dossier

20 febbraio 2019

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

4ª riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Bucarest, 24-25 febbraio 2019

Senato della Repubblica
Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

4ª riunione del Gruppo di controllo parlamentare congiunto delle attività di Europol

Bucarest, 24-25 febbraio 2019

SENATO DELLA REPUBBLICA
SERVIZIO STUDI
DOSSIER EUROPEI
N. 38

CAMERA DEI DEPUTATI
UFFICIO RAPPORTI CON
L'UNIONE EUROPEA
N. 16

Senato della Repubblica

Servizio Studi

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

Dossier europei n. 38

Camera dei deputati

Ufficio rapporti con l'Unione europea

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

Dossier n. 16

INDICE

Parliamentary Dimension

romania2019.eu
Romanian Presidency of the Council of the European Union

European Parliament

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

–

4th meeting

–

Bucharest, Romania, 24-25 February 2019

Palace of Parliament, Room I.I.C. Brătianu

—

DRAFT PROGRAMME

Sunday, 24 February

17:00 – 18:00	**Meeting of the Presidential Troika of JPSG Europol** *In camera* *Venue: Palace of Parliament, Spiru Haret Room, main floor*
18:00 – 19:00	**2nd Meeting of the Working Group on the participation of Denmark to the JPSG meetings** *In camera* *Venue: Palace of Parliament, Spiru Haret Room, main floor*
19:30 – 19:45	**Cultural programme** *Venue: Marriott Hotel, Calea13 Septembrie 90, Bucharest, 050726*
19:45 – 21:30	**Official Dinner** - Welcome address by Ms. Oana-Consuela FLOREA, Head of Delegation of the Romanian Parliament to the JPSG on Europol

- Welcome address by Mr. Claude MORAES, Chairman of the Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Parliament, and Chair of the EP delegation to the JPSG
- Welcome speech by Ms. Carmen DAN, Minister of Internal Affairs, Romania (TBC)

Venue: Marriott Hotel, Calea 13 Septembrie 90, Bucharest, 050726

Monday, 25 February

8:15-8:20 *Departure from the hotels to the JPSG meeting venue*

9:00 – 9:15 **Adoption of the agenda and opening remarks by the Co-Chairs**

- Ms Oana-Consuela FLOREA, Head of delegation of the Romanian Parliament to the JPSG on Europol
- Mr Claude MORAES, Chairman of the Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Parliament, and Head of the EP delegation to the JPSG

9:15– 10:15 **Reporting on Europol activities from September 2018 to February 2019**

- Presentation by Ms Catherine De BOLLE, Executive Director of Europol
- Exchange of views

10:15– 11:15 **Europol Management Board activities from September 2018 to February 2019**

- Presentation by Mr Victor Wili APREUTESEI, Chairperson of Europol Management Board
- Report by Mr Tsvetan TSVETANOV, Chairman of the Committee on Internal Security and Public Order, 44th National Assembly of the Republic of Bulgaria
- Exchange of views

11:15 – 11:30 **Coffee break**

11:30 – 12:30 **Reporting back by the European Data Protection Supervisor and Europol Cooperation Board**

- Report from Professor François PELLEGRINI, Chair of the Europol Cooperation Board
- Speech by Mr Giovanni BUTTARELLI, European Data Protection Supervisor (video message)

- Report from Mr Wojciech WIEWIÓROWSKI, European Data Protection Assistant Supervisor
- Exchange of views

12:30 – 13:30 **Family Photo & Official lunch**

13:30 – 14:15 **Europol Travel Intelligence Centre (ETIC): State of play and activity report**
- Presentation by Mr Wil van GEMERT, Deputy Executive Director for Operations at Europol
- Exchange of views

14:15 – 15:00 **European Cybercrime Centre (EC3): State of play and activity report including support against counterfeiting of non-cash means of payment, monitoring and countering dark web crimes**
- Presentation by Mr Wil van GEMERT, Deputy Executive Director for Operations at Europol
- Exchange of views

15:00 – 15:15 **Coffee break**

15:15– 16:00 **Keynote speech by Sir Julian KING, Commissioner for the Security Union**
- Exchange of views

16:00 – 16:45 **Designation of the JPSG representative to the meetings of the Europol Management Board**
- Chairs' information on recent developments, ways forward and exchange of views

