dossier

16 settembre 2019

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

5a riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Bruxelles, 23-24 settembre 2019

Senato della Repubblica
Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

5ª riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Bruxelles, 23-24 settembre 2019

SENATO DELLA REPUBBLICA
SERVIZIO STUDI
DOSSIER EUROPEI
N. 62

CAMERA DEI DEPUTATI
UFFICIO RAPPORTI CON
L'UNIONE EUROPEA
N. 27

Senato della Repubblica

Servizio Studi

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

Dossier europei n. 62

Camera dei deputati

Ufficio rapporti con l'Unione europea

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

Dossier n. 27

INDICE

DRAFT AGENDA

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

- 5th meeting -

23-24 September 2019

European Parliament, Brussels

Room: JAN 4Q2

Version: 13 September 2019

Monday, 23 September 2018, 14.00 – 18.30

14.00 - 14.30 - Adoption of the agenda and opening remarks

- Mr Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the delegation of the European Parliament to the JPSG;

- Ms Mari-Leena TALVITIE, Co-Chair of the JPSG and Head of delegation of the Finnish Parliament to the JPSG;

14.30 - 15.30 - Reporting on Europol activities March - September 2019 and Europol Draft Multiannual Programming Document 2020-2022

- Presentation by Ms Catherine DE BOLLE, Europol Executive Director;

- Presentation of written contributions submitted by delegations (deadline for submission: 4 September 2019);

- Exchange of views;

15.30 - 16.15 - Reporting by the Europol Management Board on activities March - September 2019 with a special focus on the functions listed in article 11 of the Europol Regulation (regulation (EU) 2016/794);

- Presentation by Mr Andrei LINTA, Chairperson of the Europol Management Board;

- Report by Ms Oana FLOREA, Head of the delegation of the Romanian Parliament to the JPSG, former JPSG Co-Chair;

- Exchange of views;

16.15 - 16.45 - Coffee Break

16.45 - 17.30 - JPSG Rules of Procedure - 1st part

- Presentation by the delegations of the tabled amendments;

- Exchange of views;

17.30 - 18.30 - Reporting back by the European Data Protection Supervisor and the Europol Cooperation Board

- Report by Mr Wojciech WIEWIÓROWSKI, Assistant Supervisor to the European Data Protection Supervisor;

- Report by Professor Francois PELLEGRINI, Chair of the Europol Cooperation Board;

- Exchange of views;

Monday, 23 September 2019, 18.45 – 21.00

Reception hosted by the European Parliament

- Opening remarks by Mr Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the delegation of the European Parliament to the JPSG, and by Ms Mari-Leena TALVITIE, Co-Chair of the JPSG and Head of delegation of the Finnish Parliament to the JPSG;

- Speech by the Commissioner for the Security Union, Julian King;

Tuesday, 24 September 2019, 9.00 - 12.30

9.00-9.45 - Keynote speech

- Ms Maria OHISALO, Minister of Interior of Finland;

- Exchange of views;

9.45 - 10.30 - Europol's information management priorities in 2019

- Presentation by Mr Luis DE EUSEBIO RAMOS, Deputy Executive Director of Europol for Capabilities;

- Presentation by Mr Anssi KANGAS, Chief Superintendent, the National Police Board of Finland of the UMF3+ Project[1];

- Exchange of views;

[1] UMF3+ Project description provided by Finland

10.30 - 10.45 - Coffee Break

10.45 - 11.45 - JPSG Rules of Procedure - 2nd part

- Continuation of the exchange of views;

- Possible adoption of the revised JPSG Rules of Procedure;

11.45 - 12.15 - Designation of the JPSG representative to the meetings of the Europol Management Board

- Exchange of views;

- Decision on the JPSG representative;

12.15 - 12.30 - Closing remarks by JPSG Co-Chairs:

- Mr Juan Fernando LÓPEZ AGUILAR, Co-Chair of the JPSG and Head of the delegation of the European Parliament to the JPSG;

- Ms Mari-Leena TALVITIE, Co-Chair of the JPSG and Head of delegation of the Finnish Parliament to the JPSG;

Next meeting: Zagreb, Croatia, 22 - 23 March 2020 (TBC)

Schede di lettura

IL RUOLO DI EUROPOL

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, 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 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 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.

Attualmente l'Agenzia impiega circa milletrecento persone e circa 250 ufficiali di collegamento, mentre il budget 2019 si è attestato a 138,3 milioni di euro. Sono circa 90 le persone dello staff di Europol fornite dall'Italia.

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).

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* (*vedi infra*);
- 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 *online* (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 *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, ove 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.

