dossier

21 settembre 2018

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

Gruppo di controllo parlamentare congiunto su Europol

Bruxelles, 24-25 settembre 2018

Senato della Repubblica
Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

Gruppo di controllo parlamentare congiunto su Europol

Bruxelles, 24-25 settembre 2018

SENATO DELLA REPUBBLICA	CAMERA DEI DEPUTATI
SERVIZIO STUDI DOSSIER EUROPEI	UFFICIO RAPPORTI CON L'UNIONE EUROPEA
N. 10	N. 4

Senato della Repubblica

Servizio Studi

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

Dossier europei n. 10

Camera dei deputati

Ufficio rapporti con l'Unione europea

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

Dossier n. 4

INDICE

Parliamentary Dimension
Austrian Presidency of the Council of the European Union

European Parliament

REPUBLIC OF AUSTRIA
Parliament

DRAFT AGENDA

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

- 3rd meeting -

24-25 September 2018

European Parliament, Brussels

Room:

24 September 2018: Hemicycle

25 September 2018: PHS 3C50

Background

Article 88 TFEU, as introduced by the Lisbon treaty, provides for a unique form of scrutiny on the functioning of Europol by the European Parliament, together with national Parliaments.

On 11 May 2016, Regulation (EU) 2016/794 of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) was adopted. The new regulation empowered Europol and enabled a joint parliamentary scrutiny by the European Parliament together with national parliaments on it.

The Conference of Speakers of the EU Parliaments adopted conclusions on 24 April 2017 on the establishment of a Europol Joint Parliamentary Scrutiny Group (JPSG) pursuant to Article 51 paragraph 1 of the Europol Regulation and in accordance with Article 9 of Protocol 1 of the Treaty on the European Union, the Treaty on the Functioning of the European Union and the Treaty establishing the European Atomic Energy Community.

According to Article 51 of the Europol Regulation, the JPSG will play an essential role to "politically monitor Europol's activities in fulfilling its mission, including as regards the impact of those activities on the fundamental rights and freedoms of natural persons."

The Conference of Speakers, at its meeting on 24 April 2017 agreed that the JPSG will meet twice a year. In the first half of the year, the JPSG is to meet in the Parliament of the country holding the rotating presidency of the Council of the European Union while, in the second half of the year, the JPSG will hold a meeting in the European Parliament.

In line with the Speakers' Conference conclusions, the constituent meeting of the JPSG, took place in the European Parliament on 9 and 10 October 2017, while the second meeting took place on 18 and 19 March 2018 in Sofia, Bulgaria. At the latter, the Rules of Procedure for the JPSG were adopted.

The tasks and responsibilities of the JPSG are set out in Article 51 of the Regulation (EU) 2016/794, and include inter alia the right to question the Chairperson of the Management Board of Europol, the Executive Director of Europol or their deputies as well as the European Data Protection Supervisor and including the right to be consulted in relation to Europol's multiannual programming and including the right to request relevant documents necessary to the fulfilment of its tasks and including the right to draw up summary conclusions on the political monitoring of Europol's activities.

Background documents

Regulation (EU) 2016/794
Conclusions Speakers conference 23-24 April 2017 - Bratislava
Rules of Procedure JPSG
Multiannual Programming Document Europol
Letter by Mr TSVETANOV following the Europol MB meeting of 4 May 2018
Contribution RU Parliament
Contribution CY Parliament

Monday, 24 September 2018, 15.00 – 18.00 - Room: Hemicycle

15.00 - 15.15 - Adoption of the agenda and opening remarks by the JPSG Co-Chairs

- Claude MORAES, Chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Chair of the EP JPSG delegation;

- Angela LUEGER, Chair of the Committee on Internal Affairs of the Austrian National Council.

15.15 - 15.45 - Presentation of JPSG priorities by Presidential Troika 2018-2019

- Tsvetan TSVETANOV, Chairman of the Committee on Internal Security and Public Order, 44th national Assembly of the Republic of Bulgaria;

- Peter WEIDINGER, Member of the Austrian National Council;

- Oana-Consuela FLOREA, Member of the Chamber of Deputies, Joint Standing Committee of the Chamber of Deputies and the Senate for the exercise of parliamentary control over the activity of the Romanian Intelligence Service (SRI).

15.45 - 17.00 - Europol Draft Multiannual Programming Document 2019-2021

- Presentation and exchange of views with Catherine DE BOLLE, Europol Executive Director;

- Presentation and exchange of views of JPSG written contributions submitted by delegations.

17.00 - 18.00 - Europol Management Board activities March-September 2018

- Exchange of views with Priit PÄRKNA, Chairperson of Europol Management Board;

- Report by Tsvetan TSVETANOV, Chairman of the Committee on Internal Security and Public Order, 44th national Assembly of the Republic of Bulgaria;

Monday, 24 September 2018, 18.00 – 19.30

Reception hosted by the European Parliament

Tuesday, 25 September 2018, 9.30 - 12.30 - Room: PHS 3C50

09.30-10.30 - Protection of fundamental rights and freedoms of natural persons, and in particular the protection of personal data, with regard to Europol's activities

- Presentation and exchange of views with Wojciech WIEWIÓROWSKI, European Data Protection Assistant Supervisor

10.30 - 11.45 - 'Europol's contribution to the fight against financial crime, asset recovery and money laundering'

- Presentation and exchange of views with Maarten RIJSSENBEEK, National Coordinating Prosecutor Terrorist Financing;

- Exchange of views with Catherine DE BOLLE, Europol Executive Director;

11.45 - 12.00 - Key note speech by

- Julian KING, European Commissioner for Security Union

12.00 - 12.30 - Closing remarks by JPSG Co-Chairs:

- Claude MORAES, Chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; Chair of EP JPSG delegation

- Angela LUEGER, Chair of the Committee on Internal Affairs of the Austrian National Council;

Next meeting: Bucharest, Romania (24-25 February 2019).

PREMESSA

ll Gruppo di controllo parlamentare congiunto esercita un monitoraggio politico delle attività di Europol, l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto, nell'adempimento della sua missione, anche per quanto riguarda l'impatto di tali attività sui diritti e sulle libertà fondamentali delle persone fisiche.

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 due volte l'anno, alternativamente nel Parlamento del Paese che detiene la Presidenza di turno del Consiglio dell'UE e nel Parlamento europeo.

La terza riunione del Gruppo rientra tra gli incontri organizzati nell'ambito della dimensione parlamentare del Semestre di Presidenza austriaco del Consiglio dell'Unione europea.

In base alla bozza di programma della riunione, nel pomeriggio del 24 settembre, dopo l'adozione dell'agenda e gli interventi introduttivi dei due Co-presidenti Claude Moraes (Presidente della Commissione per le libertà civili, la giustizia e gli affari interni LIBE del Parlamento europeo), e Angela Lueger (Presidente della Commissione Affari interni del Consiglio nazionale austriaco), sono previsti:

- l'illustrazione, da parte della parte della Trojka presidenziale, delle priorità del Gruppo di controllo per il biennio 2018-2019 (intervengono: il Presidente della Commissione Interni, sicurezza e ordine pubblico della 44° Assemblea della Repubblica di Bulgaria, Tsvetan Tsvetanov, l'onorevole Peter Weidinger, membro del Consiglio nazionale austriaco, e l'onorevole Oana-Consuela Florea, membro della Camera dei deputati rumena e della Commissione permanente congiunta di Camera e Senato rumeni per l'esercizio del controllo sulle attività del Servizio di intelligence rumeni - SRI);
- la presentazione e lo scambio di punti di vista circa la bozza del documento di programmazione pluriennale di Europol 2019-2021 (con l'intervento di Catherine De Bolle, direttore esecutivo di Europol);
- lo scambio di punti vista circa le attività del consiglio di amministrazione di Europol nel periodo marzo - settembre 2018 (con l'intervento del presidente del consiglio di amministrazione di Europol, Priit Pärkna, e la relazione del Presidente della

Commissione Interni, sicurezza e ordine pubblico della 44° Assemblea della Repubblica di Bulgaria, Tsvetan Tsvetanov).

Per la giornata del 25 settembre, la bozza di programma prevede sessioni tematiche rispettivamente concernenti:

- la tutela dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare la protezione dei dati personali, con riferimento alle attività di Europol (con l'intervento di Wojciech Wiewiórowski, supervisore aggiunto del Garante europeo per la protezione dei dati personali);
- il contributo di Europol in materia di contrasto della criminalità finanziaria, recupero dei beni e riciclaggio di denaro (con l'intervento di Maarten Rijssenbeek, procuratore coordinatore nazionale nell'ambito del finanziamento del terrorismo, e di Catherine De Bolle, direttore esecutivo di Europol).

La giornata di lavoro si concluderà con una relazione del Commissario europeo per l'Unione della sicurezza, Julian King, e i commenti finali dei Co-Presidenti del gruppo di controllo, Moraes e Lueger.

Schede di lettura

IL RUOLO DI EUROPOL

Entrato 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**), in sintesi, assiste le autorità degli Stati membri incaricate dell'applicazione della legge fornendo una piattaforma per lo **scambio** e **l'analisi** di ***intelligence*** su una serie di attività criminali gravi e a carattere transnanzionale.

L'Agenzia è altresì prevista dal Trattato sul funzionamento dell'UE, che, all'articolo 88, paragrafo 1, le assegna il compito di sostenere e potenziare l'azione delle autorità di polizia e degli altri servizi incaricati dell'applicazione della legge degli Stati membri e la reciproca collaborazione nella prevenzione e 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**.

