**, sostenuto da finanziamenti dell'UE, per affrontare scenari estremi che compromettono l'integrità e la disponibilità del sistema root DNS globale e la realizzazione di un **servizio di risoluzione DNS dell'UE** quale alternativa aperta e sicura di accesso a Internet per i cittadini, le imprese e l'amministrazione pubblica dell'UE;
- l'adozione di norme Internet chiave tra cui l'IPv6 e di norme di sicurezza Internet consolidate, nonché di buone pratiche per la sicurezza DNS, del *routing* e della posta elettronica.

  Il DNS (sistema dei nomi di dominio) è il registro utilizzato per la conversione (risoluzione) dei nomi a dominio in indirizzi IP. Il protocollo

DNSSEC (Domain Name System Security Extensions). permette di verificare l’autenticità delle risposte (siti web) del server dei nomi visualizzati. L’IPV6 è uno standard per l’utilizzo di Internet che dovrebbe consentire l’accesso a un numero maggiore di indirizzi.

Secondo la Strategia gli investimenti nell'intera catena di approvvigionamento digitale, che contribuiscono alla transizione digitale o ad affrontare le sfide che ne derivano, dovrebbero ammontare almeno al **20 per cento** pari a **134,5 miliardi di euro**, dei **672,5 miliardi di euro** del dispositivo per la ripresa e la resilienza sotto forma di sovvenzioni e prestiti.

Nell'ambito del quadro finanziario pluriennale 2021-2027 sono previsti finanziamenti dell'UE per la cibersicurezza a titolo del **programma Europa digitale**, nonché per la ricerca sulla cibersicurezza a titolo di **Orizzonte Europa**, con particolare attenzione al sostegno alle PMI, per un totale che potrebbe ammontare complessivamente a 2 miliardi di euro, cui si aggiungeranno gli investimenti degli Stati membri e dell'industria. Parte di questi investimenti dovrebbero tradursi nel contributo del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e rete di centri di coordinamento (CCCN) allo sviluppo della sovranità tecnologica dell'UE in materia di cibersicurezza e nella costruzione di capacità per garantire la sicurezza di infrastrutture sensibili come il 5G, sia ridurre la dipendenza da altre parti del mondo per le tecnologie più importanti.

Capacità operative di prevenzione, dissuasione e risposta

In tale ambito la Commissione mira a potenziare il ruolo dei principali soggetti coinvolti nel contrasto al *cybercrime*: i) autorità NIS, quali i citati CSIRT, e gli organismi di reazione alle catastrofi; ii) autorità giudiziarie e di contrasto; iii) la diplomazia informatica; e iv) la ciberdifesa.

La Commissione europea intende avviare entro febbraio 2021 la realizzazione di **un'unità congiunta per il ciberspazio**, una piattaforma virtuale e fisica di condivisione di competenze reciproche e di mutua assistenza tra le comunità già esistenti, compreso il settore privato.

La strategia per i prossimi dieci anni prevede altresì che l'UE e le autorità nazionali migliorino la capacità delle **forze dell'ordine** di indagare sulla criminalità informatica con particolare attenzione alla lotta contro l'**abuso sessuale *online* dei minori** e alle **indagini digitali**, compresa la criminalità nella "***dark net***".

In tale contesto è previsto:

- un piano d'azione per migliorare la **capacità digitale** degli organismi di contrasto;
- il **contributo di Europol alla definizione di norme forensi** comuni in materia di reati dipendenti e favoriti dall'informatica;
- misure per garantire la corretta attuazione della direttiva 2013/40/UE sulla criminalità informatica.

Si tratta di norme atte ad armonizzare la **criminalizzazione** e le **sanzioni penali** per una serie di **reati** contro i **sistemi informatici**. Tali norme comprendono il divieto di utilizzare le cosiddette **botnet**, **software maligni** progettati per controllare da remoto una rete di computer. La direttiva invita altresì i paesi dell'UE a utilizzare gli stessi punti di contatto utilizzati dal Consiglio d'Europa e dal G8 per reagire rapidamente alle minacce che riguardano la tecnologia avanzata. La direttiva introduce altresì la **responsabilità** delle **persone giuridiche**, stabilendo sanzioni che potrebbero applicarsi qualora si accerti la loro responsabilità.

La strategia prevede altresì il rafforzamento degli strumenti della **diplomazia informatica** dell'UE per prevenire, scoraggiare, dissuadere e rispondere alle attività informatiche dolose.