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

In considerazione della significativa massa di informazioni trattate e scambiate nell'ambito delle attività di Europol (cui partecipano autorità di Stati membri per finalità legate al contrasto del crimine), il rinnovato quadro giuridico dell'Agenzia include un apparato di disposizioni a tutela dei dati personali.

Tale regime, previsto al capo VI del richiamato regolamento (UE) 2016/794 (regolamento Europol), si basa sui principi contenuti nella Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale[1], 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)[2].

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 (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 i limiti dovuti ad esigenze connesse

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

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

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 di 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.[3]

Il regolamento prevede, tra l'altro, la figura di un **responsabile** della **protezione** dei **dati personali** nominato dal consiglio di amministrazione tra

[3] 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).

i membri del personale dell'Agenzia, dotato di specifiche garanzie di indipendenza, con il compito, tra l'altro di:

- garantire l'**applicazione** delle disposizioni del regolamento Europol in materia di dati personali;
- **cooperare** con il **Garante europeo** per la protezione dei dati personali;
- tenere un **registro** delle **violazioni** dei **dati.**

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 sul legittimo trattamento dei dati personali nell'ambito delle attività dell'Agenzia.

Oltre ad un ruolo di tipo consultivo (di propria iniziativa o su richiesta di **Europol**, anche in via **preventiva**, rispetto a **nuovi** tipi di **trattamento** da effettuare), la disciplina conferisce a tale organismo poteri di **indagine** 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.

Il GEPD può, tra l'altro:

- **ordinare** che siano **soddisfatte** le **richieste** di esercizio di determinati diritti (accesso ai dati o modifiche nel trattamento);
- 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 dell'UE e alla Commissione europea 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.

L'EUROPOL TRAVEL INTELLIGENCE CENTRE (ETIC)

In linea con il documento di programmazione 2018-2020, si prevede nel corso del 2019 l'istituzione all'interno di Europol di un organismo specializzato per il sostegno agli Stati membri per quanto riguarda l'uso operativo e strategico delle informazioni e dell'intelligence in materia di **viaggi** forniti in base ai **codici di prenotazione** (PNR), dalle **informazioni anticipate** dei passeggeri (Advanced passengers information –API) e dal Sistema europeo di informazione e autorizzazione ai viaggi (**ETIAS**).

I dati del codice di prenotazione (PNR) sono **informazioni personali** fornite dai passeggeri che vengono raccolte e conservate dai vettori aerei. Il PNR contiene informazioni quali il nome del passeggero, la data di viaggio, l'itinerario, il posto assegnato, i bagagli, i dati di contatto e le modalità di pagamento. Le API sono **dati anagrafici** (nome, luogo di nascita e cittadinanza dell'interessato, numero e data di scadenza del passaporto) e hanno una portata più limitata rispetto ai dati PNR; esse sono trasmesse dai vettori su richiesta delle autorità competenti per effettuare controlli sulle persone al momento dell'ingresso alle frontiere esterne di uno Stato membro Schengen. L'ETIAS è il **sistema informatico automatizzato** concepito per individuare qualsiasi rischio di migrazione irregolare e minaccia alla sicurezza rappresentato da visitatori **esenti dall'obbligo del visto** che si recano nello spazio Schengen

Secondo la direttiva (UE) n. 2016/681, ogni Stato membro istituisce un'unità designata d'informazione sui passeggeri (UIP), responsabile della raccolta conservazione e trattamento dei codici PNR e dei risultati derivanti da tali dati, e del loro **trasferimento** e scambio alle autorità nazionali competenti nonché alle corrispondenti unità degli altri Stati membri e ad **Europol**.

L'istituzione dell'unità ETIC consentirà ad Europol l'analisi delle informazioni fornite dalle UIP in materia di viaggi ai fini sia del sostegno all'azione di contrasto degli Stati membri, sia della cooperazione con la Commissione europea e con altre Agenzie europee nell'ambito degli affari interni (in particolare Frontex e l'Agenzia EU-LISA sui sistemi IT nello spazio di libertà, sicurezza e giustizia).

L'UNITÀ EC3

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

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

Il centro sostiene le autorità nazionali di contrasto alla criminalità sul piano **operativo**, **investigativo** e **forense**.

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

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

Ogni anno l'EC3 pubblica l'Internet IOCTA (*Internet Organized Crime Threat Assessment*), il suo report strategico recante le minacce emergenti, gli sviluppi nel crimine informatico e i risultati chiave dell'attività del centro.

L'UNIONE DELLA SICUREZZA

L'approccio strategico alle questioni della sicurezza

Nell'aprile 2015 l'Unione europea ha ridefinito il quadro strategico per la sua azione nel settore della sicurezza adottando un'Agenda europea sulla sicurezza, recante una serie di linee di intervento, tradotte in specifiche proposte legislative.

