Consiglio
dell'Unione europea

Bruxelles, 31 gennaio 2017
(OR. en)

5775/17

COSI 16
CT 5
FRONT 41
DAPIX 34
ENFOPOL 44
VISA 34
FAUXDOC 8
COPEN 22
DROIPEN 10
CYBER 12
JAI 76

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	26 gennaio 2017
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2017) 41 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO Quarta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza

Si trasmette in allegato, per le delegazioni, il documento COM(2017) 41 final.

All.: COM(2017) 41 final

COMMISSIONE
EUROPEA

Bruxelles, 25.1.2017
COM(2017) 41 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO

Quarta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza

Quarta relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza

I. INTRODUZIONE

Il presente documento è la quarta relazione mensile sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza, e verte sugli sviluppi attinenti a due pilastri principali: *affrontare il problema del terrorismo e della criminalità organizzata e i relativi mezzi di sostegno, nonché rafforzare le nostre difese e creare resilienza contro tali minacce*. La presente relazione si articola intorno a quattro settori fondamentali: i sistemi d'informazione e l'interoperabilità, la protezione degli obiettivi non strategici, la minaccia informatica e la protezione dei dati nel contesto delle indagini penali.

L'attentato al mercatino di Natale di Berlino compiuto nel mese di dicembre ha messo nuovamente in evidenza gravi punti deboli nei nostri sistemi d'informazione che devono essere affrontati urgentemente, in particolare a livello dell'UE, per aiutare le autorità nazionali di frontiera e di contrasto sul campo a far fronte in modo più efficace ai loro difficili compiti. Il fatto che i vari sistemi d'informazione non siano interconnessi – cosa che consente agli autori degli attentati di utilizzare identità multiple per spostarsi senza essere rintracciati, anche attraversando le frontiere – e il fatto che le informazioni non siano sistematicamente caricate dagli Stati membri nelle banche dati pertinenti dell'UE, costituiscono lacune nell'attuazione pratica cui va urgentemente posto rimedio. Altro lavoro è inoltre necessario per quanto riguarda le misure di contrasto alle frontiere e il rimpatrio delle persone la cui domanda d'asilo è stata respinta[1].

Per quanto attiene alla protezione degli obiettivi non strategici, la Commissione accelererà i lavori che sta svolgendo per riunire esperti degli Stati membri allo scopo di condividere le migliori prassi e di concordare orientamenti standard.

La minaccia informatica che incombe sull'UE sta ricevendo un'ampia copertura mediatica, e la presente relazione esamina i vari filoni di attività già in corso in questo settore. Si tratta sia dell'aspetto della prevenzione – attraverso il lavoro con l'industria per promuovere la sicurezza fin dalla progettazione e l'attuazione della direttiva sulla sicurezza delle reti e dell'informazione –, che della promozione della cooperazione fra gli Stati membri e con le organizzazioni e i partner internazionali per poter reagire in caso di attacchi informatici. Nei mesi a venire la Commissione e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza metteranno a fuoco le azioni necessarie per dare una risposta europea efficace a queste minacce sulla base della strategia dell'UE del 2013 per la cibersicurezza.

La protezione della vita privata dell'individuo e dei dati personali è un diritto fondamentale e pertanto una pietra angolare di qualsiasi azione verso un'autentica Unione della sicurezza. La direttiva sulla protezione dei dati in ambito di polizia e di giustizia penale, adottata nell'aprile 2016, garantisce norme comuni di livello elevato in materia di protezione dei dati, e faciliterà quindi l'agevole scambio dei dati rilevanti fra

[1] La Commissione presenterà nelle prossime settimane un piano d'azione riveduto sul rimpatrio – Si veda la relazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio sulle attività volte a rendere pienamente operativa la guardia di frontiera e costiera europea, COM(2017) 42.

le autorità di contrasto degli Stati membri. La Commissione ha inoltre avviato una revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche come parte del suo pacchetto "Dati" per ampliare il campo d'applicazione di tale direttiva a tutti i fornitori di comunicazioni elettroniche e per allinearne le disposizioni a quelle del regolamento generale sulla protezione dei dati. La proposta è concepita per garantire la privacy nell'ambito delle comunicazioni elettroniche definendo al tempo stesso i motivi per i quali possono essere prese in considerazione limitazioni del campo d'applicazione del regolamento sulla vita privata e le comunicazioni elettroniche (ePrivacy), inclusi motivi di sicurezza nazionale o indagini penali.