16:45 – 17:00 **Conclusions and closing remarks of the meeting by the Co-Chairs**
- Ms Oana-Consuela FLOREA, Head delegation of the Romanian Parliament to the JPSG on Europol
- Mr Claude MORAES, Chairman of the Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Parliament, and Head of the EP delegation to the JPSG

17:00 **Guided tour of the Palace of Parliament**

17:30 **Transfer by bus to the hotels**

---

* *
*

Schede di lettura

IL PROGRAMMA DELLA RIUNIONE

In base alla bozza di programma della riunione, nel pomeriggio del 24 febbraio 2019, si svolgerà la riunione della Troika presidenziale del Gruppo di controllo parlamentare congiunto delle attività di Europol, nonché il secondo incontro del gruppo di lavoro sulla partecipazione della Danimarca al medesimo organismo. Il 25 febbraio 2019, a seguito dell'adozione dell'agenda e degli interventi introduttivi di Oana Consuela Florea (Presidente della delegazione del Parlamento rumeno al Gruppo) e di Claude Moraes (Presidente della Commissione per le libertà civili, la giustizia e gli affari interni LIBE del Parlamento europeo), sono previste le seguenti sessioni aventi ad oggetto, rispettivamente:

- le attività di Europol da settembre 2018 a febbraio 2019, oggetto di presentazione da parte della direttrice esecutiva di Europol, Catherine De Bolle;
- le attività del consiglio di amministrazione di Europol da settembre 2018 a febbraio 2019. La sessione prevede la presentazione da parte di Victor Wili Apreutesei, Presidente del Consiglio di amministrazione di Europol e la relazione di Tsvetan Tsvetanov, Presidente della Commissione Interni, sicurezza e ordine pubblico della 44° Assemblea della Repubblica di Bulgaria;
- le relazioni da parte del Garante europeo per la protezione dei dati personali e del Consiglio di cooperazione di Europol. La sessione prevede l'intervento di Francois Pellegrini, Presidente del Consiglio di cooperazione, di Giovanni Buttarelli, Garante europeo per la protezione dei dati personali, e di Wojciech Wiewiórowski, Garante aggiunto europeo per la protezione dei dati personali;
- lo stato dell'arte e le attività dell'*Europol Travel Intelligence Centre* (ETIC). La sessione prevede l'introduzione da parte di Wil Van Gemert, vice direttore esecutivo di Europol per le operazioni;
- il Centro europeo per il *cybercrime* (EC3): relazione sullo stato dell'arte e le attività, inclusi il sostegno al contrasto alla contraffazione dei mezzi di pagamento diversi dal contante e il monitoraggio del crimine che riguarda il *dark web*. La sessione è introdotta dalla relazione di Wil Van Gemert;

- relazione di sir Julian King, Commissario per l’Unione della sicurezza.

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

  La giornata di lavoro terminerà con la designazione del rappresentante del Gruppo alle riunioni del consiglio di amministrazione di Europol, nonché le conclusioni e i commenti finali dei due Co-Presidenti del Gruppo.

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.

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 alla peculiare attività dell'Agenzia di sostegno alle attività di tutela della

[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.

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 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;

[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).

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

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;

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

Le principali misure in materia di contrasto al terrorismo

Riforma del quadro penale

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[4].

Nell'ambito delle misure volte a neutralizzare gli strumenti impiegati dalle organizzazioni criminali e terroristiche, la Commissione europea ha presentato, nell'aprile del 2018:

- una proposta di revisione e rafforzamento delle restrizioni attualmente previste dal regolamento 98/2013 relativo all'**immissione sul mercato e all'uso di precursori di esplosivi**, recante una serie di misure che limitano l'accesso dei privati a tali sostanze;
- 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 (su cui

[4] La direttiva è stata recepita con il D. Lgs. 10 agosto 2018, n. 104.

il 19 febbraio 2019 Parlamento europeo e Consiglio hanno raggiunto un accordo in attesa dell'adozione formale).

Si segnala, infine, la proposta, presentata 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**[5].

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 contrasto al finanziamento del terrorismo

Dando seguito al 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 rafforzare il contrasto al **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:

- la V direttiva antiriciclaggio, del 30 maggio 2018, sulla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo;
- la direttiva 2018/1673, volta a perseguire penalmente il riciclaggio dei proventi di reati;

[5] 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.