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 **protezione** dei possibili **obiettivi** degli attacchi terroristici;
- **dimensione esterna** della lotta contro il terrorismo.

Misure in materia di contrasto al terrorismo

Nel 2017, l'Unione europea ha ridefinito il quadro penale generale in materia di terrorismo approvando la direttiva (UE) n. 2017/541.

Il nuovo regime (che sostituisce la decisione quadro 2002/475/GAI e modifica la decisione 2005/671/GAI) principalmente 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).

Successivamente, l'UE ha concentrato l'attenzione sulle misure volte a neutralizzare gli strumenti impiegati dalle organizzazioni criminali e terroristiche. Sono riconducibili a tale settore di intervento:

- la direttiva (UE) n. 2017/853 relativa al controllo dell'**acquisizione e della detenzione di armi,** volta ad impedirne l'accesso ai criminali e ai terroristi, attraverso 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 (la direttiva è stata recepita con il D. Lgs. 10 agosto 2018, n. 104);
- il regolamento (UE) n. 2019/1157 sul rafforzamento della **sicurezza** delle **carte d'identità** dei cittadini dell'Unione e dei **titoli di soggiorno** rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione;
- il regolamento (UE) n. 2019/1148 relativo all'**immissione** sul **mercato** e all'uso di **precursori** di **esplosivi**.

Finanziamento del terrorismo

Nel febbraio del 2016, la Commissione europea ha presentato un Piano di azione per rafforzare la lotta contro il **finanziamento** del **terrorismo** recante, da un lato, iniziative volte ad individuare i terroristi attraverso i loro **movimenti finanziari** e impedire loro di spostare fondi o altri beni, dall'altro 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:

- la direttiva (UE) n. 2018/843 sulla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (V direttiva antiriciclaggio);
- la direttiva (UE) n. 2018/1673 volta a perseguire penalmente il riciclaggio dei proventi di reati;
- il regolamento (UE) n. 2018/1672 relativo ai controlli sul **denaro contante** in entrata nell'Unione o in uscita dall'Unione;
- il regolamento (UE) n. 2018/1805 relativo al riconoscimento reciproco dei **provvedimenti di congelamento e di confisca;**
- il regolamento (UE) n. 2019/880 volto a impedire l'**importazione** e il **deposito** nell'UE di **beni culturali** esportati **illecitamente** da un Paese terzo;
- la direttiva (UE) 2019/1153 volta ad **agevolare l'uso di informazioni finanziarie** e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati;
- la proposta di regolamento (il cui esame risulta ancora in corso presso le Istituzioni legislative) diretta a concentrare le competenze in materia di antiriciclaggio in relazione al settore finanziario in seno all'**Autorità bancaria europea (ABE)** 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. A seguito dell'accordo provvisorio con il

Consiglio, il 16 aprile 2019 il Parlamento europeo ha approvato la proposta in prima lettura.

Devono ricordarsi, infine:

- la comunicazione pubblicata dalla Commissione europea nel settembre 2018 "Rafforzare il quadro dell'Unione per la **vigilanza prudenziale** e **antiriciclaggio** degli istituti finanziari";
- le conclusioni approvate il 4 dicembre 2018 dal Consiglio Ecofin su un Piano d'azione volto a contrastare meglio il riciclaggio di denaro e il finanziamento del terrorismo;
- l'accordo multilaterale sullo scambio di informazioni sottoscritto il 10 gennaio 2019 dalla Banca centrale europea (BCE) e dalle autorità degli Stati membri preposte a contrastare il riciclaggio di denaro e il finanziamento del terrorismo.

Misure restrittive nei confronti di persone, gruppi ed entità coinvolti in atti terroristici

Dal 2001 l'Unione europea ha predisposto un elenco di persone, gruppi ed entità coinvolti in atti terroristici e soggetti a **misure restrittive**, in attuazione delle **risoluzioni dell'ONU** in materia di contrasto al terrorismo. L'elenco, comprensivo di persone e gruppi attivi sia all'interno che all'esterno dell'UE, è riesaminato periodicamente, almeno ogni 6 mesi.

Le misure restrittive consistono in:

- misure connesse al **congelamento dei capitali** e delle **attività finanziarie**;
- misure connesse alla **cooperazione di polizia e giudiziaria**.

Nel settembre 2016, il Consiglio dell'UE ha rafforzato l'azione antiterroristica adottando un quadro giuridico che consente all'UE di applicare **sanzioni in maniera autonoma nei confronti dell'ISIS/Da'esh e di Al Qaeda** e di persone ed entità ad essi associate o che li sostengono, indipendentemente dalla presenza di tali persone ed entità in elenchi elaborati dalle Nazioni Unite o da Stati membri dell'UE agenti a titolo individuale. In particolare, con la decisione

(PESC) 2016/1693 e il regolamento (UE) 2016/1686 (entrambi aggiornati nel febbraio 2019) l'UE ha imposto il divieto di viaggio nei confronti di persone identificate come associate all'ISIS (Da'esh)/Al Qaeda e il congelamento dei beni nei confronti di persone ed entità nella stessa situazione.