II. RAFFORZARE I SISTEMI DI INFORMAZIONE E L'INTEROPERABILITÀ

La dichiarazione sullo stato dell'Unione rilasciata dal Presidente Juncker nel settembre 2016 e le conclusioni del Consiglio europeo del dicembre 2016 fanno riferimento all'importanza di ovviare alle attuali carenze nella gestione delle informazioni e di migliorare **l'interoperabilità e l'interconnessione tra i sistemi d'informazione esistenti**. I recenti eventi hanno nuovamente evidenziato l'urgente necessità di collegare fra loro le banche dati esistenti dell'UE, non da ultimo per dare alle autorità di frontiera e alle autorità di contrasto sul campo gli strumenti necessari per individuare le frodi di identità. L'autore dell'attentato terroristico di Berlino del dicembre 2016, ad esempio, ha usato almeno 14 identità diverse ed è riuscito a passare da uno Stato membro all'altro senza essere individuato. Per bloccare questa strada ai terroristi e ai criminali vi è la chiara necessità che i sistemi di informazione dell'UE esistenti e futuri siano consultabili simultaneamente usando identificatori biometrici.

La Commissione ha avviato lavori a tale riguardo nell'aprile 2016 con le sue proposte per dei "sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza"[2]. Facendo questo ha individuato carenze nelle funzionalità dei sistemi esistenti, lacune nell'architettura della gestione dei dati dell'UE, problemi con il complesso mosaico di sistemi di informazione gestiti in maniera diversa, e una frammentazione generale causata dal fatto che i sistemi esistenti sono stati concepiti individualmente piuttosto che per funzionare insieme. Come parte di tale processo la Commissione ha varato il Gruppo di esperti di alto livello sui sistemi d'informazione e l'interoperabilità con le agenzie dell'UE, gli Stati membri e le parti interessate. Il 21 dicembre 2016[3] una relazione del presidente ha esposto i **risultati provvisori** del gruppo, che includono come opzione prioritaria la creazione di un unico portale di ricerca che consenta alle autorità di contrasto e alle autorità frontaliere di effettuare ricerche contemporanee nelle banche dati e nei sistemi informativi dell'UE esistenti. La relazione provvisoria sottolinea inoltre l'importanza della qualità dei dati – dato che l'efficacia dei sistemi di informazione dipende dalla qualità e dal formato dei dati che vi vengono inseriti – e formula raccomandazioni per migliorare tale qualità dei dati nei sistemi dell'UE con controlli automatizzati.

[2] Comunicazione intitolata "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza", COM(2016) 205 final.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

La Commissione darà rapido seguito all'opzione relativa alla creazione di un unico portale di ricerca e, insieme all'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), inizierà a lavorare a un portale in grado di effettuare ricerche parallele in tutti i sistemi esistenti europei pertinenti. Un studio collegato dovrebbe essere pronto per giugno, come base per ideare e testare un prototipo del portale entro la fine dell'anno. La Commissione ritiene che, parallelamente, Europol dovrebbe continuare i suoi lavori su un'interfaccia di sistema che consentirà agli agenti che operano in prima linea di consultare automaticamente e simultaneamente anche le banche dati di Europol quando effettuano ricerche nei propri sistemi nazionali.