Si ricorda in particolare il quadro giuridico introdotto nel maggio 2019 in base al quale l'UE ha imposto sanzioni che includono il **divieto di viaggio** e il **congelamento dei beni** e il divieto alle persone ed entità dell'UE di **mettere fondi a disposizione** delle persone ed entità inserite nell'elenco degli individui ritenuti responsabili di *cibercrime*. In tale contesto la strategia prevede che siano valutate **ulteriori opzioni** per **misure restrittive**, nonché il **voto a maggioranza qualificata** in seno al Consiglio per l'inserimento negli elenchi nell'ambito del regime di sanzioni orizzontali contro gli attacchi informatici.

*Il **14 maggio 2020** il Consiglio ha adottato una decisione che proroga per un altro anno, **fino al 18 maggio 2021**, il quadro di **misure restrittive contro gli attacchi informatici** che minacciano l'UE o i suoi Stati membri.*

La strategia prevede altresì:

- una revisione del quadro strategico in materia di **ciberdifesa** concernente l'utilizzo dell'IA, della crittografia e del calcolo quantistico;
- l'ulteriore promozione della cooperazione tra gli Stati membri in materia di ricerca, innovazione e sviluppo delle capacità nel campo della ciberdifesa incoraggiando gli Stati membri a sfruttare appieno il potenziale della cooperazione strutturata permanente (**PESCO**) e del Fondo europeo per la difesa (**FED**);

- un nuovo piano d'azione della Commissione sulle sinergie tra l'**industria** civile, della difesa e dello spazio.

LA REVISIONE E L'AMPLIAMENTO DEL MANDATO DI EUROPOL

Il **9 dicembre 2020** la Commissione europea ha presentato una proposta di modifica al regolamento (UE) 2016/794 volta a **rafforzare il mandato di Europol** (COM(2020)796).

Principali obiettivi della proposta sono i seguenti:

- consentire a Europol di cooperare con **soggetti privati**;

  I terroristi spesso abusano dei servizi forniti da società private per reclutare volontari, compiere attacchi terroristici e diffondere la loro propaganda. Il mandato riveduto dovrebbe consentire ai soggetti privati di riferire tali informazioni direttamente a Europol. L'Agenzia potrebbe quindi: ricevere dati personali direttamente da soggetti privati e analizzarli per identificare tutti gli Stati membri interessati; richiedere dati personali a soggetti privati (tramite lo Stato membro in cui si trova); e fungere da canale per le richieste degli Stati membri ai privati.

- consentire a Europol di sostenere efficacemente le indagini penali degli Stati membri attraverso l'analisi di **serie di dati ampie e complesse** ("*big data*"), rispettando nel contempo il quadro giuridico applicabile;

- rafforzare il ruolo di Europol in materia di **ricerca e innovazione**. Dovrebbero essere ampliati le funzioni di Europol con riferimento allo sviluppo di **nuove tecnologie** per l'applicazione della legge, al fine di contribuire alla dotazione, per le autorità nazionali di contrasto, di mezzi più moderni per combattere i crimini gravi e il terrorismo;

- rafforzare la cooperazione di Europol con i **Paesi terzi** in situazioni specifiche e caso per caso al fine di prevenire e contrastare i reati rientranti nel quadro degli obiettivi di Europol;