Le aree di intervento di Europol (individuate dall'allegato I del regolamento citato) sono: **terrorismo**, **criminalità organizzata**, traffico di **stupefacenti**, attività di **riciclaggio** del denaro, criminalità nel settore delle materie nucleari e radioattive, organizzazione del **traffico** di **migranti**, tratta di esseri umani, criminalità connessa al traffico di **veicoli rubati**, **omicidio** volontario e lesioni personali gravi, **traffico** illecito di **organi** e tessuti umani, **rapimento**, **sequestro** e presa di ostaggi, **razzismo** e **xenofobia**, **rapina** e **furto** aggravato, traffico illecito di beni culturali, compresi gli oggetti d'antiquariato e le opere d'arte, **truffe** e **frodi**, **reati** contro gli **interessi finanziari dell'Unione**, abuso di informazioni privilegiate e **manipolazione** del **mercato finanziario**, racket e estorsioni, contraffazione e pirateria in materia di prodotti, **falsificazione** di atti amministrativi e traffico di documenti falsi, **falsificazione** di **monete** e di altri mezzi di **pagamento**, criminalità informatica, corruzione, **traffico** illecito di **armi**, munizioni ed esplosivi, traffico illecito di **specie animali protette**, traffico illecito di specie e di essenze vegetali protette, criminalità ambientale, compreso l'inquinamento provocato dalle navi, traffico illecito di sostanze ormonali ed altri fattori di crescita, **abuso** e **sfruttamento sessuale**, compresi materiale **pedopornografico** e adescamento di minori per scopi sessuali, genocidio, crimini contro l'umanità e crimini di guerra.

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

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

L'Agenzia, oltre alla raccolta, conservazione, trattamento, analisi e scambio di informazioni, può, tra l'altro, e al fine di sostenere e rafforzare le azioni delle autorità competenti degli Stati membri, **coordinare**, **organizzare** e svolgere **indagini** e **azioni** operative che sono condotte:

i) **congiuntamente** con le autorità competenti degli Stati membri; o

ii) nel quadro di **squadre investigative comuni**, ove opportuno, in collegamento con Eurojust.

In ogni caso, in conformità del TFUE e del diritto derivato dell'UE, **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.

Attualmente l'Agenzia impiega oltre mille persone e oltre 200 ufficiali di collegamento, mentre il budget ha registrato negli anni una costante crescita passando dagli oltre 104 milioni di euro nel 2016, ai circa 120 milioni nel 2017, ai 135 del 2018.

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**), con la quale si individuano e valutano le minacce emergenti, e si descrivono inoltre la struttura dei gruppi della criminalità organizzata e il loro modo di operare, nonché le principali tipologie di crimini che interessano l'UE;
- la **relazione** sulla **situazione** e sulle **tendenze** del **terrorismo** nell'UE (**TE-SAT**), che dà un resoconto dettagliato dello stato del terrorismo nell'UE;
- la **relazione annuale dell'Europol**, che delinea i risultati e le informazioni specifiche sui tipi di funzioni e sui sistemi che Europol ha a sua disposizione e in base ai quali eroga la propria attività, sotto forma di sostegno coordinato per operazioni di polizia in Europa.

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). L'accesso alle informazioni avviene in prima battuta tramite la richiesta di riscontro

(positivo o negativo) di un determinato dato. In caso di riscontro positivo, Europol avvia la procedura tramite cui l'informazione che lo ha generato può essere condivisa, conformemente alla decisione del fornitore (ad esempio un altro Stato membro).

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, in particolare:

- 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 *on line*;
- 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 delle 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 on line (avvalendosi della unità *EU Internet Referral Unit*), del traffico illegale di armi, cooperando altresì con le atre 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 *on line* 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.

Si segnala che, dando attuazione a quanto disposto dall'articolo 88, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, con

l’approvazione del nuovo regolamento 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.

Il nuovo quadro giuridico di Europol ha altresì rafforzato il regime di protezione dei dati oggetto di trattamento dell’Agenzia, con particolare riguardo al ruolo del Garante europeo per la protezione dei dati personali, cui sono stati conferiti significativi poteri di intervento (*vedi infra*).

IL DOCUMENTO DI PROGRAMMAZIONE PLURIENNALE DI EUROPOL

Basandosi sul Regolamento finanziario e sulle linee guida elaborate dalla Commissione europea, il Documento di programmazione di Europol contiene componenti di programmazione pluriennale e annuale per il periodo 2019-2021, accompagnate dall'individuazione - a titolo indicativo - delle risorse di bilancio e di personale necessarie a realizzarle.

La componente pluriennale del Documento si basa in larga parte sulla Strategia 2016-2020, adottata dal Consiglio di amministrazione di Europol il 1° dicembre 2015. Gli obiettivi strategici individuati in quella sede sono stati incorporati tra gli obiettivi e le azioni concrete previste per il triennio.

Nei prossimi tre anni, Europol continuerà a sostenere le autorità di polizia nella loro lotta contro il crimine organizzato e il terrorismo, con una strategia che si sposterà in modo progressivo dall'incremento delle capacità operative alla fornitura di servizi operativi con impatto massimizzato. Il consolidamento delle *capabilities* e della *expertise* si tradurrà in un supporto diretto alle attività investigative degli Stati membri.

Il lavoro di Europol si concentrerà pertanto su due tematiche fondamentali:

- offrire un contributo significativo alla **gestione delle informazioni sul crimine** a livello di Unione europea;
- garantire il **massimo impatto operativo della propria azione di supporto agli Stati membri**.

Il Documento di programmazione si concentra su tre grandi obiettivi, di cui vengono qui fornite, in sintesi, le rispettive modalità di attuazione.

1. **Europol deve trasformarsi nel Centro dell'UE per lo scambio di informazioni in materia criminale, e fornire gli strumenti di accesso e di elaborazione delle informazioni stesse a tutte le autorità di polizia degli Stati membri**.
   La gestione delle informazioni include l'accesso, la raccolta e l'organizzazione di informazioni provenienti da fonti multiple e in formati multipli, al fine di renderle accessibili agli Stati membri. Per ottenere tale scopo, Europol, intende concentrarsi su tre assi:

- **sviluppare le capacità ICT che consentano di massimizzare lo scambio e la disponibilità di informazioni sui reati**, tenendo conto che il nuovo quadro giuridico di Europol sposta l'accento da sistemi e database specifici all'introduzione di un nuovo Concetto per la gestione integrata dei dati (IDMC), incentrato in primis sulle necessità concrete delle autorità di polizia - con un conseguente riposizionamento del focus sui dati stessi, rispetto ai sistemi o ai database destinati a conservarli;
- **garantire uno scambio di informazioni immediato, efficace e ininterrotto.** A tale scopo è già disponibile un Centro informazioni in funzione 24 ore su 24, che consente di massimizzare l'acquisizione, la prima elaborazione e la disponibilità delle informazioni per gli Stati membri. Europol intende altresì lavorare a stretto contatto con gli Stati membri per incrementare la qualità della loro cooperazione, con particolare riferimento alla **qualità delle informazioni scambiate e alla rapidità di reazione** (per esempio, attraverso un maggiore uso del cd. *Universal Message Format*, o UMF);
- **rafforzare in modo strategico i rapporti di cooperazione con i partner**. Europol intende continuare a promuovere e sviluppare ulteriormente la cooperazione con tutte le autorità di polizia competenti, ivi inclusi i servizi doganali e antiterrorismo degli Stati membri. Allo stesso tempo, è decisa a rafforzare ulteriormente i partenariati con i paesi terzi (Stati Uniti, paesi mediterranei, Balcani occidentali, Medio Oriente e paesi nordafricani), attraverso iniziative **che preservino la natura operativa di Europol e la sua funzione di supporto agli Stati membri**. "In considerazione delle sfide globali che l'UE si trova ad affrontare, per esempio nelle aree della cybercriminalità, dell'immigrazione e del terrorismo, la cooperazione con Interpol rimarrà particolarmente rilevante e verrà rafforzata tramite un allineamento più stretto e la predisposizione di azioni strategiche comuni." Analogo rafforzamento, sulla base della complementarità, dovrà essere previsto per quanto concerne **la *partnership* con agenzie dell'UE come Frontex ed Eurojust**.

2. **Europol fornirà supporto operativo ed expertise ai massimi livelli per le indagini effettuate dagli Stati membri, sviluppando e utilizzando un ampio portafoglio di servizi.** Più nel dettaglio, il supporto di Europol si esplicherà:

- per le indagini degli Stati membri nell'area del crimine organizzato, attraverso un particolare impegno nel contrasto ai gruppi gerarchicamente strutturati che operano in aree differenziate (o **gruppi di tipo mafioso**), e nella **lotta contro il traffico di esseri umani** connesso alle migrazioni (attraverso lo European Migrant Smuggling Centre, o EMSC);
- per la lotta alla cybercriminalità, tramite una particolare concentrazione sui reati commessi da gruppi organizzati, specie laddove generino profitti significativi, come le **frodi online**; sui reati che provocano danni gravi alle vittime, come lo **sfruttamento sessuale dei minori online**, e sui reati che colpiscono le infrastrutture critiche e i sistemi di informazione dell'UE;
- nell'area dell'antiterrorismo, tramite un impegno volto a rafforzare e rendere più fluidi la cooperazione e lo scambio di informazioni. Più nel dettaglio, il Centro europeo antiterrorismo (ECTC), operativo all'interno di Europol dal 2016, proseguirà nel suo impegno volto a promuovere e costruire le infrastrutture necessarie per potenziare lo scambio di informazioni e la capacità di fornire un sostegno analitico e operativo alle indagini di maggior portata. **La *Internet Referral Unit* dell'Unione (IRU) sarà utilizzata a fini di contrasto della radicalizzazione online, come la *Financial Intelligence Unit* (FIU.net) e il *Terrorist Finance Tracking Programme* (TFTP) potranno fornire un supporto decisivo nel rafforzare il quadro di intelligence sulle fonti di finanziamento del terrorismo**;
- più in generale, tramite lo sviluppo e la gestione di un supporto analitico di alta qualità e di un portafoglio di capacità operative trasversali e in costante evoluzione.