I lavori finalizzati all'interoperabilità dei sistemi di informazione servono a porre rimedio all'attuale frammentazione dell'architettura della gestione dei dati per il controllo delle frontiere e la sicurezza e alle zone d'ombra che ne conseguono. Quando le banche dati usano un archivio comune per i dati relativi all'identità – come previsto dalle proposte relative al sistema UE di ingressi/uscite e al sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) – una persona può essere registrata nelle varie banche dati solo con un'unica identità, cosa che impedisce l'utilizzo di varie false identità. Come primo passo suggerito nei risultati provvisori del Gruppo di esperti di alto livello, la Commissione ha chiesto a eu-LISA di analizzare gli aspetti tecnici e operativi dell'attuazione di un servizio comune di confronto biometrico. Un servizio di questo tipo consentirebbe di effettuare ricerche in varie banche dati utilizzando dati biometrici, cosa che potrebbe far emergere false identità usate dalla persona in questione in un altro sistema. Oltre a ciò, il Gruppo di esperti di alto livello dovrebbe ora valutare se è necessario, tecnicamente fattibile e proporzionato estendere ad altri sistemi l'**archivio comune per i dati relativi all'identità** previsto per il sistema UE di ingressi/uscite e per ETIAS. Oltre ai dati biometrici conservati nel servizio di confronto biometrico, l'archivio comune per i dati relativi all'identità includerebbe anche dati di identità alfanumerici. Il gruppo dovrebbe presentare i propri risultati in merito a ciò nella sua relazione finale entro la fine di aprile 2017.

I recenti eventi che hanno compromesso la sicurezza sottolineano la necessità di riesaminare la questione dello **scambio obbligatorio di informazioni** fra Stati membri. La proposta della Commissione del dicembre 2016 di rafforzare il **Sistema d'informazione Schengen** prevede – per la prima volta – l'obbligo, per gli Stati membri, di introdurre segnalazioni per le persone legate a reati di terrorismo. È importante che il co-legislatore ora si adoperi per una rapida adozione delle misure proposte. La Commissione è pronta a esaminare l'opportunità di introdurre anche per altre banche dati dell'UE un obbligo vincolante di condivisione delle informazioni.

III. PROTEGGERE GLI OBIETTIVI NON STRATEGICI DAGLI ATTENTATI TERRORISTICI

L'attentato di Berlino è stato l'attacco più recente nell'UE diretto contro i cosiddetti obiettivi non strategici, che sono tipicamente siti civili in cui si concentrano un gran numero di persone (ad es. luoghi pubblici, ospedali, scuole, arene sportive, centri culturali, caffè e ristoranti, centri commerciali e snodi per i trasporti). Per loro natura, questi luoghi sono vulnerabili e difficili da proteggere. Ciò che li caratterizza, inoltre, è l'alta probabilità che un attentato vi possa mietere un gran numero di vittime. Per tutte queste ragioni sono obiettivi privilegiati dai terroristi. Come confermano le valutazioni disponibili, compresa la relazione di Europol sui cambiamenti del modus operandi del

Daesh[4], la minaccia di futuri attentati contro obiettivi non strategici, compresi i trasporti, resta alta.

L'Agenda europea sulla sicurezza del 2015 e la comunicazione sull'Unione della sicurezza del 2016 hanno evidenziato la necessità di intensificare i lavori per migliorare la sicurezza e l'uso di strumenti e di tecnologie di rilevamento innovativi per proteggere gli obiettivi non strategici. La Commissione si adopera per sostenere e incoraggiare la condivisione delle migliori prassi fra gli Stati membri sviluppando strumenti migliori per prevenire gli attentati agli obiettivi non strategici e per reagirvi. Questo lavoro ha prodotto manuali operativi e documenti di orientamento. Attualmente la Commissione sta elaborando, in stretta cooperazione con esperti degli Stati membri, un ampio manuale sulle procedure di sicurezza e i modelli applicabili ai vari obiettivi non strategici (ad es. centri commerciali, ospedali, manifestazioni sportive e culturali). Lo scopo è quello di pubblicare all'inizio del 2017 degli orientamenti sulla protezione degli obiettivi non strategici a uso degli Stati membri, sulla base delle loro migliori prassi.