- il regolamento 2018/1672 relativo ai controlli sul **denaro contante** in entrata nell'Unione o in uscita dall'Unione;
- il regolamento 2018/1805 relativo al riconoscimento reciproco dei **provvedimenti di congelamento e di confisca.**

Sono tuttora all'esame delle Istituzioni europee:

- una proposta di regolamento 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 (*il 12 febbraio 2019 il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sulla proposta della Commissione).*

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 ha 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).

Il 4 dicembre 2018, il Consiglio Ecofin ha adottato conclusioni su un **Piano d'azione** volto a contrastare meglio il **riciclaggio di denaro e il finanziamento del terrorismo**.

Le conclusioni delineano una serie di azioni non legislative a breve termine tese a conseguire **8 obiettivi fondamentali**: individuare i fattori che hanno contribuito ai recenti casi di riciclaggio dei proventi nelle banche dell'UE, così da dare forma a eventuali ulteriori azioni a medio e lungo termine; repertoriare i

pertinenti rischi relativi al riciclaggio dei proventi e al finanziamento del terrorismo nonché le migliori prassi in materia di vigilanza prudenziale per affrontarli; migliorare la convergenza in materia di vigilanza e prendere meglio in considerazione gli aspetti relativi all'antiriciclaggio nel processo di vigilanza prudenziale; garantire una cooperazione efficace tra le autorità di vigilanza prudenziale e le autorità di vigilanza in materia di riciclaggio; chiarire gli aspetti relativi alla revoca di un'autorizzazione alle banche in caso di gravi violazioni; migliorare la vigilanza e lo scambio di informazioni tra le autorità competenti; condividere le migliori prassi e trovare un terreno di convergenza tra le autorità nazionali; migliorare la capacità delle autorità europee di vigilanza di sfruttare maggiormente gli strumenti e i poteri esistenti.

Il 10 gennaio 2019 è stato infine sottoscritto un **accordo multilaterale sullo scambio di informazioni fra la Banca centrale europea (BCE) e le 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'ISIL/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 l'UE ha imposto il divieto di viaggio nei confronti di persone identificate come associate all'ISIL (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'ISIL (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'ISIL (Da'esh)/Al Qaeda o di ricevere addestramento dagli stessi (**combattenti stranieri**).

Previo accordo sulle proposte di inserimento da parte degli Stati membri, le persone ed entità sono inserite nell'elenco tramite una decisione del Consiglio e un regolamento del Consiglio, adottati all'unanimità.

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 per il 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.

La Commissione europea ha infine avviato un programma di azioni per migliorare la **sicurezza dei passeggeri del trasporto ferroviario** nell'UE, che prevede fra l'altro l'istituzione di una piattaforma volta a raccogliere informazioni pertinenti sulla sicurezza ferroviaria e fornire orientamenti sulle buone pratiche per gli Stati membri, nonché 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 strategiche (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 *online*** attraverso una cooperazione volontaria rafforzata.

L'IRU 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.

Nel quadro degli interventi della Commissione europea per la prevenzione e il contrasto dei contenuti illeciti *online* 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 *online*** al fine di intensificare la lotta contro i contenuti illeciti *online* 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** *online* 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 sullo 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 di 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** 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 (le stime Europol riferiscono un volume assai approssimativo nel 2017, intorno **alle 7 mila persone**) espatriati per aderire alle milizie ISIS.

Da ultimo, si segnala che 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[6].

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.

Il 19 novembre 2018, il Consiglio dell'UE ha inoltre approvato tre proposte di regolamento volte a rafforzare il **Sistema d'informazione Schengen (SIS)**, relative 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.

---

[6] Il 29 novembre 2018, il Parlamento europeo ha approvato emendamenti al testo della Commissione europea, rinviando la questione alla Commissione parlamentare competente per l'avvio di negoziati interistituzionali.

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.

Si ricorda infine che attiene alla gestione del controllo delle frontiere esterne dell'UE la proposta di regolamento COM(2018)631 volta a potenziare il sistema della **Guardia di frontiera e costiera europea**, tra l'altro prevedendo in seno all'Agenzia europea omonima (meglio conosciuta con il nome di Frontex) la costituzione di un corpo permanente di 10 mila unità operative, entro il 2020, abilitate a svolgere compiti che implicano competenze esecutive; la Commissione europea propone peraltro di rafforzare 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.