3. **Europol diverrà un organismo sempre più efficiente, con accordi di governance funzionali e una reputazione positiva.** Come conseguenza del nuovo regolamento, Europol sarà soggetto a una supervisione di nuovo tipo, da parte del Supervisore europeo sulla protezione dei dati (EDPS) e del Joint Parliamentary Scrutiny Group. In linea con la policy dell'Unione europea, l'Agenzia continuerà a potenziare la trasparenza delle sue attività, facilitando l'accesso ai relativi documenti tramite un registro pubblico.

Un capitolo a parte del Documento di programmazione è espressamente dedicato alla **Strategia esterna di Europol per gli anni 2017-2020**, e tiene

conto in particolare del dettato dell'articolo 12 del Regolamento (UE) 2016/794, nel quale viene espressamente prevista la predisposizione di una strategia per i rapporti con i paesi terzi e le organizzazioni internazionali. La Strategia trae altresì fondamento dalla Strategia globale dell'UE per la politica estera e di sicurezza, dalla comunicazione della Commissione su una Agenda europea per la sicurezza e la lotta contro il terrorismo e dalla Agenda europea sulla migrazione.

Gli obiettivi della Strategia esterna di Europol consistono primariamente:

- nell'**ottimizzare i partenariati**, operativi e strategici, assicurando uno scambio efficace di informazioni e rafforzando il proprio ruolo come centro dell'Unione per le informazioni sul crimine;
- nel rafforzare il ruolo di Europol quale **piattaforma privilegiata per la cooperazione internazionale di polizia** contro le minacce connesse alla sicurezza dell'Unione. In tal senso appare particolarmente necessario potenziare ulteriormente la comunità degli ufficiali di collegamento che prestano i loro servizi presso l'Agenzia, e i rispettivi uffici: "lo sviluppo di una rete di ufficiali di collegamento dovrebbe condurre a una cooperazione di polizia migliore e maggiormente coordinata", anche tramite un utilizzo sistematico di SIENA (*Secure Information Exchange Network Application*) e del formato universale per lo scambio di messaggi (UMF);
- nel rafforzare la posizione di Europol all'interno dell'architettura dell'UE per la sicurezza, attraverso una **cooperazione più intensa e continua con la Commissione europea e il Servizio europeo per l'azione esterna (SEAE)**, onde assicurare "uno scambio adeguato di informazioni strategiche, offrire un'analisi congiunta delle minacce che hanno una dimensione sia interna che esterna, e facilitare i contatti con i paesi terzi con i quali Europol non ha ancora avviato una cooperazione;
- nel promuovere Europol quale modello di successo nell'ambito della cooperazione.

Per quanto concerne le priorità dell'azione esterna di Europol, in accordo con le urgenze individuate nei documenti strategici dell'Unione per quanto concerne la sicurezza interna - terrorismo, minacce ibride, cybersicurezza e sicurezza energetica, crimine organizzato e gestione delle frontiere esterne-,

esse si concentreranno in particolare **nelle aree della lotta al crimine organizzato, al cybercrimine e al terrorismo**. Le minacce ibride, infatti, "sono un nuovo fenomeno che deve essere analizzato più a fondo onde definire il ruolo di Europol e l'eventuale sostegno che potrebbe offrire nella lotta contro questa minaccia globale."

Quanto infine ai partner, la Strategia esterna stabilisce che Europol deve puntare a rafforzare ulteriormente il suo partenariato con i paesi terzi, senza limitarsi all'adozione di meri criteri geografici, "poiché per alcune tipologie di reato la prossimità geografica di un partner non può essere l'unico criterio da seguire." Nella Strategia vengono comunque espressamente menzionati gli Stati Uniti, i paesi del Mediterraneo e i Balcani occidentali.

Più nel dettaglio:

- gli **Stati Uniti** rimarranno il partner chiave di Europol, a partire dalle aree principali di interesse comune: terrorismo e cybersicurezza (ma anche crimine organizzato e traffico illegale di migranti);
- i paesi del **Medio Oriente** e del **Nordafrica** rappresentano i soggetti principali con i quali rafforzare il partenariato, con particolare riferimento alla lotta contro il terrorismo e le migrazioni illegali, e in stretto coordinamento con il Servizio europeo di azione esterna;
- anche con i paesi dei **Balcani Occidentali** sarà necessario implementare un modello di cooperazione che peraltro ha già portato a risultati significativi, concentrandosi in particolare sul traffico di migranti, il terrorismo e il crimine organizzato;
- le medesime aree - strategiche per la sicurezza interna ed esterna - richiederebbero una cooperazione molto più stretta con la **Turchia**, la cui definizione è però fortemente legata all'evoluzione dei rapporti tra il paese e l'Unione europea;
- altri paesi con i quali puntare a una cooperazione più strutturata sono India e Pakistan; **Cina** (visto l'impatto della criminalità organizzata cinese nel territorio dell'Unione e l'alto profilo internazionale dei gruppi criminali cinesi); i paesi centro e sudamericani (con particolare riferimento al narcotraffico e ai reati connessi); Israele e la Federazione russa.

Per quanto concerne invece i rapporti con le organizzazioni internazionali, **Interpol** rimarrà ovviamente il principale partner di Europol in un'azione di supporto agli Stati membri e di rafforzamento di una

cooperazione di polizia che operi sull'intero territorio dell'Unione. Europol dovrà però produrre ulteriori sforzi per potenziare la cooperazione con altri organismi internazionali, primo fra tutti la **NATO**, con particolare riferimento ad aree di interesse comune come la lotta al terrorismo e al traffico illegale di migranti.

L'ultimo capitolo del Documento di programmazione è dedicato infine alle **risorse finanziarie e umane per gli anni 2019-2021**, e muove dalla considerazione che, nel corso degli ultimi anni, "a Europol sono state affidate una serie di funzioni completamente nuove come il Centro europeo sul cybercrimine, il Centro europeo sul traffico illegale di migranti, la European Internet Referral Unit (IRU), il Centro europeo antiterrorismo e la già citata FIU.net. Benché siano state messe a disposizione alcune risorse per questi nuovi incarichi, Europol ha dovuto dipendere pesantemente dalla riallocazione interna di personale con mansioni operative e dallo spostamento di taluni incarichi da funzioni di supporto al Dipartimento operazioni."

L'evoluzione costante del ruolo di Europol, legata alle nuove esigenze di sicurezza dell'Unione richiede, secondo quanto rilevato nel Documento, una **revisione continua e complessiva delle necessità dell'Agenzia in termini di risorse umane**, per fronteggiare un ampio ventaglio di sviluppi che attengono, a mero titolo esemplificativo:

- alla prevenzione o reazione ad attacchi di matrice terroristica;
- all'individuazione e soppressione di propaganda online;
- al rafforzamento della pressione sulle reti di trafficanti di esseri umani, da ottenersi anche tramite la **presenza diretta di personale Europol negli hotspot** degli Stati membri più affetti dal fenomeno;
- alla necessità di fornire un miglior supporto centralizzato in termini di informatica forense e di decrittazione;
- a un uso più sistematico dell'intelligence finanziaria nel corso delle indagini;
- allo sviluppo di una maggior capacità di individuare potenziali "vittime", specie per proteggere i bambini dagli abusi e dallo sfruttamento sessuale.

Dopo aver ricordato che, nel precedente Documento di programmazione, era stato previsto un incremento approssimativo di 70 agenti temporanei, poi ridotto a 26 unità, Europol afferma di aver risagomato la sua programmazione tenendo conto dell'approccio molto prudente seguito dall'autorità di bilancio per il 2018, e richiede pertanto, per il triennio 2019-2021, 111 nuovi incarichi, così ripartiti:

- 54 unità per la Direzione operazioni;
- 46 unità per il Dipartimento ICT;
- 11 unità per *governance* e amministrazione.

Analogamente contenuto è l'incremento di bilancio che il Documento prefigura: + 21 milioni nel 2019, per un budget totale di 143,3 milioni che crescerebbe in modo ancor più contenuto nel 2020 (+ 2,8 milioni) e nel 2021 (+5,9 milioni).

LA PROTEZIONE DEI DATI PERSONALI NELL'AMBITO DELLE ATTIVITÀ DI EUROPOL

In considerazione della significativa massa di informazioni (concernenti, tra l'altro, autori, sospetti autori, vittime e testimoni di reato) trattate e scambiate nell'ambito delle attività di Europol (cui partecipano anche autorità di Stati membri e altri soggetti per finalità legate al contrasto del crimine), il rinnovato quadro giuridico[1] dell'Agenzia dedica una sezione specifica (il Capo VI) a una serie di garanzie in materia di protezione dei dati personali.