Parallelamente, nel mese di febbraio, la Commissione organizzerà con le autorità nazionali il primo seminario sulla protezione degli obiettivi non strategici, allo scopo di scambiare informazioni e sviluppare migliori prassi su tale complessa questione così come sulla sicurezza e difesa pubblica. La Commissione sta inoltre finanziando un progetto pilota condotto da Belgio, Paesi Bassi e Lussemburgo nell'ambito del Fondo sicurezza interna per istituire un centro di eccellenza regionale per gli interventi speciali delle autorità di contrasto, che proporrà offrirà delle formazioni per gli agenti di polizia, che sono spesso i primi a intervenire in caso di attentati.

La reazione agli attentati contro gli obiettivi non strategici è una componenti principale del lavoro della Commissione in materia di protezione civile. Nel mese di dicembre la Commissione ha annunciato le azioni che intende portare avanti con gli Stati membri per proteggere i cittadini dell'UE e ridurre le vulnerabilità nei periodi immediatamente successivi agli attentati terroristici. Queste azioni rafforzeranno il coordinamento fra tutte le parti coinvolte nella gestione delle conseguenze di attentati, e la Commissione si è impegnata a sostenere gli sforzi degli Stati membri facilitando formazioni ed esercitazioni comuni e garantendo un dialogo continuo attraverso i punti di contatto e i gruppi d'esperti esistenti. La Commissione sosterrà anche lo sviluppo di moduli specializzati ai fini della reazione agli attentati terroristici nel quadro del meccanismo di protezione civile dell'Unione europea, e iniziative per condividere gli insegnamenti acquisiti e per fare opera di sensibilizzazione.

Insieme agli Stati membri, la Commissione esaminerà anche quale tipo di sostegno potrebbe essere mobilitato dall'UE per contribuire a creare resilienza e a rafforzare la sicurezza intorno ai potenziali obiettivi non strategici. Gli Stati membri potrebbero anche chiedere finanziamenti alla Banca europea per gli investimenti (BEI) (anche dal Fondo europeo per gli investimenti strategici) in linea con le politiche dell'UE e del gruppo BEI. Ogni progetto seguirebbe le normali procedure decisionali stabilite dalla legislazione.

---

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited* ("Modifiche del modus operandi dello Stati islamico – Relazione riveduta"), novembre 2016 – Pubblicazione di Europol, disponibile all'indirizzo: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

Per quanto riguarda gli specifici obiettivi non strategici legati alle zone pubbliche dei trasporti, come le aree pubbliche degli aeroporti o delle stazioni ferroviarie, l'apposito seminario organizzato dalla Commissione nel novembre 2016 con numerose parti interessate ha evidenziato la necessità di mantenere un equilibrio fra le esigenze di sicurezza, la convenienza dei passeggeri e le operazioni di trasporto. Le conclusioni sottolineano l'importanza di costruire una cultura della sicurezza che inglobi non solo il personale ma anche i passeggeri, la rilevanza delle valutazioni dei rischi a livello locale come base per definire contromisure appropriate e la necessità di rafforzare la comunicazione fra tutte le parti coinvolte.

IV. AFFRONTARE LA SFIDA DELLA MINACCIA INFORMATICA

La criminalità informatica e gli attacchi informatici sono sfide importanti che l'Unione deve affrontare, e un ambito in cui l'azione a livello dell'UE può contribuire a rafforzare la resilienza collettiva. Ogni giorno, incidenti che pregiudicano la sicurezza informatica hanno gravi conseguenze negative sulla vita dei cittadini e causano grossi dani economici all'economia e alle imprese europee. Gli attacchi informatici sono una componente essenziale delle minacce ibride: combinate in precisa corrispondenza temporale con le minacce fisiche, ad esempio se collegate al terrorismo, possono avere un impatto devastante. Possono anche contribuire a destabilizzare un paese o a mettere in difficoltà le istituzioni politiche e i processi democratici fondamentali. Poiché facciamo sempre più affidamento sulle tecnologie on-line, le nostre infrastrutture critiche (dagli ospedali alle centrali nucleari) diventeranno sempre più vulnerabili.