Per persone ed entità interessate si intendono quelle che hanno partecipato alla **pianificazione** o al **compimento di attentati terroristici** o hanno fornito all'ISIS (Da'esh)/Al Qaeda **finanziamenti**, petrolio o armi, o hanno ricevuto dagli stessi addestramento terroristico. Persone ed entità potrebbero inoltre essere inserite nell'elenco per attività quali **reclutamento**, **istigazione** o **provocazione** pubblica ad atti e attività a sostegno di tali organizzazioni, o coinvolgimento in gravi abusi dei diritti umani al di fuori dell'UE, tra cui sequestro, stupro, violenza sessuale, matrimonio forzato e riduzione in schiavitù. Le misure restrittive si estendono inoltre alle persone che viaggiano o cercano di recarsi sia al di fuori dell'UE che all'interno dell'UE allo scopo di sostenere l'ISIS (Da'esh)/Al Qaeda o di ricevere addestramento dagli stessi **(combattenti stranieri)**.

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.

Tra le iniziative previste dal piano, si ricorda il **Forum degli operatori**, istituito dalla Commissione per promuovere il **partenariato pubblico privato** in materia di sicurezza degli spazi pubblici. Il forum riunisce responsabili politici ed operatori degli Stati membri di diversi settori, come eventi di massa e intrattenimento, ospitalità, centri commerciali, sportivi e culturali, snodi di trasporto e altri ancora. Si ricorda, infine, che il 20 marzo 2019 è stato pubblicato un documento di lavoro dei Servizi della Commissione sulle "buone pratiche per rafforzare la sicurezza degli spazi pubblici" (SWD(2019)140).

Nello stesso settore di intervento la Commissione europea ha presentato:

- un Piano d'azione per rafforzare la preparazione contro i **rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare (CBRN);**
- un programma di azioni per migliorare la **sicurezza dei passeggeri del trasporto ferroviario**.

Radicalizzazione e linguaggio d'odio

È tuttora oggetto di *iter* legislativo la proposta di regolamento COM(2018)640 presentata dalla Commissione al fine di **eliminare** rapidamente i **contenuti terroristici dal web**. La proposta mira a introdurre un **termine vincolante** di **un'ora** per l'eliminazione dalla rete 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. Sulla proposta, il 17 aprile 2019, il Parlamento europeo ha approvato la propria posizione in prima lettura. Il neoeletto Parlamento europeo dovrà negoziare con il Consiglio dell'UE il testo definitivo del regolamento.

In tale settore, si ricorda che l'unità IRU (*Internet Referral Unit*), istituita nel 2015 in seno ad Europol, ha il compito di segnalare ai fornitori di servizi *online* interessati i **contenuti** volti alla **propaganda terroristica** o all'estremismo violento su Internet ai fini della loro rimozione.

Nell'ambito del contrasto alla radicalizzazione, l'UE ha altresì messo in campo una serie di strumenti 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 strategiche (ESCN).**

Da ultimo, si ricorda che, il 6 giugno 2019, il Consiglio dell'UE giustizia e affari interni ha approvato una serie di conclusioni sulla prevenzione e la lotta alla **radicalizzazione** nelle **carceri** e sulla gestione degli autori di reati di terrorismo ed estremismo violento dopo la **scarcerazione**,

Nel quadro generale della prevenzione e del **contrasto dei contenuti illeciti *on line*** si ricordano, infine: il Code of conduct siglato dalla Commissione 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 in cooperazione con le autorità nazionali (settembre 2017); 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).

Frontiere e Spazio Schengen

L'UE ha avviato un processo di rafforzamento dei **controlli alle frontiere esterne**, da un lato, aumentando le **verifiche** in **ingresso** e **uscita** dai confini UE, dall'altro, consolidando i tradizionali **sistemi** di **informazione** utilizzati dalle autorità di contrasto e di gestione delle frontiere, nonché istituendone di nuovi e prevedendo un unico meccanismo di interrogazione delle varie banche dati relative ai settori della giustizia e degli affari interni.

In tale contesto, deve essere inquadrato anche il potenziamento del sistema della **guardia di frontiera e costiera europea**.

Istituita con il regolamento (CE) n. 2007/2004 (con l'originaria denominazione di Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea), e da ultimo riformata con il regolamento (UE) 2016/1624, l'Agenzia europea della **guardia di frontiera** e **costiera** (**Frontex**) sostiene i Paesi dell'UE e i Paesi associati alla zona Schengen nella gestione delle loro frontiere esterne.