Tale regime è basato sui principi contenuti nella Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale[2], e sulla raccomandazione n. R(87) del Comitato dei Ministri del medesimo organismo in materia di uso dei dati personali nel settore della polizia.

La disciplina è, inoltre, coerente con quanto stabilito a livello UE dalla direttiva (UE) 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei **dati personali** da parte delle **autorità** competenti a fini di **prevenzione**, **indagine**, **accertamento** e **perseguimento** di **reati** o esecuzione di sanzioni penali nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, nell'ambito di un disegno complessivo di riforma (caratterizzato da elevati standard di protezione armonizzati) che ha previsto anche l'adozione del nuovo **regolamento generale sulla protezione dei dati** (regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)[3].

Europol applica addizionalmente il regolamento (CE) n. 45/2001 sul trattamento dei dati personali da parte delle **Istituzioni** e degli **organismi comunitari**, attualmente in fase di revisione, con particolare riguardo a **dati personali "non operativi**", ovvero non collegati ad indagini penali, come i dati personali relativi ai membri del personale Europol.

In sintesi, il Capo VI del regolamento Europol stabilisce, tra l'altro: i **principi generali** in materia di protezione dei dati personali trattati dall'Agenzia (articolo 28), anche con riferimento a particolari categorie di dati (cosiddetti **dati sensibili**), e di soggetti interessati al trattamento (articolo 30); i termini per la **conservazione** e la **cancellazione** dei dati

[1] Regolamento (Ue) 2016/794,

[2] La Convenzione, approvata a Strasburgo nel 1981, è stata ratificata dall'Italia nel 1997.

[3] II pacchetto normativo, entrato in vigore nel maggio 2016 e diventato applicabili due anni dopo.

(31); le disposizioni che vincolano l'Agenzia a garantire sotto diversi profili la **sicurezza** dei dati (articoli 32 e 33); la **notificazione** di una violazione dei dati personali alle autorità di controllo (articolo 34), e la relativa **comunicazione** (compresi limiti dovuti ad esigenze connesse alla peculiare attività dell'Agenzia di sostegno alle attività di tutela della sicurezza) agli interessati (articolo 35). Disposizioni particolari sono altresì previste con riguardo, tra l'altro, al **diritto di accesso** dell'**interessato** ai propri dati (articolo 36), e ai connessi diritti di **rettifica**, **cancellazione** e limitazione dell'**accesso** ai dati (articolo 37), il cui esercizio è circoscritto in funzione delle citate esigenze di tutela della sicurezza.

La disciplina delinea, inoltre, il quadro delle **responsabilità** in materia di protezione dei dati personali, ripartendole in linea di massima tra **Europol** e gli **Stati membri** (articolo 38) viene altresì individuato tra i membri del personale dell'Agenzia un **responsabile della protezione,** nominato dal consiglio di amministrazione dell'organismo (articolo 41).

Il regime include inoltre un articolato sistema di **vigilanza** sul rispetto delle disposizioni in materia di protezione dei dati personali (articoli 41-45), che coinvolge significativamente il **Garante europeo per la protezione dei dati** personali, e le **autorità di controllo nazionali** (*vedi infra*).

Da ultimo, è previsto un apparato di **mezzi di ricorso** e di **responsabilità** che, in estrema sintesi, prevede il diritto degli interessati a presentare **reclamo** al Garante citato e **ricorso** alla Corte di giustizia dell'UE, nonché il diritto al **risarcimento,** da parte di Europol o dello Stato membro (a seconda dei profili di responsabilità), del **danno** cagionato da un **trattamento illecito** di dati (articoli 47- 50).

La sorveglianza sulla protezione dei dati personali può altresì considerarsi inclusa nel **monitoraggio politico** dal Gruppo di controllo parlamentare congiunto delle attività di Europol anche per quanto riguarda l'impatto sui **diritti** e sulle **libertà fondamentali** delle persone fisiche.[4]

Più approfonditamente, secondo i principi generali (articolo 28), nell'ambito di Europol i dati personali devono essere, tra l'altro:

- trattati in modo **corretto** e **lecito**;

[4] A tal proposito, merita ricordare che il diritto alla protezione dei dati di carattere personale è incluso nella Carta europea dei diritti fondamentali dell'UE (articolo 8) che, a seguito del Trattato di Lisbona, ha assunto il rango di diritto primario dell'Unione. al pari del Trattato sull'Unione europea (TUE) e del Trattato sul funzionamento dell'UE (TFUE).

- raccolti per **finalità determinate**;
- **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esatti** e **aggiornati**;
- **conservati** in una forma che consenta l'**identificazione** degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle loro specifiche finalità;
- trattati in modo tale da garantire un'**adeguata sicurezza** dei dati personali.

Il regolamento, da un lato, consente il trattamento di dati personali relativi a **vittime di reato**, **testimoni** o altre **persone** che possono fornire informazioni riguardanti reati e a persone di età inferiore a diciotto anni **se strettamente necessario** e **proporzionato** per prevenire o combattere forme di criminalità rientranti negli obiettivi di Europol, dall'altro **limita** la facoltà di trattare (mediante procedimenti automatizzati o meno) **dati personali** che rivelino la **razza**, l'origine **etnica**, le **opinioni politiche**, le convinzioni **religiose** o **filosofiche** o l'appartenenza **sindacale**, nonché dati **genetici** o dati relativi alla **salute** e alla **vita sessuale** di un individuo ai casi in cui sia **strettamente necessario** e **proporzionato** per prevenire o combattere forme di criminalità rientranti negli obiettivi di Europol e se tali dati integrano altri dati personali trattati da Europol (regime dei **dati sensibili** - articolo 30).

Oltre alle citate norme sulla **durata della conservazione** dei dati, il regolamento stabilisce una serie di **obblighi** a carico di Europol e (nel caso di trattamento automatizzato) degli Stati membri concernenti misure adeguate per **proteggere** i dati personali. Si tratta, tra l'altro, di misure idonee a garantire: il controllo dell'**accesso alle attrezzature**, il controllo dei **supporti** dei dati, della conservazione dei dati; degli **utilizzatori** dei dati, dell'accesso, della **comunicazione**, dell'**introduzione**, e del **trasporto** dei dati, nonché il **ripristino**, l'**affidabilità** e l'**integrità** delle funzioni dei sistemi (articolo 32). In caso di violazione dei dati personali, Europol è tenuta a notificarla senza giustificato ritardo al Garante europeo per la protezione dei dati personali e alle autorità competenti degli Stati membri, nonché al fornitore dei dati interessato (articolo 34, par. 1).

Vi è inoltre l'obbligo di comunicare all'interessato **violazioni** dei dati suscettibili di lederne gravemente di diritti e le libertà, salvo il caso in cui:

- Europol abbia applicato ai dati personali oggetto della violazione misure tecnologiche di protezione appropriate che rendano i **dati incomprensibili** a chiunque non sia autorizzato ad accedervi;
- Europol abbia **successivamente** adottato misure atte a far sì che i diritti e le libertà dell'interessato **non rischino** più di essere gravemente pregiudicati; oppure
- tale comunicazione richiederebbe sforzi sproporzionati, in particolare, a motivo del numero di casi in questione (in una simile circostanza, si procede invece a una comunicazione pubblica o a una misura simile che informi gli interessati in questione con analoga efficacia).

La comunicazione all'interessato può inoltre essere **rinviata**, **limitata** o **omessa** nel caso in cui ciò costituisca una **misura necessaria**, tenuto debito conto dei legittimi interessi del soggetto in questione:

- per **non compromettere indagini**, inchieste o procedimenti ufficiali o giudiziari;
- per non compromettere la **prevenzione**, l'**indagine**, l'**accertamento** o il **perseguimento di reati** o l'esecuzione di sanzioni penali;
- per proteggere la sicurezza pubblica e nazionale;
- per proteggere i diritti e le libertà di terzi (articolo 35).

L’articolo 36 prevede il **diritto** dell’interessato, a intervalli ragionevoli, di ottenere **informazioni** per sapere se i dati personali che lo riguardano sono trattati da Europol, descrivendo altresì il tipo di informazioni che, in tal caso, l’Agenzia deve fornire (a seguito di apposita domanda all’autorità designata a tal fine nello Stato membro). Tale diritto dell’interessato **non può considerarsi assoluto**, potendo la comunicazione di informazioni essere **rifiutata** o **limitata** ove tale rifiuto o limitazione (tenendo conto dei diritti fondamentali e degli interessi del richiedente) costituisca una **misura necessaria** per:

- consentire il corretto svolgimento dei **compiti di Europol**;
- tutelare la **sicurezza** e l'**ordine pubblico** o prevenire **attività criminali**;
- garantire che nessuna all’**indagine nazionale** sia **compromessa**; oppure

- proteggere i **diritti** e le **libertà di terzi**.

Ove l'interessato abbia avuto accesso ai dati personali che lo riguardano trattati da Europol, ha il diritto di chiederne la **rettifica**, l'i**ntegrazione** o l'**aggiornamento** degli stessi, o ancora la cancellazione nel caso in cui tali dati non siano più necessari per le finalità per le quali sono stati raccolti e successivamente trattati.