La strategia dell'Unione europea del 2013 per la cibersicurezza fa parte del nucleo delle misure di risposta alle sfide in materia di sicurezza informatica. L'elemento centrale è costituito dalla direttiva sulla sicurezza delle reti e dell'informazione (SRI)[5], adottata il luglio scorso. Essa pone le basi per un miglioramento della cooperazione a livello dell'UE e della ciberresilienza sostenendo la collaborazione e lo scambio di informazioni fra Stati membri, e promuovendo la cooperazione operativa in caso di specifici incidenti di cibersicurezza e la condivisione delle informazioni sui rischi. Per garantire un'attuazione coerente nei vari settori e oltre frontiera, la Commissione organizzerà nel mese di febbraio la prima riunione del Gruppo di cooperazione SRI con gli Stati membri.

Nell'aprile 2016, la Commissione e l'Alto rappresentante dell'UE hanno adottato un Quadro congiunto per contrastare le minacce ibride[6], che ha proposto 22 azioni operative volte alla sensibilizzazione, alla creazione di resilienza, a una migliore reazione alle crisi e al rafforzamento della cooperazione fra l'UE e la NATO. Come ha chiesto il Consiglio, la Commissione e l'Alto rappresentante dell'UE presenteranno una relazione entro luglio 2017 per valutare i progressi compiuti.

La Commissione sta anche promuovendo e sostenendo l'innovazione tecnologica, anche utilizzando i fondi per la ricerca dell'UE, per portare a nuove soluzioni e creare nuove tecnologie che possano contribuire a rafforzare la resilienza agli attacchi informatici (ad es. i progetti di "sicurezza fin dalla progettazione"). L'estate scorsa è stato varato un

[5] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[6] JOIN (2016)18.

partenariato pubblico-privato sulla cibersicurezza con l'industria per 1,8 miliardi di euro[7].

Nel settore dei trasporti, la digitalizzazione sta diventando il principale fattore grazie al quale può essere posta in atto la tanto necessaria trasformazione del sistema attuale. Il rapido ritmo della digitalizzazione apporta molti vantaggi, ma rende al tempo stesso i trasporti più vulnerabili ai rischi relativi alla sicurezza e alla protezione informatica. Per attenuare la minaccia a vari livelli, nello specifico l'aviazione ma anche il settore dei trasporti marittimi, fluviali ferroviari e stradali, vengono adottate numerose misure[8]. Resta la sfida di continuare a chiarire, armonizzare e completare le attività delle varie parti interessate impegnate nel rafforzamento dei vari aspetti della resilienza informatica.

Più in generale, e data la natura in rapida evoluzione delle minacce, nei mesi a venire la Commissione e l'Alto rappresentante dell'UE individueranno le azioni necessarie per apportare un'efficace risposta a livello dell'UE a queste minacce, basandosi sulla strategia dell'Unione europea del 2013 per la cibersicurezza.

V. PROTEGGERE I DATI PERSONALI SOSTENENDO AL TEMPO STESSO L'EFFICACIA DELLE INDAGINI PENALI

La direttiva sulla protezione dei dati in ambito di polizia e di giustizia penale[9] è uno dei mattoni della lotta contro il terrorismo e le forme gravi di criminalità. Sulla base di una normativa comune relativa alla protezione dei dati stabilita nella direttiva, le autorità di contrasto degli Stati membri potranno scambiarsi agevolmente dati rilevanti, proteggendo debitamente, al tempo stesso, le informazioni riguardanti le vittime, i testimoni e le persone sospettate.