L'Agenzia contribuisce ad **armonizzare** i **controlli** alle frontiere in tutta l'UE e agevola la **collaborazione** tra le autorità di frontiera dei singoli paesi dell'UE fornendo assistenza tecnica e *know how*; l'Agenzia può coordinare l'invio di **attrezzatura tecnica aggiuntiva** e di **personale** di frontiera, e le **operazioni** alle frontiere marittime e terrestri esterne. Tra gli ambiti di competenza di Frontex figurano: analisi dei rischi; operazioni congiunte; risposta rapida; ricerca; formazione; rimpatri congiunti; scambio di informazioni.

Presentata dalla Commissione europea nel settembre del 2018, la proposta di regolamento COM(2018)631 mira a potenziare il sistema della **Guardia di frontiera e costiera europea**, tra l'altro, dotando Frontex di un **corpo permanente** di 10 mila unità operative abilitate a svolgere compiti che implicano **competenze esecutive**. Il regolamento rafforza inoltre il mandato dell'Agenzia prevedendo un suo maggior coinvolgimento nel sostegno alle **procedure di rimpatrio** effettuate dagli Stati membri e nella **cooperazione con i Paesi terzi interessati**.

*Il **20 febbraio 2019**, il Consiglio ha adottato la sua posizione negoziale sulla proposta della Commissione e, sulla base di tale mandato, il 28 marzo 2019 è stato raggiunto un accordo politico con il Parlamento europeo. Il 1° aprile 2019, tale accordo è stato confermato in sede di Consiglio. A tal proposito, si segnala che il Rappresentante permanente d'Italia presso l'Unione europea, Ambasciatore Maurizio Massari (in sede di audizione del **2 aprile 2019** presso le Commissioni Politiche dell'Unione europea del Senato e della Camera dei deputati) ha precisato che, in tale occasione, l'**Italia**, insieme alla Spagna e alla Slovenia, ha **espresso voto contrario** alla proposta, in quanto: la misura dell'istituzione del corpo permanente risulterebbe troppo onerosa (quantificata in circa 11 miliardi di euro, che secondo la Commissione potrebbero essere ridotti a 9 miliardi); la proposta sottrarrebbe, pertanto, risorse nazionali necessarie agli Stati membri per la gestione delle rispettive frontiere; essa, peraltro, non risulterebbe efficace per quanto riguarda la politica di rimpatrio.*

Sulla base dell'accordo interistituzionale del marzo 2019, il 17 aprile 2019 il Parlamento europeo ha approvato la posizione in prima lettura sulla riforma, che è tuttora in attesa dell'adozione da parte del Consiglio.

I rischi connessi al fenomeno del **terrorismo** e dei processi di **radicalizzazione,** e in particolare alla minaccia dei *foreign fighters*

(anche in previsione del loro eventuale ritorno in Europa dagli scenari di guerra), considerata altresì la facoltà di libero movimento in uno spazio privo di controlli alle frontiere interne, sono le principali ragioni che hanno indotto l'Unione europea a mettere inoltre in campo una serie di **riforme** (alcune delle quali risultano tuttora in esame) relative al **Codice frontiere Schengen**.

Tra gli elementi chiave in tale settore, l'approvazione della riforma del codice frontiere Schengen, entrata in vigore nell'aprile 2017, volta a rendere obbligatorie le **verifiche sistematiche** nelle 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 espatriati per aderire alle milizie ISIS.

Il Codice frontiere Schengen è attualmente oggetto di una proposta di riforma 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. Il **Governo italiano**, confermando riserve già manifestate nei confronti della proposta originaria della Commissione europea, ha individuato **criticità** anche con riferimento al testo che dovrebbe costituire la base per i negoziati interistituzionali tra Parlamento europeo e Consiglio.

Le iniziative istituite dall'UE per rafforzare gli strumenti di controllo degli ingressi alle frontiere esterne dell'UE includono:

- un sistema di ingressi/uscite dell'UE (EES), volto a consentire la registrazione dei dati di ingresso e uscita dei cittadini dei Paesi terzi all'atto di attraversare le frontiere esterne;
- 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;
- la riforma del quadro giuridico del **Sistema d'informazione Schengen (SIS)**, mediante l'adozione di tre regolamenti relativi all'uso del sistema d'informazione Schengen, rispettivamente, nel settore della cooperazione di polizia e della cooperazione

giudiziaria in materia penale, delle verifiche di frontiera e per il rimpatrio di cittadini di Paesi terzi il cui soggiorno è irregolare.