L'onere relativo alla rettifica o cancellazione dei dati personali ricade su **Europol** o sugli **Stati membri** a seconda della fonte che li ha forniti. Senza ingiustificato ritardo, e in ogni caso **entro tre mesi** dal ricevimento della domanda, Europol informa per iscritto l'interessato che i dati sono stati **rettificati**, **cancellati**, o **limitati** per quanto riguarda l'accesso; il termine di tre mesi vige anche per quanto riguarda l'**eventuale rifiuto** alle operazioni citate, mediante il quale viene altresì indicata all'interessato la facoltà di proporre **reclamo** al Garante europeo per la protezione dei dati e di proporre **ricorso** giurisdizionale (articolo 37).

La responsabilità della qualità dei dati è attribuita ad Europol dal regolamento con riferimento alle informazioni fornite da Paesi terzi, organizzazioni internazionali, o parti private, o reperiti direttamente da Europol da fonti pubbliche, mentre rimane in capo agli Stati membri quando questi ultimi siano gli stessi fornitori dei dati personali (articolo 38, par. 1).

La disciplina prevede, inoltre, la figura di un **responsabile** della **protezione** dei **dati personali** nominato dal consiglio di amministrazione tra i membri del personale dell'Agenzia, con un mandato di quattro anni rinnovabile fino agli otto complessive, dotato di specifiche garanzie di indipendenza, le cui funzioni sono tra l'altro:

- garantire l'**applicazione** delle disposizioni del regolamento Europol in materia di dati personali;
- garantire che sia mantenuta **traccia** del trasferimento e del **ricevimento** dei dati personali secondo il regolamento citato;
- garantire che gli interessati siano **informati**, su richiesta, dei rispettivi diritti;
- **cooperare** con il **Garante europeo** per la protezione dei dati personali;
- redigere una **relazione annuale** e trasmetterla al consiglio di amministrazione e al Garante citato;
- tenere un **registro** delle **violazioni** dei **dati.**

Da ultimo, oltre al potere di **accesso** a tuti i dati trattati e tutti i locali dell'Agenzia, al responsabile è attribuita la facoltà di **chiedere** ai principali organi direttivi di Europol di **porre rimedio** alle **violazioni** delle regole sulla protezione dei dati, potendo altresì, in caso di diniego, **rivolgersi** direttamente al **Garante** citato (articolo 42)

Il Capo VI del regolamento Europol attribuisce al Garante europeo per la protezione dei dati personali (GEPD - in cooperazione con le autorità

nazionali designate dagli Stati membri) le principali funzioni di sorveglianza circa l'applicazione da parte di Europol del quadro giuridico specifico e di qualsiasi altro atto dell'Unione relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali sul legittimo trattamento dei dati personali nell'ambito delle attività dell'Agenzia.

Il GEPD svolge anzitutto attività consultiva, di propria iniziativa o su richiesta da parte di **Europol**, su qualsiasi argomento circa il trattamento dei dati, anche in via **preventiva** rispetto a **nuovi** tipi di **trattamento** da effettuare (articoli 39 e 43, paragrafo 2, lettera *d)*).

In generale, la disciplina conferisce a tale organismo poteri di **indagine** (anche in assenza di reclamo da parte degli interessati) che il GEPD svolge, tra altro, esercitando il potere di **accesso** a tutti i **dati personali** e informazioni, nonché a tutti i **locali** di Europol.

Nell'ambito delle attività di monitoraggio, il GEPD può, tra l'altro:

- offrire **consulenza** agli interessati sull'esercizio dei loro diritti;
- rivolgersi a Europol in caso di **presunta violazione** delle disposizioni sul trattamento dei dati personali e, all'occorrenza, presentare **proposte** volte a **porvi rimedio**;
- **ordinare** che siano **soddisfatte** le **richieste** di esercizio di determinati diritti (accesso ai dati o modifiche nel trattamento) in relazione ai dati allorché dette richieste siano state respinte in violazione degli articoli 36 e 37;
- ordinare a Europol di effettuare la **rettifica**, la **limitazione** dell'**accesso**, la **cancellazione** o la **distruzione** dei dati personali che sono stati trattati in violazione delle disposizioni sul trattamento dei dati personali e la notificazione di misure ai terzi ai quali tali dati sono stati comunicati;
- **vietare** a titolo provvisorio o definitivo i trattamenti da parte di Europol che violano le disposizioni sul trattamento dei dati personali;
- rivolgersi al Parlamento europeo, al Consiglio e alla Commissione e adire la Corte di giustizia dell'Unione europea alle condizioni previste dal TFUE o intervenire nelle cause dinanzi alla stessa Corte (articolo 43).

La vigilanza del GEPD è svolta in **collaborazione** con le **autorità nazionali designate**, in particolare tramite il **Consiglio di cooperazione**, un forum cui sono attribuite **funzioni consultive** nel quale vengono principalmente discusse questioni di carattere comune e sviluppate **linee guida** e **migliori pratiche** (articolo 45). Da ultimo, si ricorda che le autorità nazionali svolgono la vigilanza sulla liceità del **trasferimento**, **reperimento** e **comunicazione** a Europol di **dati personali** da parte degli **Stati membri** interessati.

Il nuovo regime attribuisce all'interessato lo strumento del reclamo al GEPD ove si ritenga il trattamento dei dati non conforme alle disposizioni del regolamento Europol; su tale reclamo, a seconda dei casi, il GEPD decide autonomamente o in cooperazione con le autorità nazionali designate (articolo 47).

Avverso tali decisioni è possibile ricorrere innanzi alla Corte di giustizia dell'UE (articolo 48).

Infine, l'articolo 50 stabilisce che la persona fisica che subisca un **danno** cagionato da un **trattamento illecito** dei dati ha il diritto di ottenere il **risarcimento** del danno da **Europol**, conformemente all'articolo 340 TFEU, o dallo **Stato membro** in cui si è verificato il fatto generatore del danno, conformemente al diritto nazionale.

L'azione contro Europol è proposta dalle persone fisiche dinanzi alla Corte di giustizia dell'Unione europea, mentre quella contro lo Stato membro è da esse proposta dinanzi all'autorità giurisdizionale competente di tale Stato membro.

Il primo monitoraggio da parte del GEPD sulle attività di Europol

Il Garante europeo sulla protezione dei dati personali ha dato conto delle prime attività di sorveglianza su Europol, nel Rapporto annuale 2017 (presentato nel marzo del 2018). In particolare, nei primi mesi di sorveglianza il GEPD è stato consultato da Europol in merito alle modalità di trattamento dei dati personali nell'ambito di **progetti di analisi operative** dell'Agenzia (volte a sostenere attività di indagini e operazioni di intelligence) in specifici **settori criminali**, ed ha altresì trasmesso all'Agenzia un **parere** circa le **linee guida** da essa provvisoriamente adottate sul concetto di **trattamento integrato dei dati** da parte di Europol.

Inoltre, alla fine del 2017, il GEPD ha condotto la prima **ispezione** presso l'Agenzia che ha riguardato, tra l'altro, il **ciclo di vita** dei dati trattati da Europol, una valutazione dei **sistemi di sicurezza** informatica, il rispetto delle disposizioni in materia di limiti di **conservazione** e di **cancellazione** dei dati.

Il GEPD, nel 2017, ha altresì ricevuto tre richieste d **consultazione preventiva** da parte di Europol, nonché due **reclami**, uno solo dei quali è stato dichiarato ammissibile. Tale reclamo (alla fine del 2017 ancora oggetto di indagine) ha riguardato il diniego di **accesso** ai **dati personali** da parte dell'interessato.

POLITICHE UE IN MATERIA DI SICUREZZA INTERNA: L'ATTUAZIONE DELL'UNIONE DELLA SICUREZZA

L'approccio strategico alle questioni della sicurezza

L'Unione europea ha definito un nuovo quadro strategico per la sua azione nel settore della sicurezza con l'adozione dell'**Agenda europea sulla sicurezza** nell'aprile 2015, prospettando linee di intervento tradotte in specifiche proposte legislative (*v. paragrafi successivi*).

Con la successiva Comunicazione sulla realizzazione dell'**Unione della sicurezza** (aprile 2016), la Commissione europea si è data precise scadenze per la realizzazione delle principali misure di prevenzione e di contrasto ai fenomeni del **terrorismo**, della **criminalità organizzata** e del ***cybercrime***.

Inoltre, per rafforzare l'approccio a tali materie, la Presidenza Juncker della Commissione europea ha creato uno **specifico portafoglio** per **l'Unione della sicurezza** (attribuito al Commissario Julian King) coadiuvato da una *task force* trasversale che abbraccia numerose competenze all'interno dell'Esecutivo europeo, cui è stato attribuito il mandato di garantire l'attuazione delle iniziative previste nei documenti programmatici citati.

I principali temi approfonditi nell'ambito dell'Unione della sicurezza sono:

- la revisione del **quadro penale** europeo in materia di terrorismo, con particolare riguardo al contrasto del fenomeno dei *foreign fighters*;
- una serie di misure volte a sottrarre alle organizzazioni criminali e terroristiche gli **strumenti** necessari alle loro attività (accesso alle **risorse finanziarie**, alle **armi,** utilizzo di Internet e di documenti contraffatti);
- le politiche in materia di prevenzione e contrasto ai processi di radicalizzazione;
- il rafforzamento dei **dispositivi di sicurezza** impiegati nella **gestione delle frontiere interne ed esterne** dell'UE;
- le misure di **prevenzione e contrasto** del ***cybercrime***;
- il miglioramento dei sistemi di **scambio di informazioni** tra autorità di contrasto (polizia e magistratura penale) e di *intelligence* tra Stati membri;

- misure volte a rafforzare la **resilienza** dei possibili **obiettivi** degli attacchi terroristici;
- **dimensione esterna** della lotta contro il terrorismo.