Inoltre, per garantire un elevato livello di riservatezza delle comunicazioni sia per le persone che per le imprese, e parità di trattamento per tutti gli operatori di mercato, come stabilito nella strategia per il mercato unico digitale dell'aprile 2015, l'11 gennaio la Commissione ha adottato il proposto **regolamento sulla ePrivacy** (che sostituisce la direttiva 2002/58/CE)[10]. Così come l'attuale direttiva, il regolamento sulla ePrivacy

---

7 Annunciato nella comunicazione del 2016 sulla resilienza informatica, COM(2016) 410 final.

8 Ad esempio orientamenti internazionali, come quelli elaborati dall'Organizzazione marittima internazionale o con una risoluzione dell'ICAO recentemente adottata, su iniziativa congiunta dell'UE e degli USA; una segnalazione di incidenti, nell'ambito della quale l'Agenzia europea per la sicurezza aerea sta attualmente sviluppando una modalità più reattiva, e il concetto di sicurezza informatica fin dalla progettazione, applicabile ai nuovi sistemi in via di elaborazione, come il piano generale per la gestione del traffico aereo da parte dell'impresa comune SESAR.

9 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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. La direttiva, in vigore dal 5 maggio 2016, deve essere recepita dagli Stati membri entro il 6 maggio 2018. La Commissione ha istituito un gruppo di esperti con gli Stati membri per scambiarsi i punti di vista sul recepimento di tale direttiva.

10 Regolamento sulla vita privata e le comunicazioni elettroniche, COM(2017) 10.

rivisto precisa il regolamento generale sulla protezione dei dati[11] e stabilisce un quadro che disciplina la tutela della vita privata e dei dati personali nel settore delle comunicazioni elettroniche.

A seguito di questa revisione, tutti i dati delle comunicazioni elettroniche, anche quando la comunicazione è accessoria, sono considerati riservatissimi o riservati – che siano trasmessi attraverso servizi di telecomunicazione tradizionali o altri cosiddetti servizi over-the-top (OTT) che sono equivalenti sul piano funzionale (ad es. Skype e WhatsApp), e che spesso, per molti utenti, sono diventati interscambiabili con i normali operatori di telecomunicazioni[12]. Fra gli obblighi imposti ai fornitori di servizi – oltre a quello di rispettare le scelte relative alla vita privata dei loro clienti per quanto riguarda l'uso, la conservazione e il trattamento dei loro dati – vi è anche quello, per i fornitori stabiliti al di fuori dell'UE, di nominare un rappresentante in uno Stato membro. Questo darà agli Stati membri la possibilità di facilitare la cooperazione fra le autorità di contrasto e le autorità giudiziarie e i fornitori di servizi per quanto riguarda l'accesso alle prove elettroniche (vedi sotto).

Come avviene nel quadro delle attuali norme sulla vita privata e le comunicazioni elettroniche, l'accesso delle autorità di contrasto e delle autorità giudiziarie alle informazioni elettroniche rilevanti e necessarie ai fini delle indagini penali sarà disciplinato dall'eccezione di cui all'articolo 11 della proposta di regolamento ePrivacy[13]. Questa disposizione offre la possibilità, nel diritto dell'Unione o nel diritto nazionale, di limitare la riservatezza delle comunicazioni, ove necessario e proporzionato, per salvaguardare la sicurezza nazionale, la difesa, la sicurezza pubblica e la prevenzione, le indagini, l'accertamento e il perseguimento dei reati o l'esecuzione delle sanzioni penali. Questa disposizione è particolarmente rilevante per le norme nazionali relative alla **conservazione dei dati**, cioè per obbligare i fornitori di servizi di telecomunicazione a conservare i dati delle comunicazioni per un periodo preciso nell'ottica di un eventuale accesso da parte delle autorità di contrasto, a seguito dell'annullamento, da parte della Corte europea di giustizia, della direttiva sulla conservazione dei dati nel 2014.[14] Da allora non vi è alcuno strumento dell'Unione europea relativo alla conservazione dei dati, e alcuni Stati membri hanno adottato proprie leggi nazionali in materia. Le leggi svedese e britannica sulla conservazione dei dati sono state contestate dinanzi alla Corte europea di giustizia, che il 21 dicembre ha emesso la sentenza *Tele2*[15]. La Corte europea di giustizia ha ritenuto incompatibile con il diritto dell'Unione una legislazione nazionale che, per combattere la criminalità, prevede la

---

[11] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 (regolamento generale sulla protezione dei dati), che sarà applicabile a decorrere dal 25 maggio 2018.