Nella relazione, presentata ai sensi dell'articolo 6, comma 4, della legge n. 234 del 2012, il **Governo italiano**, pur condividendo le finalità perseguite dall'iniziativa, ritiene tuttavia che la proposta normativa tenda a conferire un maggior peso e autorità decisionale alla Commissione europea e all'Agenzia stessa, rilevando in particolare che le diposizioni che prefigurano il dispiegamento delle guardie europee sul territorio di uno Stato interessato in assenza del consenso di quest'ultimo potrebbero considerarsi come violazione della sovranità nazionale.

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):

- **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)[7].

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

[7] Recepita in Italia con il Decreto legislativo 21 maggio 2018, n. 53.

- la messa in rete dei **casellari giudiziari,** anche con riferimento a cittadini di Stati terzi (COM(2017)344);
- 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 (COM(2017)793 e COM(2017)794);
- 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).

LE POLITICHE UE IN MATERIA DI CYBERSICUREZZA

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** e gli **attacchi informatici**, 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 cybersicurezza (per approfondimenti si consigliano i temi web su: Consiglio europeo 28-29 giugno 2018, Consiglio europeo 17-18 ottobre 2018; Consiglio europeo 13-14 dicembre 2018.

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**[8] di alcune tipologie di attacchi informatici.

In tale ambito, si ricorda la **direttiva**, approvata nel luglio 2016, **sulla sicurezza delle reti e dell'informazione** (direttiva NIS)[9], 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**.

In particolare, 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*). Conformemente alla direttiva NIS, ogni Paese dell'UE è inoltre tenuto a designare una o più **autorità nazionali**, nonché a elaborare una **strategia** per affrontare le minacce informatiche.

L'UE ha rafforzato il quadro mediante un'ulteriore proposta di regolamento sulla cibersicurezza (cosiddetto *cybercecurity act*) il cui iter legislativo è particolarmente avanzato, 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 è tuttora in corso di esame legislativo 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).

---

[8] 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.

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

L’uso dei sistemi informatici a fini criminali

È tuttora all’esame delle istituzioni legislative europee la riforma della normativa europea relativa alla lotta contro le **frodi** e le **falsificazioni di mezzi di pagamento** diversi dai contanti.

La riforma intende: **ampliare** la portata dei reati per includere, ad esempio, le transazioni mediante **valute virtuali**; armonizzare le definizioni di alcuni reati *online*, quali la **pirateria** informatica o il ***phishing***; introdurre livelli minimi per le **sanzioni** più elevate per le persone fisiche; chiarire la **competenza** giurisdizionale riguardo le frodi transfrontaliere; migliorare la **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 cybersicurezza, 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 una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei **rappresentanti legali** ai fini dell'**acquisizione di prove** nei procedimenti penali.

L’impiego dei sistemi informatici per la diffusione di contenuti illegali: recenti iniziative

Oltre alla citata proposta di regolamento COM(2018)640, volta a eliminare i contenuti terroristici dal *web*, si segnalano le seguenti iniziative della Commissione Europea in materia di diffusione di contenuti illegali *online*: **raccomandazioni** del marzo 2018 agli Stati membri recanti misure operative volte a garantire maggiore rapidità nella rilevazione e nella rimozione dei contenuti illegali *online* anche di stampo **terroristico** o riconducibili a **reati** di **odio; orientamenti politici** del settembre 2017 per le piattaforme *online* al fine di intensificare la lotta contro i contenuti illeciti *online* in cooperazione con le autorità nazionali; ***Code of conduct*** del maggio 2016 per la prevenzione e il contrasto dei contenuti illeciti *online* 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**.

Iniziative per il contrasto alle attività di disinformazione

Il tema delle minacce informatiche è affrontato dall'UE anche con riferimento alle **attività** di **disinformazione**, ed in particolare alla propaganda di enti e organismi situati in Stati terzi volta a diffondere informazioni fuorvianti o palesemente false.