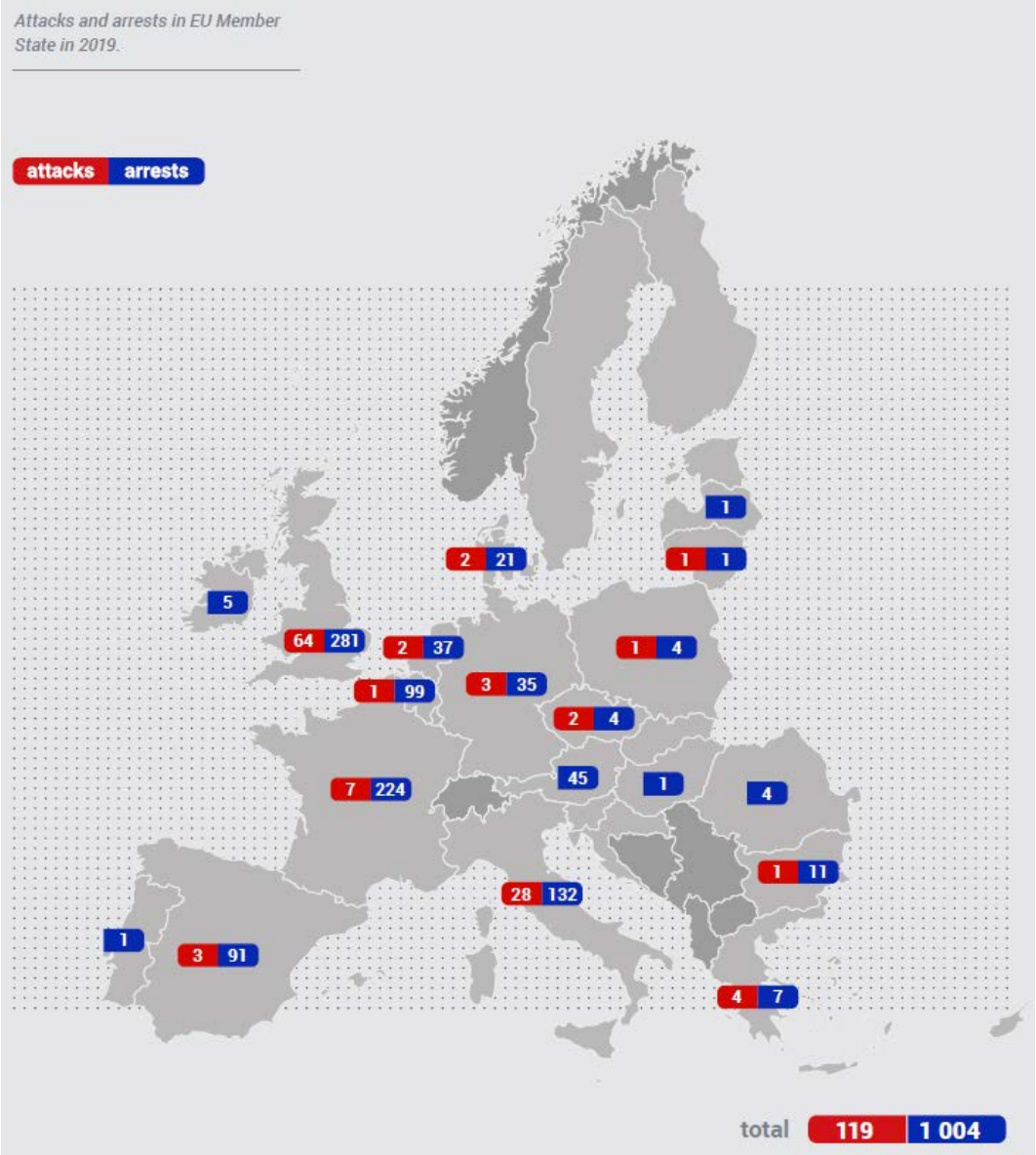
- chiarire che Europol potrà richiedere, nei casi specifici in cui ritenga debba essere avviata un'indagine penale, alle autorità competenti di uno Stato membro di avviare, condurre o coordinare un'indagine su forme di criminalità che ledono un interesse comune oggetto di una politica dell'UE, senza l'obbligo di una **dimensione transfrontaliera** del crimine in questione (Europol potrebbe agire anche come punto focale qualora non sia chiaro quale Stato membro abbia la competenza giurisdizionale);

- rafforzare la cooperazione di Europol con la **Procura europea (EPPO),** anche attraverso il supporto analitico al lavoro della Procura e lo scambio di informazioni, e con **l'Ufficio europeo per la lotta antifrode (OLAF)**;
- rafforzare ulteriormente il quadro per la **protezione dei dati** applicabile a Europol;
- rafforzare ulteriormente il **controllo parlamentare** e la responsabilità di Europol, anche con l'introduzione di nuovi obblighi di comunicazione al Gruppo di controllo parlamentare congiunto incaricato di monitorare le sue attività (art. 51 del regolamento modificato).

La proposta è stata presentata contestualmente alla proposta di modifica del regolamento (UE) 2018/1862 **sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale per quanto riguarda l'inserimento di segnalazioni da parte di Europol** (COM(2020)791).