Le principali misure in materia di contrasto al terrorismo

Riforma del quadro penale - Misure volte a ridurre i mezzi impiegati da organizzazioni criminali e terroristiche

Nel corso del 2017, l'Unione europea ha rafforzato le misure per il contrasto del terrorismo, tra l'altro, adottando:

- una direttiva che amplia le fattispecie penali riconducibili ai **reati di terrorismo**, con particolare riguardo al fenomeno dei **combattenti stranieri** (ricomprendendovi i viaggi a fini terroristici; la partecipazione a un addestramento a fini terroristici; la fornitura o la raccolta di capitali, con l'intenzione o la consapevolezza che tali fondi saranno utilizzati per commettere reati di terrorismo e reati connessi);
- una direttiva relativa al controllo dell'**acquisizione e della detenzione di armi,** volta ad impedirne l'accesso ai criminali e ai terroristi, attraverso, tra l'altro, una **maggiore tracciabilità** delle armi da fuoco, il **divieto** dell'uso civile delle armi da **fuoco semiautomatiche** più pericolose, nonché misure più severe riguardo all'acquisizione e alla detenzione delle **armi** da **fuoco** più **pericolose**[5].

  Per completare tale ultima iniziativa, la Commissione ha, altresì, presentato una **raccomandazione** sull'adozione di disposizioni immediate miranti a migliorare la sicurezza delle misure di **esportazione**, **importazione** e **transito** di **armi** da **fuoco**, loro parti e componenti essenziali e munizioni. In tale settore si segnala, altresì, la comunicazione congiunta, recentemente presentata dalla Commissione europea e dall'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, "Elementi per una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni".

  Da ultimo, nell'ambito delle misure volte a neutralizzare gli strumenti impiegati dalle organizzazioni criminali e terroristiche, la Commissione europea ha altresì presentato, nell'aprile del 2018, una proposta di revisione e rafforzamento delle **restrizioni** attualmente previste dal regolamento 98/2013 relativo all'**immissione**

[5] Il relativo decreto legislativo di recepimento (Atto del Governo n. 23) è all'esame delle competenti Commissioni parlamentari. (*il termine per l'espressione del parere scade il 31 luglio 2018*)

sul **mercato** e all'uso di **precursori** di **esplosivi**, recante una serie di misure che limitano l'accesso dei privati a tali sostanze, nonché una proposta di regolamento volto a rafforzare la **sicurezza** delle **carte d'identità** rilasciate ai cittadini dell'Unione e dei **titoli di soggiorno** rilasciati ai cittadini dell'Unione e ai loro familiari. Le due proposte sono tuttora all'esame delle Istituzioni legislative europee.

Si segnala infine la proposta, prefigurata dalla Commissione europea in occasione del Discorso sullo Stato dell'Unione del Presidente Jean-Claude Juncker del 12 settembre 2018, di estendere i compiti della recentemente istituita Procura europea al fine di includervi la lotta contro i reati di terrorismo (la proposta è contenuta nella comunicazione COM(2018)641).

La Procura europea, la cui piena operatività è prevista entro la fine del 2020, è un **ufficio indipendente** dell'Unione europea composto da **magistrati** aventi la competenza di individuare, perseguire e rinviare a giudizio gli autori di **reati** a **danno** del **bilancio** dell'**UE**, come la frode, la corruzione o le gravi frodi transfrontaliere in materia di IVA.

Attualmente **partecipano** alla Procura europea 22 Stati membri dell'UE: Austria, Belgio, Bulgaria, Croazia, Cipro, Repubblica ceca, Estonia, Germania, Grecia, Spagna, Finlandia, Francia, **Italia**, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Romania, Slovenia e Slovacchia.

Il Trattato sul funzionamento dell'Unione europea (TFUE) prevede la possibilità di estendere le competenze di tale organismo allo scopo di includere tra le sue le attribuzioni i **reati gravi** che colpiscono più di uno Stato membro, mediante una decisione presa all'**unanimità** da tutti gli Stati membri partecipanti e dagli altri, previa approvazione del **Parlamento europeo** e previa consultazione della **Commissione**.

Misure per il contrasto al finanziamento del terrorismo

Dando seguito ad un Piano di azione presentato dalla Commissione europea nel 2016, l'Unione europea ha messo in campo una serie di misure che hanno l'obiettivo specifico di contrastare il **finanziamento** del **terrorismo**.

Il Piano prevedeva due principali filoni d'azione:

- iniziative volte ad **individuare** i **terroristi** attraverso i loro **movimenti finanziari** e impedire loro di spostare fondi o altri beni;
- misure dirette allo **smantellamento** delle **fonti** di **entrata** usate dalle organizzazioni terroristiche, in primo luogo colpendo le capacità di raccolta fondi.

Devono ricomprendersi in tale ambito di intervento:

- l'adozione, il 30 maggio 2018, della **V direttiva** sulla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, con l'obiettivo in particolare di migliorare la

trasparenza sulla titolarità delle **società** e dei ***trust***; contrastare i rischi connessi alle **carte prepagate** e alle **valute virtuali**; rafforzare la cooperazione tra le unità di informazione finanziaria; potenziare i controlli sulle operazioni che coinvolgono **paesi terzi** ad alto rischio;

- una proposta di direttiva per perseguire **penalmente** il **riciclaggio** dei proventi di reati, recante norme minime per la definizione dei reati e delle sanzioni connesse al riciclaggio di denaro;

  L'iter della proposta normativa è essenzialmente **concluso** a seguito della posizione del Parlamento europeo definita in **prima lettura** il 12 settembre 2018 sulla base dei precedenti negoziati con il Consiglio.

- una proposta di regolamento volto, in particolare, a rafforzare i **controlli** sul **denaro contante** per coloro che entrano o escono dall'UE con somme in contanti superiori ai 10 mila euro (ferma restando la possibilità di agire anche in caso di somme inferiori laddove si sospettino attività criminose) e migliorare lo scambio di informazioni tra le autorità preposte**;**

  L'iter della proposta normativa è essenzialmente **concluso** a seguito della posizione del Parlamento europeo definita in **prima lettura** il 12 settembre 2018 sulla base dei precedenti negoziati con il Consiglio.

- una proposta di regolamento sul **riconoscimento reciproco** degli ordini di **congelamento** e **confisca** dei proventi di reato;

  L'approvazione della proposta dovrebbe essere posta all'ordine del giorno della Assembla plenaria del Parlamento europeo del 4 ottobre 2018.

- una proposta di regolamento, tuttora all'esame delle Istituzioni legislative europee, relativa all'**importazione** di **beni culturali**;

- una proposta di direttiva recante disposizioni per **agevolare** l'**uso** di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati.

Da ultimo, si ricorda che, in occasione del citato Discorso sullo Stato dell'Unione, la Commissione europea ha presentato nuove iniziative volte a lottare più efficacemente contro il **riciclaggio di denaro** a livello transfrontaliero.

Si tratta in particolare della proposta di regolamento COM(2018)646 diretta a **concentrare** le **competenze** in materia di **antiriciclaggio** in relazione al settore finanziario in seno all' **Autorità bancaria europea** e a rafforzarne il mandato per garantire una vigilanza efficace e coerente sui rischi di riciclaggio di denaro da parte di tutte le autorità pertinenti e la cooperazione e lo scambio di informazioni tra queste autorità. La Commissione europea ha presentato, inoltre, una **strategia** per migliorare lo

scambio di informazioni e la cooperazione tra le **autorità antiriciclaggio** e quelle **prudenziali**, e invitato le autorità europee di vigilanza, e in particolare l'ABE, ad adottare linee guida per aiutare le autorità di vigilanza prudenziale ad integrare gli aspetti relativi all'antiriciclaggio nei loro diversi strumenti e ad assicurare la convergenza in materia di vigilanza (tale strategia è contenuta nella comunicazione COM(2018)645). La Commissione ha, infine, annunciato l'intenzione di incoraggiare la Banca centrale europea a concludere con le autorità di vigilanza antiriciclaggio un protocollo d'intesa multilaterale sullo scambio di informazioni entro il 10 gennaio 2019, come previsto dalla disciplina europea antiriciclaggio in vigore.

Misure per la protezione degli obiettivi degli atti terroristici

La Commissione europea sta procedendo in via prioritaria all'attuazione di un Piano di azione, presentato nell'ottobre del 2017, per migliorare la protezione degli spazi pubblici, recante, tra l'altro, lo stanziamento *ad hoc* di risorse finanziarie nell'ambito del bilancio UE.

Si tratta, in particolare, oltre ad iniziative nel campo della cooperazione e dello scambio di *best practicies*, dello stanziamento di **18 milioni** di euro, nell'ambito del **Fondo sicurezza interna,** per sostenere progetti transnazionali volti a migliorare la protezione di tali spazi, e di ulteriori **100 milioni** di euro, previsti nel 2018, nel quadro di **azioni urbane innovative** a sostegno delle città che investono in soluzioni in materia di sicurezza.

La Commissione europea ha contestualmente presentato un Piano d'azione per rafforzare la preparazione contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare (CBRN), che prefigura una serie di misure destinate a ridurre l'**accessibilità** dei materiali CBRN, a eliminare le lacune nelle capacità di **individuare** tali **materiali** e a rafforzare la **preparazione** e la **risposta** agli **incidenti** di tipo CBRN.