Il Consiglio europeo del 13-14 dicembre 2018, evidenziando preliminarmente che la diffusione della disinformazione intenzionale, sistematica e su larga scala, anche nel quadro della guerra ibrida, rappresenta una grave sfida strategica per i nostri sistemi democratici e richiede una risposta urgente che deve essere mantenuta nel tempo, nel pieno rispetto dei diritti fondamentali, ha: sottolineato la necessità di una risposta decisa che affronti la dimensione interna e quella esterna e che sia globale, coordinata e dotata di risorse adeguate sulla base di una valutazione delle minacce; chiesto **l'attuazione tempestiva e coordinata del piano d'azione congiunto contro la disinformazione** presentato dalla Commissione e dall'Alta rappresentante dell'Unione europea per gli Affari esteri e la politica di sicurezza, in modo da potenziare le capacità dell'UE, rafforzare le risposte coordinate e congiunte tra l'Unione e gli Stati membri, mobilitare il settore privato e accrescere la resilienza della società alla disinformazione; chiesto un intervento rapido e decisivo, a livello sia europeo sia nazionale, per **assicurare elezioni europee e nazionali libere e regolari**.

I più recenti strumenti proposti dalla Commissione europea in materia di disinformazione sono:

- una serie di misure per garantire elezioni libere ed eque (presentate in occasione del discorso sullo Stato dell'Unione del settembre 2018), che comprendono una maggiore trasparenza della pubblicità politiche *online* e la possibilità di imporre sanzioni per **l'uso illegale di dati personali** al fine di influenzare deliberatamente il risultato delle elezioni europee[10];

[10] Tali misure sono contenute in una serie di provvedimenti: 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 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; una proposta di modifica del regolamento del 2014 relativo al **finanziamento dei partiti politici europei**, volta a consentire di infliggere sanzioni pecuniarie per le violazioni delle norme in materia di protezione dei dati commesse allo scopo di influenzare deliberatamente l'esito delle elezioni europee.

- un Piano d'azione contro la disinformazione, articolato in quattro settori chiave.

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

In tale settore si ricorda, inoltre, che, a seguito all'invito del Consiglio europeo a contrastare le campagne di disinformazione da parte della Russia, nel 2015 è stata creata la Task force East StratCom, 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.

Si segnala infine che, con la **comunicazione** dell'aprile 2018 in materia di **contrasto alla disinformazione *online***, si è tra l'altro avviato il **codice di buone pratiche**[11] dell'UE sulla disinformazione in regime di autoregolamentazione, firmato da grandi piattaforme *online* e dall'industria pubblicitaria.

Risorse finanziarie

A giugno 2018, la Commissione europea ha avanzato la proposta del **Quadro Finanziario Pluriennale 2021-2027**. Fra le altre cose, la Commissione prefigura un **Fondo per la Sicurezza Interna** (proposta COM(2018)472, con una dotazione di **2,5 miliardi di euro**) e il

[11] Nell'ottobre del 2018 alcune tra le principali società *online* (Google, Facebook, Twitter e Mozilla) e associazioni che rappresentano il settore pubblicitario hanno firmato **un codice di buone pratiche**, impegnandosi ad attuare una serie di misura in previsione delle elezioni europee per affrontare efficacemente il problema dell'utilizzo delle nuove tecnologie e dei *social media* finalizzato a diffondere, mirare e amplificare la disinformazione. Il 29 gennaio 2019 la Commissione europea ha pubblicato le prime relazioni presentate dai firmatari del Codice.

Programma Europa Digitale (proposta COM(2018)434, con una dotazione di **9,2 miliardi di euro**).

In particolare, il Fondo Sicurezza Interna mira a garantire un elevato livello di sicurezza nell'UE, prestando attenzione al contrasto al **terrorismo,** alla **radicalizzazione**, alla **criminalità organizzata**, **informatica** e al ***cybercrime***.

Col fondo sarà possibile **finanziare** anche l'acquisto e l'implementazione delle infrastrutture tecniche necessarie all'**interoperabilità** dei vari **sistemi d'informazione** Ue per la sicurezza, in sinergia col Programma Europa Digitale

Inoltre, il nuovo **Programma Europa Digitale** è volto a sostenere la trasformazione digitale delle società e delle economie europee mediante importanti investimenti nei settori del supercalcolo, dell'intelligenza artificiale, della cibersicurezza e delle competenze digitali avanzate. La Commissione europea propone di investire quasi **2 miliardi di euro** per sostenere, insieme agli Stati membri, gli appalti di **attrezzature**, **strumenti** e **infrastrutture di dati** di grado avanzato, garantire un'ampia diffusione delle **conoscenze** e delle **competenze** nel campo della cibersicurezza in tutta l'economia e rafforzare il livello di **sicurezza delle reti** e dei **sistemi informatici** in tutta l'Unione europea.