Nella **relazione del giugno 2020 sul terrorismo** *("European Union Terrorism Situation and Trend report - TE-SAT"*), Europol ha segnalato la presenza di un **alto numero di combattenti terroristi stranieri** di cui **non si sa nulla.** Secondo la relazione, il caos e la mancanza di informazioni dalle zone di conflitto hanno fatto sì che i dati a disposizione degli Stati membri sui combattenti terroristi stranieri siano limitati e non verificabili. Le conclusioni del Consiglio del giugno 2020 sull'azione esterna dell'UE per la prevenzione e la lotta contro il terrorismo e l'estremismo violento hanno in proposito affermato che *"i combattenti terroristi stranieri resteranno un'importante sfida per la sicurezza comune negli anni a venire"*, e hanno espresso l'invito a rafforzare e rendere tempestive **la cooperazione e la condivisione delle informazioni fra Stati membri, con Europol e con altri soggetti rilevanti dell'UE**.

Si segnala infine che il **Consiglio europeo dell'11 e 12 dicembre 2020** ha da ultimo invitato i colegislatori a esaminare la proposta relativa al rafforzamento del **mandato di Europol** in vista della sua rapida adozione; e ha inoltre sottolineato l'importanza generale della **cooperazione giudiziaria e di polizia in tutti i suoi aspetti**.



Secondo le stime di Europol, attualmente **mancano nel SIS informazioni su circa 1.000 combattenti terroristi stranieri di Paesi terzi**, fornite da Paesi terzi fidati a Europol e a singoli Stati membri. Per mettere a disposizione degli Stati membri l'analisi delle informazioni provenienti dai Paesi terzi sui sospetti e i criminali, Europol utilizza i suoi sistemi di informazione e inserisce le informazioni nell'elenco di controllo del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) per i cittadini di Paesi terzi esenti dall'obbligo di possedere un visto al momento dell'attraversamento delle frontiere esterne. Europol può effettuare controlli sulle persone nel SIS, ma non può effettuare segnalazioni nel SIS. La proposta relativa al SIS intende affrontare questa lacuna e si pone l'obiettivo di istituire una nuova categoria di segnalazione specifica per Europol, in

modo da fornire le informazioni direttamente e in tempo reale agli agenti di prima linea. La modifica del regolamento (UE) 2018/1862 dovrebbe pertanto **consentire a Europol** di effettuare **"segnalazioni di informazioni" su sospetti e criminali, come nuova categoria di segnalazioni nel SIS**.

Con la proposta di regolamento modificato, la Commissione propone di consentire a Europol di inserire segnalazioni di informazioni su sospettati e criminali, in particolare combattenti terroristi stranieri, nel sistema d'informazione Schengen in modo che tali informazioni siano accessibili direttamente e in tempo reale agli agenti in prima linea negli Stati membri. In caso di "*hit*", l'allerta informerebbe l'ufficiale in prima linea che Europol detiene informazioni sulla persona.

SECONDO DIBATTITO TEMATICO - L'IMPATTO DELLA COVID-19 SULLA SICUREZZA INTERNA DELL'UE: IL RUOLO DELLA COOPERAZIONE DI POLIZIA