Da ultimo, nella quindicesima relazione sull'attuazione dell'Unione della sicurezza, la Commissione europea ha avviato un programma di azioni per migliorare la **sicurezza** dei **passeggeri** del **trasporto ferroviario** nell'UE, che prevede tra le prime iniziative (entro la fine del 2018) l'istituzione di una piattaforma volta a raccogliere **informazioni** pertinenti sulla sicurezza ferroviaria e fornire orientamenti sulle **buone pratiche** per gli Stati membri, e l'elaborazione di un metodo di **valutazione comune** dei rischi.

Radicalizzazione e linguaggio d'odio

Fin dagli attentati terroristici di Londra del 2005, l'UE ha avviato politiche in materia di contrasto alla **radicalizzazione**, basate su un approccio trasversale, che include strumenti sia di tipo **reattivo** (tra i quali il richiamato nuovo quadro giuridico in materia di terrorismo) sia di

carattere preventivo (processi di **integrazione** e **inclusione sociale**, di **reinserimento** e **deradicalizzazione** delle persone considerate a rischio e degli stessi combattenti stranieri che fanno ritorno nei rispettivi Stati membri di provenienza).

Tra gli strumenti di prevenzione adottati a livello di Unione devono ricomprendersi il **Gruppo di esperti di alto livello in materia di radicalizzazione**, la **Rete per la sensibilizzazione alla radicalizzazione** (RAN), il **Forum dell'UE su Internet, la Rete europea per le comunicazioni strategich**e (ESCN) e l'unità **IRU** (*Internet Referral Unit*) istituita in seno ad Europol, l'Agenzia europea per la cooperazione di polizia.

Il **Gruppo di esperti** di alto livello in materia di radicalizzazione è stato istituito dalla Commissione europea nel luglio del 2017 con l'incarico di definire **raccomandazioni** in materia di contrasto e prevenzione del fenomeno con particolare riguardo al coordinamento e alla cooperazione tra tutti i portatori di interesse.

La **RAN**, recentemente rafforzata con l'istituzione al suo interno di un centro di eccellenza, è una **piattaforma** per **scambiare esperienze**, mettere in comune le **conoscenze**, identificare le **migliori pratiche** e sviluppare nuove iniziative per affrontare la radicalizzazione, cui partecipano diversi attori provenienti dagli Stati membri.

Il **Forum dell'UE su internet** riunisce rappresentanti dell'**industria**, degli **Stati membri**, delle autorità di **pubblica sicurezza** e partner della società civile per esaminare il modo in cui affrontare le sfide poste dalla **propaganda terroristica ed estremistica on line** attraverso una cooperazione volontaria rafforzata.

L'IRU ha il compito di **segnalare** ai fornitori di servizi *on-line* interessati i contenuti volti alla **propaganda terroristica o all'estremismo violento** su Internet ai fini della loro rimozione.

Nel quadro degli interventi della Commissione europea per la prevenzione e il contrasto dei contenuti illeciti *on-line* devono ricomprendersi, inoltre, il *Code of conduct* siglato con le principali imprese operanti nel settore dei *social media*, recante l'impegno da parte di queste di eliminare i messaggi illegali di incitamento all'odio (maggio 2016); gli **orientamenti politici** per le **piattaforme *on-line*** al fine di intensificare la lotta contro i contenuti illeciti *on line* in cooperazione con le autorità nazionali (settembre 2017), nonché le raccomandazioni agli Stati membri recanti misure operative volte a garantire maggiore **rapidità nella rilevazione e nella rimozione dei contenuti illegali** *on-line* anche di stampo terroristico o riconducibili a reati di odio (marzo 2018). Nel caso di contenuti **terroristici** la Commissione europea chiede, in particolare, agli

Stati membri la loro **rimozione entro un'ora** dai siti *web*, nonché l'impiego di meccanismi di **rilevazione automatizzata** di tali contenuti.

Da ultimo, si ricorda che, in occasione del citato Discorso sull' Stato dell'Unione la Commissione europea ha presentato nuove regole per **eliminare** rapidamente i **contenuti terroristici** dal web (si tratta della proposta di regolamento COM(2018)640).

La nuova disciplina introduce un **termine vincolante** di un'ora per la **rimozione** dei contenuti di stampo terroristico a seguito di un ordine di rimozione emesso dalle autorità nazionali competenti. Sono altresì previsti: un quadro di **cooperazione rafforzata** tra **prestatori** di servizi di *hosting*, **Stati membri** ed **Europol**, per facilitare l'esecuzione degli ordini di rimozione; meccanismi di **salvaguardia** (reclami e ricorsi giurisdizionali) per proteggere la **libertà di espressione** su Internet e per garantire che siano colpiti esclusivamente i contenuti terroristici; un **apparato sanzionatorio** per i prestatori di servizi nel caso di mancato rispetto (o ancora, di omissione sistematica) degli ordini di rimozione.

Frontiere UE e Spazio Schengen

L'azione europea in tale settore si è anzitutto tradotta in misure volte al **rafforzamento dei controlli alle frontiere esterne**, da un lato, aumentando le verifiche in ingresso e uscita dai confini UE, dall'altro, proponendo nuovi meccanismi automatici di controllo dei transiti dei cittadini di Stati terzi nonché migliorando il **funzionamento** e l'**accesso** ai **sistemi informazione** attualmente utilizzati dalle autorità di contrasto e di gestione delle frontiere.

Tra gli elementi chiave in tale settore, l'approvazione della riforma del **Codice frontiere Schengen** volta a rendere obbligatorie le **verifiche sistematiche** nella banche dati di sicurezza di tutti i viaggiatori, compresi i **cittadini dell'UE** che attraversano le frontiere, misura resasi necessaria tra l'altro in considerazione della significativa componente di cittadini europei (le stime Europol riferiscono un volume assai approssimativo nel 2017, intorno **alle 7 mila persone**) espatriati per aderire alle milizie ISIS.

Il Codice frontiere Schengen è oggetto di un'ulteriore significativa proposta di riforma, tuttora all'esame delle Istituzioni legislative europee, volta ad **ampliare** i **periodi** di **ripristino temporaneo** dei **controlli** di **frontiera** alle **frontiere interne** tra Stati membri.

La proposta, originata da un lato, dall'obiettivo di impedire i movimenti secondari dei migranti, dall'altro dall'intenzione di stringere le maglie dei controlli nei confronti degli spostamenti intra UE di possibili terroristi e *foreign fighters*, è tuttora all'esame delle Istituzioni legislative europee.

L'Italia, confermando riserve già manifestate nei confronti della proposta originaria, in sede di Consiglio dell'UE ha espresso un **giudizio critico** sul testo di compromesso che dovrebbe costituire la base per i prossimi negoziati tra Parlamento europeo e Consiglio e ha dichiarato la propria indisponibilità a sostenere il mandato alla Presidenza del Consiglio per i negoziati con il Parlamento europeo.

Sono molteplici le iniziative europee volte a rafforzare gli strumenti di controllo degli ingressi alle frontiere esterne dell'UE. In tale settore, l'Unione europea ha istituito, alla fine del 2017 un **sistema di ingressi /uscite dell'UE (EES)**[6], volto a consentire la registrazione dei dati di ingresso e uscita dei cittadini dei paesi terzi all'atto di attraversare le frontiere esterne.

Da ultimo, (a seguito dell'approvazione da parte del Parlamento europeo della relativa posizione in prima lettura del 5 luglio 2018), il 5 settembre 2018 il Consiglio ha adottato un regolamento che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), volto a consentire controlli di sicurezza su passeggeri che viaggiano in Europa in regime di **esenzione del visto** prima di arrivare alle frontiere UE.

Si ricorda, infine, che, nel giugno 2018, i colegislatori hanno raggiunto un accordo politico in merito a tre proposte legislative[7] volte a rafforzare il **Sistema d'informazione Schengen (SIS)**, il **principale database** a livello europeo utilizzato dalle autorità di contrasto alla criminalità e di sorveglianza alle frontiere, che l'Unione europea intende migliorare, tra l'altro, mediante l'inserimento nel sistema di alcune categorie di provvedimenti di Stati membri, come ad esempio il **divieto di ingresso** e l'**ordine di rimpatrio** dei cittadini di Stati terzi non legittimati ad entrare e rimanere sul territorio dell'UE. Tale accordo apre la strada all'approvazione del pacchetto sul SIS, che per quanto riguarda la posizione in prima lettura del Parlamento europeo è indicativamente programmata nella sessione plenaria del 22 ottobre 2018.

Scambio di informazioni

L'Unione ha adottato una serie di misure volte a eliminare le **lacune riscontrate in materia di scambio di informazioni** tra autorità di contrasto (polizia e magistratura penale) oltreché tra servizi di *intelligence*, tra le quali:

---

[6] Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011

[7] Si tratta delle proposte di regolamento COM(2016)881, COM(2016)882 e COM(2016)883

- l'aggiornamento del quadro giuridico di Europol, trasformato in Agenza europea con un mandato rafforzato per quanto riguarda l'assistenza alle autorità degli Stati membri nelle attività di **contrasto** delle forme gravi di **criminalità internazionale** e del **terrorismo**;
- la direttiva sui **codici di prenotazione dei viaggi aerei** (codici PNR) da e verso l'Europa (voli extra UE, salva la facoltà per gli Stati membri di applicare la disciplina anche ai voli intra UE)[8].