Il sistema di informazione Schengen è il sistema IT più ampiamente utilizzato nello spazio di libertà, sicurezza e giustizia dell'UE. Il sistema contiene oltre 76 milioni di segnalazioni. Il nuovo regime consente 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.

È tuttora all'esame dell'Istituzioni legislative europee una proposta di aggiornamento del **sistema d'informazione visti** (**VIS**), la banca dati che contiene informazioni su coloro che chiedono visti Schengen. Il 13 marzo 2019 il Parlamento europeo ha adottato la proposta in prima lettura.

Scambio di informazioni e cooperazione giudiziaria penale

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):

- **l'aggiornamento del quadro giuridico di Europol,** trasformato in Agenzia 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) (recepita in Italia con il Decreto legislativo 21 maggio 2018, n. 53).

Il miglioramento della condivisione delle informazioni è alla base inoltre di una serie di iniziative normative, che interessano, tra l'altro:

- il rafforzamento del sistema europeo di informazione sui casellari giudiziali (ECRIS), attraverso il regolamento n. 2019/816 istitutivo di un meccanismo per individuare gli Stati membri in possesso di informazioni sulle **condanne pronunciate** a carico di cittadini di **Paesi terzi** e **apolidi** e la

direttiva (UE) n. 2019/884 sullo scambio di informazioni relativamente ai cittadini di Paesi terzi;

- l'istituzione del quadro per **l'interoperabilità** tra i sistemi d'informazione dell'UE nel settore della giustizia e degli affari interni: si tratta del regolamento (UE) n. 2019/817 nel settore delle frontiere e dei visti e del regolamento (UE) n. 2019/818 nei settori della cooperazione giudiziaria e di polizia, dell'asilo e della migrazione. L'innovazione consiste in uno **sportello unico** in grado di **interrogare simultaneamente** i molteplici sistemi di informazione, potenziato da un unico meccanismo 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 si è concluso con l'adozione del regolamento (UE) 2018/1726).

Si ricorda, infine, che in occasione del Discorso sullo Stato dell'Unione del Presidente Jean-Claude Juncker del 12 settembre 2018, la Commissione europea ha proposto di estendere i compiti della **Procura europea** al fine di includervi la **lotta contro i reati di terrorismo**.

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 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.

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.

POLITICHE UE IN MATERIA DI CIBERSICUREZZA

L'approccio UE all'azione di contrasto al cybercrime

Nel corso degli anni l'UE ha progressivamente rafforzato le misure volte a contrastare la **criminalità informatica**, articolando il proprio intervento con 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, hate speech/discorso di odio, etc.) per mezzo di sistemi informatici.

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

Le minacce alle reti e ai sistemi informatici

La prima categoria di illeciti è considerata di particolare rilievo, attesa la vitale importanza delle reti e dei sistemi informatici rispetto al funzionamento delle **infrastrutture critiche** (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** di alcune tipologie di attacchi informatici.

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

destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

In particolare, con la **direttiva** 2016/1148, sulla **sicurezza delle reti** e **dell'informazione** (direttiva NIS) (recepita in Italia con il Decreto legislativo 18 maggio 2018, n. 65), l'Unione europea ha posto le basi per un miglioramento della **cooperazione operativa** tra Stati membri in caso di incidenti di cibersicurezza e della **condivisione delle informazioni sui rischi**.

La direttiva definisce **obblighi di sicurezza** per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, l'assistenza sanitaria e la finanza) e i fornitori di servizi digitali (mercati online, motori di ricerca e servizi di *cloud*); inoltre, ogni Paese dell'UE è tenuto a designare una o più **autorità nazionali** con il compito, tra l'altro, di monitorare l'applicazione della direttiva, nonché a elaborare una **strategia** per affrontare le minacce informatiche.

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

- il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (**ENISA**) che si intende trasformare nell'Agenzia UE per la cibersicurezza;
- l'introduzione di **sistemi europei di certificazione** della cibersicurezza dei prodotti e dei servizi TIC nell'Unione (che consisterebbero in una serie di norme, requisiti tecnici e procedure).

Si ricorda infine che, il 17 aprile 2019, il Parlamento europeo ha adottato la propria posizione in prima lettura circa la proposta di regolamento istitutiva di un **centro europeo** di ricerca e di competenza sulla cibersicurezza, affiancato da una rete di centri analoghi a livello di Stati membri. Tra gli obiettivi chiave della proposta, il miglioramento del coordinamento dei **finanziamenti** disponibili per la cooperazione, la ricerca e l'innovazione in tale ambito. La proposta è in attesa dell'adozione da parte del Consiglio dell'UE. Disposizioni volte alla sicurezza delle reti sono altresì contenute nel Codice delle comunicazioni elettroniche.