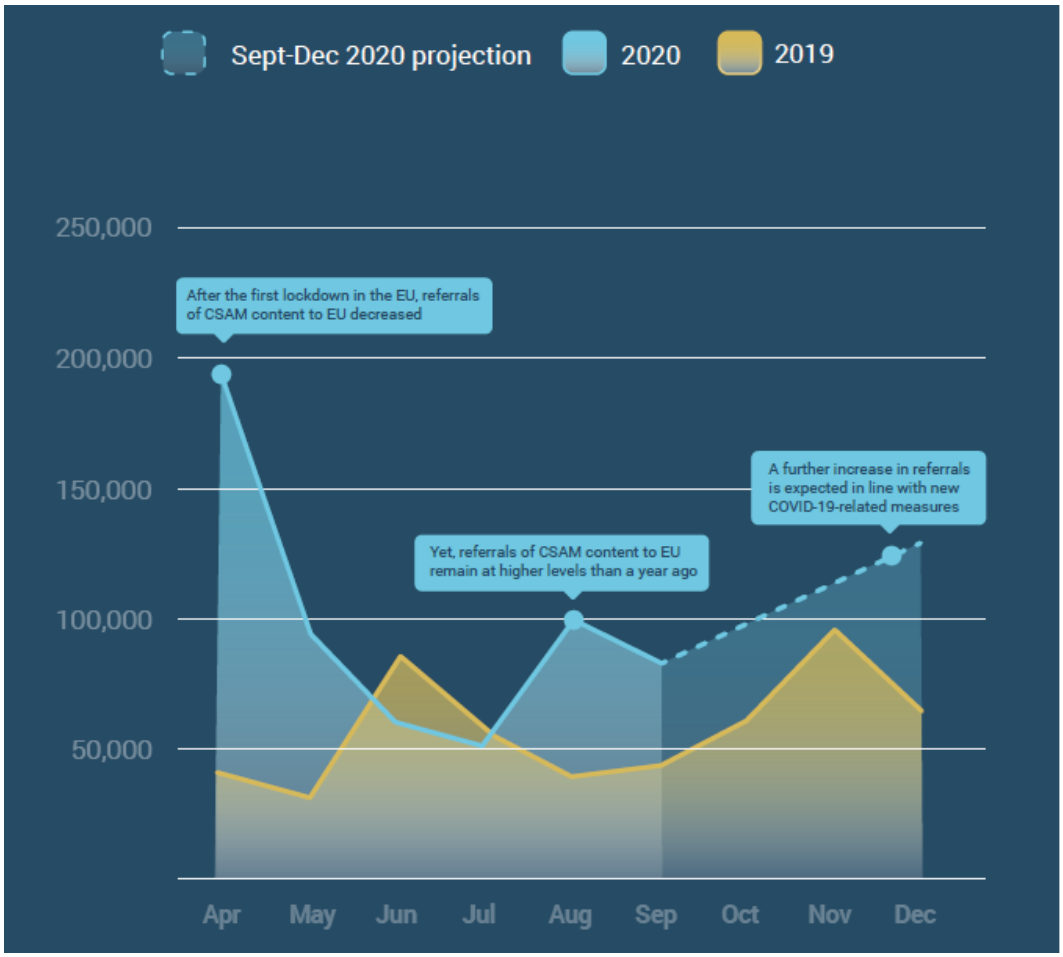
Nella relazione *How COVID-19-related crime infected Europe during 2020*, pubblicata da Europol il 12 novembre 2020, viene posto in evidenza come, sebbene la pandemia di COVID-19 sia prima di tutto una crisi globale per la salute pubblica, questa abbia anche avuto un impatto significativo e potenzialmente di lunga durata sul panorama della criminalità grave e organizzata e del terrorismo in Europa, nonché sulla capacità delle autorità di contrasto degli Stati membri di fronteggiare le minacce alla sicurezza.

In merito all'impatto della COVID-19 sulla sicurezza interna il documento conclude che:

- l'Europa sembra essere nella morsa di una seconda ondata della pandemia di COVID-19. Durante il 2020, l'impatto della COVID-19 sulla criminalità è cambiato nel corso del tempo. Mentre alcuni tipi di reato, correlati in modo specifico al **contesto della pandemia**, continuano a essere presenti, altri evolvono con la diffusione della pandemia e delle misure adottate. Una maggiore consapevolezza ha tuttavia ridotto l'impatto di alcuni tipi di criminalità;
- la distribuzione (*online* e *offline*) di **dispositivi di protezione individuale**, nonché di **prodotti farmaceutici e sanitari contraffatti e scadenti**, fra cui i falsi '*corona home test kits*' " e i presunti vaccini per prevenire l'infezione di COVID-19, continua a essere una delle principali attività criminali correlate alla pandemia;
- il settore del **materiale pedopornografico** (*child sexual abuse material* - CSAM) continua a essere molto preoccupante; con i bambini che trascorrono più tempo *online*, l'aumento della domanda potenziale di CSAM e i tentativi di sfruttamento sessuale dei minori rappresentano una grave minaccia;
- le organizzazioni legate ai **crimini contro il patrimonio** hanno modificato nel corso della pandemia i propri schemi di frode (adottando, fra gli altri, il cd. "trucco del nipote"). Sembrano inoltre essere aumentati i furti nelle strutture mediche e nelle farmacie;
- hanno avuto luogo un'ampia gamma di attività legate **alla criminalità informatica**, comprese campagne di *phishing*, *ransomware*, *malware*

e attacchi volti a compromettere la posta elettronica aziendale. Anche le organizzazioni sanitarie e legate alla salute sono state prese di mira e sono state vittime di attacchi *ransomware*;

- dopo un'iniziale interruzione nella fornitura di droga ad alcuni mercati europei legati al traffico di stupefacenti, nel complesso l'impatto della crisi sul **mercato della droga dell'UE** sembra essere limitato;
- le conseguenze della pandemia sul terrorismo e sull'estremismo violento non sono particolarmente rilevanti, limitandosi principalmente al fatto che alcuni estremisti abbiano adattato le proprie narrazioni e il materiale propagandistico all'argomento COVID-19. Questo sviluppo è stato sempre meno evidente dopo maggio 2020;
- il volume di notizie false, di teorie del complotto e la disinformazione volta a minare la fiducia nelle istituzioni pubbliche è stato considerevole.