Il miglioramento della condivisione delle informazioni è alla base altresì di una serie di iniziative europee, tuttora in corso di esame, che interessano, tra l'altro:

- la messa in rete dei **casellari giudiziari** anche con riferimento a cittadini di Stati terzi;
- la cosiddetta **interoperabilità** delle **banche dati europee** impiegate dalle autorità di contrasto e di gestione delle frontiere, che dovrebbe tradursi nella realizzazione di uno **sportello unico** in grado di **interrogare simultaneamente** i molteplici **sistemi di informazione**, potenziato da un **unico sistema di confronto biometrico** al fine di consentire alle autorità competenti di verificare tramite le impronte digitali identità false o multiple;
- il potenziamento di EU-LISA, l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà sicurezza e giustizia (l'iter di tale provvedimento è sostanzialmente concluso);
- il rafforzamento del sistema di informazione visti (VIS), la banca dati dell'UE che collega tra loro le **guardie di frontiera** che operano alle frontiere esterne dell'UE con i **consolati** degli Stati membri in tutto il mondo.

Cybercrime

A partire dal 2013 l'UE ha progressivamente rafforzato le misure volte a contrastare la **criminalità informatica** e gli **attacchi informatici**, con particolare riferimento a 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, etc.) per mezzo di sistemi informatici.

---

[8] Recepita in Italia con il decreto legislativo 21 maggio 2018, n. 53.

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** (tra 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**[9] di alcune tipologie di attacchi informatici.

In tale ambito, l'iniziativa più rilevante è rappresentata dalla **direttiva**, approvata nel luglio 2016, **sulla sicurezza delle reti e dell'informazione** (direttiva NIS)[10], con la quale l'Unione europea ha posto le basi per un miglioramento della **cooperazione operativa** tra Stati membri in caso di specifici incidenti di cibersicurezza e della **condivisione delle informazioni sui rischi**.

Nel settembre 2017 la Commissione europea ha poi presentato un articolato pacchetto di iniziative volte tra le altre cose:

- a rafforzare il quadro giuridico dell'ENISA, l'Agenzia UE per la sicurezza delle reti e dei sistemi informativi, trasformandola in un'**Agenzia europea per la cibersicurezza**, e a istituire un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza dei prodotti e dei servizi TIC nell'Unione;
- a valutare se istituire un **Fondo per la risposta alle emergenze cibernetiche** per gli Stati membri in linea con la normativa europea di settore;
- ad includere la ciberdifesa nel quadro della **cooperazione strutturata permanente** (PESCO) e del **Fondo europeo per la difesa**, a sostegno dei progetti di ciberdifesa;

---

[9] 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. Si ricorda che il **Quadro congiunto per contrastare le minacce ibride** (Join(2016)18), presentato il **6 aprile 2016** dalla Commissione europea e dall'Alta rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, propone un approccio comune e coordinato, sulla base della premessa che la **responsabilità principale ricade sugli Stati membri**. Da ultimo, la comunicazione congiunta "Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride" fa il punto sulle iniziative già avviate e sui prossimi passi a livello europeo per contrastare le minacce ibride

[10] Recepita in Italia con il decreto legislativo 18 maggio 2018, n. 65.

- al rafforzamento della **cooperazione UE NATO** nella **ricerca** in materia di ciberdifesa e cooperazione per l'innovazione, inclusa la partecipazione a **esercitazioni parallele coordinate**;
- alla riforma (tuttora all'esame delle Istituzioni legislative europee) della normativa europea relativa alla lotta contro le **frodi** e le **falsificazioni di mezzi di pagamento** diversi dai contanti.

Da ultimo, nell'aprile del 2018 la Commissione europea ha presentato un pacchetto di proposte legislative volto a migliorare l'**acquisizione transfrontaliera** di **prove elettroniche** per i **procedimenti penali**: una proposta di regolamento relativo agli ordini europei di **produzione** e di **conservazione** di prove elettroniche nei procedimenti penali e una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei **rappresentanti legali** ai fini dell'**acquisizione di prove** nei procedimenti penali.

In proposito, il **Consiglio europeo del 28 e 29 giugno 2018** ha sottolineato la necessità di **rafforzare le capacità contro minacce alla *cybersecurity*** provenienti dall'esterno dell'UE e invitato a dare rapida attuazione alle misure concordate a livello europeo.

Infine, merita segnalare che l'esposizione dei cittadini alla **disinformazione** su **vasta scala** (in particolare le informazioni fuorvianti o palesemente false) è una fattispecie che l'UE considera alla stregua di una tipologia di **minaccia informatica**. In particolare, il tema della propaganda e guerra di informazioni è stato affrontato dall'Unione europea con riferimento alle attività di propaganda di enti e organismi situati in Stati terzi. A tal fine, sono stati adottati strumenti, nell'ambito della **politica estera** e di **sicurezza comune**, volti a contrastare la **falsa propaganda** diffusa da tali soggetti anche, e soprattutto, attraverso la **rete**.

Tra le misure adottate in tale settore, si ricorda l'istituzione della ***Task Force East StratCom***, operativa dal settembre 2015, sotto la responsabilità dell'Alta rappresentante, volta a far fronte alle **campagne di disinformazione** organizzate dalla **Russia**. Tale organismo ha il compito di sviluppare prodotti e campagne di comunicazione incentrate sulla **spiegazione delle politiche dell'UE** nella regione del **partenariato orientale**.

Viene altresì in considerazione la ***Task Force for Outreach and Communication** in the Arab world*, organismo istituito a seguito delle conclusioni del Consiglio dell'UE affari esteri del febbraio 2015, impegnato, tra l'altro, nel sostegno alle iniziative internazionali in materia di **lotta** alla **radicalizzazione** e al **terrorismo**, nella **costruzione di partenariati regionali con l'UE**; nello sviluppo di contro-narrazioni rispetto alla propaganda terroristica; nella promozione dei diritti fondamentali coinvolgendo i social media e nella facilitazione del dialogo interreligioso e con la società civile.

La Commissione europea ha recentemente presentato una **comunicazione** in materia di **contrasto alla disinformazione *on-line***, recante una serie di misure tra le quali si ricordano: la realizzazione di un

codice di buone pratiche dell'UE sul tema della disinformazione, il sostegno a una **rete indipendente** di verificatori di fatti; una politica di **incentivi** al **giornalismo di qualità** e promozione dell'**alfabetizzazione mediatica**.

In proposito, il **Consiglio europeo del 28 e 29 giugno 2018** ha invitato l'Alto rappresentante e la Commissione a presentare entro dicembre 2018, in cooperazione con gli Stati membri e in linea con le conclusioni del Consiglio europeo del marzo 2015, **un piano d'azione con proposte specifiche per una risposta coordinata dell'UE al problema della disinformazione**, comprensivo di mandati appropriati e risorse sufficienti per le pertinenti squadre di comunicazione strategica del Servizio europeo per l'azione esterna (SEAE).

Ai temi della cibersicurezza (anche con particolare riguardo al fenomeno della disinformazione) sono infine riconducibili le iniziative contenute nella comunicazione COM(2018)637, presentata in occasione del citato Discorso sullo Stato dell'Unione.

In particolare, la Commissione europea ha:

- presentato una raccomandazione (C(2018)5949) relativa alle **reti di cooperazione in materia elettorale, alla trasparenza online, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione**.
  Gli Stati membri sono invitati a istituire reti nazionali di cooperazione in materia elettorale composte delle pertinenti autorità - come le autorità competenti in materia elettorale e in materia di cibersicurezza, le autorità incaricate della protezione dei dati e le autorità di contrasto - e a designare punti di contatto che partecipino a un'analoga rete di cooperazione in materia elettorale di livello europeo;
- annunciato la promozione di una maggiore trasparenza nella propaganda politica *online*.
  I partiti politici, le fondazioni politiche e gli organizzatori delle campagne europee e nazionali dovrebbero rendere disponibili le informazioni sulla spesa sostenuta per le campagne di propaganda online, rivelando quale partito o quale gruppo di supporto politico si trovi a monte della propaganda politica online e pubblicando informazioni sui criteri usati per la selezione dei cittadini destinatari di tali comunicazioni. Qualora tali principi non siano seguiti, gli Stati membri dovrebbero applicare sanzioni nazionali;
- invitato le autorità nazionali, i partiti politici e i media ad adottare misure per **proteggere le proprie reti e i propri sistemi informativi dalle minacce** alla cibersicurezza;
- presentato **orientamenti sull'applicazione del diritto dell'Unione in materia di protezione dei dati** volti a aiutare le autorità nazionali e i

partiti politici europei e nazionali ad applicare gli obblighi in materia di protezione dei dati derivanti dal diritto dell'UE nel contesto elettorale (cfr. COM(2018)638);

- proposto la **modifica del regolamento** del 2014 relativo al **finanziamento dei partiti politici europei**, volta a consentire di infliggere sanzioni pecuniarie (pari al 5 % del bilancio annuale del partito politico o fondazione politica europei interessati) per le violazioni delle norme in materia di protezione dei dati commesse allo scopo di influenzare deliberatamente l'esito delle elezioni europee (COM(2018)636);
- annunciato **una proposta di regolamento** per mettere in comune risorse e competenze nella tecnologia di **cibersicurezza** con l'obiettivo di creare una rete di centri di competenza sulla cibersicurezza per coordinare meglio i finanziamenti disponibili per la cooperazione, la ricerca e l'innovazione in tale ambito.