Cibersicurezza e 5G

Il **5G** viene considerato cruciale per una connettività di alta qualità nell'intero territorio dell'Unione, ai fini del completamento del mercato unico digitale e a sostegno dell'innovazione in tutti settori.

Si richiama in materia la recente approvazione della direttiva (UE) 2018/1972 che istituisce il citato Codice delle comunicazioni elettroniche e prevede che entro il 2020 tutti gli Stati membri dell'UE assegnino le frequenze necessarie per l'introduzione della rete 5G.

L'importanza strategica del 5G, sia per le funzioni vitali della società e dell'economia, come l'energia, i trasporti, le banche e la sanità, sia nel contesto della protezione del **processo democratico** contro le interferenze e la **disinformazione**, ha indotto l'UE ad avviare l'elaborazione di strumenti volti a garantire a tale infrastrutture digitale un livello adeguato di sicurezza e resilienza.

A tal proposito si ricordano:

- la risoluzione non legislativa (2019/2575 (RSP), adottata dal Parlamento europeo il 12 marzo 2019, sulle " **minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione** e sulla possibile azione a livello di Unione per ridurre tali minacce";

  Nell'atto di indirizzo si esprime forte preoccupazione in relazione alla possibilità che le **infrastrutture cinesi** per le reti 5G possano avere incorporate delle *'backdoor'* in grado di consentire a fornitori ed autorità cinesi un accesso non autorizzato ai dati personali e alle telecomunicazioni nell'UE. La legislazione cinese contempla una definizione estesa della sicurezza nazionale tale da comportare l'obbligo per le imprese di cooperare con lo Stato, pertanto vi è il timore che i fornitori di dispositivi di un paese terzo come la Cina possano costituire un rischio per la sicurezza dell'Unione europea.

- la comunicazione congiunta del "UE - Cina una prospettiva strategica" della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, nella quale si sottolinea la necessità di un approccio comune per la cibersicurezza delle reti 5G;

- la raccomandazione del 26 marzo 2019, con la quale la Commissione europea (in attuazione dell'indirizzo espresso dal

Consiglio europeo del 22 marzo 2019 a favore di un approccio concertato alla sicurezza delle reti 5G) propone un approccio comune dell'UE ai rischi per la sicurezza delle reti 5G, basato su una **valutazione coordinata dei rischi** e su misure coordinate di **gestione dei rischi**, su un quadro efficace per la cooperazione e lo **scambio di informazioni** e su una **conoscenza comune** della situazione delle reti di comunicazione.

L'uso dei sistemi informatici a fini criminali

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

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

La materia è stata da ultimo trattata dall'UE anche per i profili di **politica estera**. A tal proposito, il 6 giugno 2019, il Consiglio dell'UE ha conferito alla Commissione europea due **mandati** per svolgere negoziati internazionali intesi a migliorare l'accesso transfrontaliero alle prove elettroniche nelle indagini penali, da un lato, con gli **Stati Uniti**, dall'altro con particolare riguardo al secondo protocollo aggiuntivo alla **Convenzione di Budapest** del Consiglio d'Europa sulla

criminalità informatica. I mandati includono disposizioni recanti garanzie a tutela dei diritti fondamentali in materia di protezione dei dati, *privacy* e diritti procedurali delle persone.

L'impiego dei sistemi informatici per la diffusione di contenuti illegali: recenti iniziative per il contrasto alle attività di disinformazione

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

Tra i primi strumenti per contrastare la **propaganda** di enti e organismi situati in **Stati terzi** volta a diffondere **informazioni fuorvianti** o palesemente false (in particolare, da parte della Russia), la Task force East StratCom, istituita nel 2015 con il compito di sviluppare prodotti e campagne di comunicazione incentrate sulla **spiegazione delle politiche dell'UE** nella regione del **partenariato orientale**. Sono incentrate su aree geografiche diverse: la Task Force **StratCom per i Balcani occidentali** e la **Task Force South Med Stratcom** per il mondo di lingua araba.

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

- la **comunicazione** dell'aprile 2018, con la quale la Commissione europea delinea un **approccio comune** alla materia e prevede quale misura chiave l'elaborazione da parte dei rappresentanti delle piattaforme on line, dell'industria della pubblicità e dei principali inserzionisti di un **codice di buone pratiche** dell'UE sulla disinformazione in regime di autoregolamentazione;

  Il codice è stato adottato nell'ottobre del 2018 dalle principali piattaforme *on line* (tra le quali Facebook, Google, e Twitter), dalle società di software (in particolare, nel maggio 2019, ha aderito al codice la Microsoft), e dalle organizzazioni che rappresentano il settore della pubblicità. Il codice prevede una serie di impegni, che comprendono la garanzia della **trasparenza** dei **messaggi**

pubblicitari di natura politica, la **chiusura** dei **profili falsi**, l'etichettatura dei messaggi diffusi dai "bot" e il miglioramento della **visibilità** dei **contenuti** sottoposti a **verifica dei fatti.** La Commissione europea ha manifestato l'intenzione di procedere ad una valutazione dell'efficacia del codice entro la fine del 2019, preannunciando peraltro ulteriori iniziative, anche di natura regolamentare, qualora i risultati di tale valutazione non fossero soddisfacenti.