[12] Questo segue l'approccio adottato nella proposta di direttiva che istituisce il codice europeo delle comunicazioni elettroniche, presentata dalla Commissione il 14 settembre 2016 (pacchetto sulle telecomunicazioni), COM(2016) 590 final.

[13] Si veda l'articolo 11, paragrafo 1, la "clausola sulla conservazione dei dati", che è invariata rispetto all'articolo 15 della direttiva ePrivacy e in linea con i requisiti del regolamento generale sulla protezione dei dati. Tale restrizione deve rispettare l'essenza dei diritti fondamentali ed essere necessaria, appropriata e proporzionata.

[14] Sentenza della Corte nelle cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, dell'8 aprile 2014.

[15] Sentenza della Corte nelle cause riunite C‑203/15 e C‑698/15, *Tele2*, del 21 dicembre 2016.

conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione degli abbonati e degli utenti per tutti i mezzi di comunicazione elettronica. Le implicazioni di questa decisione sono in corso d'analisi e la Commissione svilupperà degli orientamenti su come elaborare le leggi nazionali relative alla conservazione dei dati conformemente ad essa.

La commissione di reati lascia dietro di sé tracce digitali che possono servire come prove nei procedimenti giudiziari. Le comunicazioni elettroniche fra i sospetti sono spesso l'unico indizio che le autorità di contrasto e i pubblici ministeri possono raccogliere. Tuttavia, ottenere l'accesso alle **prove elettroniche** – specialmente se conservate all'estero o su una Nuvola – può essere complesso sia dal punto di vista tecnico che giuridico, e spesso oneroso dal punto di vista procedurale, cosa che ostacola le esigenze di rapida azione degli inquirenti. Per affrontare questi problemi, la Commissione sta attualmente valutando soluzioni che consentano agli inquirenti di ottenere prove elettroniche transfrontaliere, anche rendendo più efficace l'assistenza giudiziaria reciproca, trovando modalità di cooperazione diretta con i fornitori di servizi Internet, e proponendo criteri relativi alla determinazione e alla competenza esecutiva nel ciberspazio, nel pieno rispetto delle norme applicabili in materia di protezione dei dati[16]. La Commissione ha riferito al Consiglio "Giustizia e affari interni" del 9 dicembre 2016 in merito ai progressi compiuti[17].

Un ampio (e ancora in corso) processo di consultazione di esperti ha permesso alla Commissione di definire i diversi, spesso complessi, problemi che pone l'accesso alle prove elettroniche, di comprendere meglio le attuali norme e prassi degli Stati membri, e di individuare possibili opzioni d'azione. La relazione sui progressi compiuti fornisce un quadro generale delle idee emerse finora nel corso della raccolta delle informazioni e del processo di consultazione degli esperti, idee che la Commissione, di concerto con le parti interessate, esaminerà più approfonditamente nei prossimi mesi. Come ha annunciato nel suo programma di lavoro, la Commissione presenterà un'iniziativa a riguardo nel 2017.

VI. CONCLUSIONE

La prossima relazione, che dovrà essere presentata il 1° marzo, offrirà l'opportunità di analizzare i progressi realizzati nell'attuazione di questi ed altri importanti filoni di attività.

[16] Come si è impegnata a fare nell'Agenda europea sulla sicurezza, COM(2015) 185 final, e nella comunicazione dal titolo "Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per l'Unione della sicurezza", COM(2016) 230 final.

[17] Nelle sue conclusioni del 9 giugno 2016 sul miglioramento della giustizia penale nel ciberspazio, il Consiglio ha invitato la Commissione a prendere misure concrete, a sviluppare un approccio comune dell'UE e a presentare risultati entro giugno 2017.