NCMEC referrals to EU, April-December, 2019 vs 2020, including projection. Source: NCMEC.

Come riportato sul sito di Eurojust, dall'inizio della pandemia nove agenzie dell'UE (**CEPOL**, **EASO**, **EIGE**, **EMCDDA**, **eu-LISA**, **Eurojust**, **Europol**, **FRA** e **Frontex**), ognuna per le proprie competenze, hanno sostenuto gli Stati membri e le istituzioni europee nell'affrontare le sfide senza precedenti generate dalla diffusione del virus. Gli sforzi individuali e congiunti delle agenzie per affrontare il problema dell'impatto della pandemia sono stati raccolti in un documento congiunto sulle risposte alla COVID-19, discusso il 9 luglio 2020 in una riunione in videoconferenza del presidenti delle agenzie Giustizia e affari interni (GAI).

È stato in particolare rilevato il rapido adattarsi della criminalità organizzata al mutare delle condizioni, nonché il recente aumento dell'**uso di droghe**, della **violenza domestica** e degli **abusi sessuali su minori**. E' stato quindi evidenziato che, al fine di affrontare in modo più efficiente i problemi legati alla protezione dei cittadini e delle loro libertà, è necessario aumentare la cooperazione fra le agenzie nel campo digitale. Pertanto, le forze dell'ordine internazionali dovranno operare con il più alto livello di connettività, sia fisica che virtuale, per garantire la **condivisione delle informazioni nella lotta alla criminalità**.

Per quanto concerne **Europol**, le iniziative da questa adottate durante la crisi comprendono:

- l'introduzione della ***Europol Platform for Experts***, al fine di dotare le forze dell'ordine dei Paesi partner di una piattaforma sicura per la condivisione di informazioni strategiche sulle questioni legate alla pandemia;
- la creazione di un'app di videoconferenza sicura, attraverso la condivisione delle informazioni operative fra gli Stati membri e garantendo, in tal modo, una cooperazione virtuale durante la pandemia;
- la dotazione, per i suoi agenti, gli analisti strategici e gli esperti, di risorse atte a garantire il flusso di informazioni. È stato in tal senso rilevato un aumento dell'1,8% del numero di messaggi SIENA (tramite il sistema di scambio Secure Information Exchange Network Application) scambiati fra gli Stati membri nel 2020.

Infine, fra le più recenti operazioni di Europol si segnalano:

- l'operazione EMMA, una delle più grandi operazioni mai effettuate da Europol, che ha portato allo smantellamento di una rete di telefonia

mobile crittografata - EncroChat - ampiamente utilizzata da gruppi criminali;

- l'Operazione Retrovirus 2020, un'operazione globale per contrastare lo smaltimento illegale di rifiuti sanitari e sanitari; e
- l'Operazione Shield 2020, guidata da Finlandia, Francia, Grecia e Italia, e che ha coinvolto le autorità di contrasto di 27 Paesi, l'OLAF, il *Pharmaceutical Security Institute* e il settore privato. Ha preso di mira il traffico di medicinali contraffatti e utilizzati in modo improprio e di sostanze dopanti.

Da ultimo, si segnala che nel paragrafo della relazione citata sulle prospettive in materia di crimine e terrorismo nel **mondo post pandemico** Europol sottolinea una serie di minacce sul lungo periodo. In primo luogo, la crisi economica globale causata dal Covid potrebbe avere conseguenze simili alla recessione del 2007, in particolare, da un lato, agevolando il **reclutamento** da parte delle organizzazioni criminali delle persone che a causa della pandemia hanno perso il lavoro, aumentando i casi di **corruzione**, **frode** e dei **reati finanziari** in genere.

Infine le **misure restrittive** adottate da tutti gli Stati membri per contrastare la diffusione del virus hanno indirettamente causato una maggiore **esposizione** delle persone alla **propaganda terroristica *online***, e in definitiva al rischio dei processi di **radicalizzazione**, specialmente con riferimento alle persone che hanno sofferto i maggiori danni economici dovuti alla pandemia.