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

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

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

  I settori sono: capacità di **individuazione** dei casi di **disinformazione**, in particolare tramite il rafforzamento delle task force di comunicazione strategica e della cellula dell'UE per l'analisi delle minacce ibride del servizio europeo per l'azione esterna (SEAE); **risposta coordinata**, dotando istituzioni UE e Stati membri di un **sistema di allarme rapido** per la condivisione e valutazione delle campagne di disinformazione; **attuazione** efficace da parte delle **piattaforme online** e dell'industria firmatarie degli impegni nell'ambito del **codice di buone pratiche**; **campagne di sensibilizzazione** e **di responsabilizzazione** dei **cittadini** in

particolare mediante l'alfabetizzazione mediatica. Il 14 giugno 2019, è stata pubblicata una relazione sullo stato dell'arte dell'attuazione del piano.

Data la sensibilità del tema, con particolare riguardo alla questione della protezione delle elezioni europee, il contrasto alla disinformazione è stato oggetto di conclusioni da parte dei Consigli europei del 13-14 dicembre 2018, del 22 marzo e del 20-21 giugno 2019.

In particolare, nella riunione del 20-21 giugno 2019, il Consiglio europeo ha chiesto un impegno costante per **sensibilizzare** sul tema della disinformazione e rafforzare la preparazione e la resilienza delle nostre democrazie di fronte a tale fenomeno. Oltre ad accogliere favorevolmente l'intenzione della Commissione di valutare approfonditamente l'attuazione degli **impegni** assunti dai firmatari del citato **codice di buone pratiche**, il Consiglio europeo ha, altresì, sottolineato la necessità di una valutazione costante e di una risposta adeguata nei confronti della continua evoluzione delle minacce e del crescente rischio di interferenze dolose e manipolazioni online, associati allo sviluppo dell'**intelligenza artificiale** e di **tecniche di raccolta dati**.

Nuovo regime di sanzioni per contrastare le minacce esterne

Nell'ambito delle azioni contemplate dal pacchetto del 2017 sugli strumenti della diplomazia informatica, il 17 maggio 2019, con il regolamento 2019/796 e la decisione (PESC) 2019/797, il Consiglio dell'UE ha introdotto **misure restrittive** volte a **scoraggiare** e **contrastare** gli **attacchi informatici** che costituiscono una minaccia **esterna** per l'UE o i suoi Stati membri, compresi gli **attacchi informatici** nei confronti di **Stati terzi** o **organizzazioni internazionali** qualora le misure restrittive siano ritenute necessarie per conseguire gli obiettivi della **politica estera e di sicurezza comune** (PESC).

Gli attacchi informatici che rientrano nell'ambito di applicazione del nuovo regime di sanzioni sono quelli che hanno effetti significativi e che:

- provengono o sono sferrati dall'esterno dell'UE o
- impiegano infrastrutture esterne all'UE o

- sono compiuti da persone o entità stabilite o operanti al di fuori dell'UE o
- sono commessi con il sostegno di persone o entità operanti al di fuori dell'UE.

Il regime di sanzioni copre anche i **tentati attacchi** informatici con effetti potenzialmente significativi.

Tale regime consente all'UE di imporre **sanzioni** a **persone** o **entità** responsabili di attacchi informatici o tentati attacchi informatici, che forniscono **sostegno finanziario**, **tecnico** o **materiale** per tali attacchi o che sono altrimenti coinvolti. Le sanzioni possono anche essere imposte a persone o entità associate ad esse. Le misure restrittive includono un **divieto** per le persone che **viaggiano verso l'UE** e un **congelamento** dei **beni** delle persone o entità. È fatto inoltre divieto alle persone ed entità dell'UE di mettere fondi a disposizione di persone ed entità inserite nell'elenco.

L'importanza del nuovo regime di misure restrittive è stata da ultimo sottolineata dal Consiglio europeo del 20 - 21 giugno 2019, che ha altresì invitato le istituzioni dell'UE, insieme agli Stati membri, a lavorare a misure per aumentare la resilienza e migliorare la cultura della sicurezza dell'UE contro le **minacce informatiche e ibride provenienti dall'esterno dell'UE**, nonché per meglio proteggere da qualsiasi attività dolosa le **reti di informazione** e di **comunicazione dell'UE** e i suoi processi decisionali.