Consiglio
dell'Unione europea

Bruxelles, 9 giugno 2016
(OR. en)

10007/16

JAI 552
COPEN 195
DROIPEN 109
CYBER 67
JAIEX 61
EJUSTICE 121

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	9 giugno 2016
Destinatario:	delegazioni
n. doc. prec.:	9579/16 + COR 1
Oggetto:	Progetto di conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciberspazio - Conclusioni del Consiglio (9 giugno 2016)

Si allegano per le delegazioni le conclusioni del Consiglio sul miglioramento della giustizia penale nel ciberspazio, adottate dal Consiglio nella sua 3473ª sessione, tenutasi il 9 giugno 2016.

ALLEGATO

Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciberspazio

DETERMINATI a negare ai criminali la possibilità di trovare un porto sicuro nel ciberspazio,

RILEVANDO il crescente impatto della criminalità informatica, dei reati favoriti dall'uso del ciberspazio o di qualsiasi altra attività criminale che lasci una traccia digitale nel ciberspazio,

SOTTOLINEANDO la crescente importanza delle prove elettroniche nei procedimenti penali per tutti i tipi di reati, in particolare quelli di terrorismo,

SOTTOLINEANDO l'importanza di proteggere il ciberspazio da abusi e attività criminali nell'interesse delle nostre economie e società e, di conseguenza, la necessità per le autorità di contrasto e giudiziarie di disporre di strumenti efficaci per indagare e perseguire atti criminali connessi al ciberspazio,

RICORDANDO che la lotta alla criminalità informatica figura tra le priorità dell'Agenda europea sulla sicurezza, del 28 aprile 2015, che comprende l'impegno della Commissione a riesaminare gli ostacoli alle indagini sulla criminalità informatica, in particolare le norme in materia di accesso alle prove e alle informazioni,

RAMMENTANDO la discussione svolta dai ministri della giustizia, in occasione del Consiglio "Giustizia e affari interni" del dicembre 2015, sulle sfide da affrontare per una giustizia penale efficace nell'era digitale[1],

RICORDANDO il sostegno espresso dai ministri della giustizia, nella riunione informale del Consiglio "Giustizia e affari interni" del 26 gennaio 2016, allo sviluppo di elementi concreti per un approccio comune dell'UE in materia di competenza nel ciberspazio,

[1] Doc. 14369/15.

RAMMENTANDO la dichiarazione comune dei ministri della giustizia e degli interni e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 2016, in cui si sottolinea la necessità di trovare, in via prioritaria, modalità per assicurare e ottenere più rapidamente ed efficacemente prove elettroniche, intensificando la cooperazione con i paesi terzi e con i fornitori di servizi operanti nel territorio europeo, al fine di migliorare la conformità con la legislazione dell'UE e degli Stati membri e i contatti diretti con le autorità incaricate dell'applicazione della legge, nonché di individuare misure concrete per affrontare questa complessa materia durante il Consiglio "Giustizia e affari interni" di giugno[2],

RICORDANDO la comunicazione al Parlamento europeo, al Consiglio europeo e al Consiglio, del 20 aprile 2016, relativa all'attuazione dell'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per un'Unione della sicurezza autentica ed efficace, nella quale la Commissione si è impegnata a proporre soluzioni per affrontare il problema dell'ottenimento di prove digitali connesse ad indagini penali,

PRENDENDO ATTO della relazione[3] della conferenza sulla competenza nel ciberspazio tenutasi il 7 e 8 marzo ad Amsterdam, che riflette le discussioni su possibili soluzioni per migliorare le indagini nel ciberspazio, in particolare per quanto riguarda le procedure di assistenza giudiziaria, la cooperazione con il settore privato e le indagini nel ciberspazio quando l'ubicazione dei dati o l'origine di attacchi informatici non sono (ancora) noti,

RILEVANDO l'adozione da parte del COSI di una serie di raccomandazioni per migliorare la cooperazione operativa nelle indagini penali nel ciberspazio[4],

RILEVANDO il settimo ciclo di valutazioni reciproche in corso dedicate all'attuazione pratica e al funzionamento delle politiche europee in materia di prevenzione e lotta alla criminalità informatica quale importante contributo agli sforzi per intensificare la lotta contro la criminalità informatica,

---

2 Doc. 7371/16.
3 Doc. 7323/16.
4 Cfr. doc. 8634/2/16 REV 2.

PRENDENDO ATTO dei risultati del riesame dell'accordo di assistenza giudiziaria UE-USA[5],

PRENDENDO ATTO delle conclusioni del Consiglio sulla rete giudiziaria europea per la criminalità informatica[6],

RICORDANDO la convenzione del Consiglio d'Europa sulla criminalità informatica, del 23 novembre 2001, e il relativo protocollo addizionale, che è promosso dall'Unione come quadro di riferimento globale per la lotta alla criminalità informatica,

RICORDANDO la direttiva 2014/41/UE relativa all'ordine europeo di indagine penale, che mira a rendere le indagini transfrontaliere in tutta l'UE più veloci ed efficaci, in particolare sulla base del riconoscimento reciproco, nonché la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, che invita gli Stati membri, tra l'altro, a predisporre un punto di contatto operativo nazionale nell'ambito delle reti di cooperazione esistenti attive h 24 - 7/7,

RICONOSCENDO che, sebbene tali strumenti offrano maggiori possibilità di attività di contrasto nel ciberspazio, permangono ostacoli pratici e giuridici, anche a causa della rapida evoluzione delle tecnologie, ad esempio nei casi in cui l'origine di attacchi informatici o l'ubicazione di prove elettroniche non sono (ancora) noti o sono mutevoli, ovvero nei casi in cui normative confliggenti ostacolano la cooperazione con fornitori di servizi,

RILEVANDO che la criminalità informatica e i reati favoriti dall'uso del ciberspazio violano i diritti e le libertà fondamentali e che è necessario garantire la piena tutela di tali diritti e libertà,

RICONOSCENDO che il ricorso ad atti d'indagine dovrebbe essere improntato alla tutela dei diritti e delle libertà fondamentali e ai principi di necessità e proporzionalità,

PRENDENDO ATTO dell'adozione degli strumenti UE di riforma della protezione dei dati, in particolare della direttiva concernente la tutela 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, e la libera circolazione di tali dati,

---

5 Doc. 9291/16.

6 Doc. 10025/16.

PRENDENDO ATTO delle relazioni 2012 e 2013 del gruppo transfrontaliero della commissione per la convenzione sulla criminalità informatica, da cui risulta che vari paesi praticano già l'accesso transfrontaliero ai dati al di là del campo di applicazione della convenzione di Budapest in forza di una base giuridica poco chiara,

RICONOSCENDO che gli Stati membri hanno un legittimo interesse a determinare nelle indagini penali, come minimo, l'ubicazione delle prove elettroniche o l'origine di un attacco informatico,

DETERMINATO ad agire per difendere lo stato di diritto nel ciberspazio,

IL CONSIGLIO DELL'UE,

RICONOSCE che è opportuno applicare gli orientamenti seguenti ai lavori futuri tesi a migliorare l'applicazione dello stato di diritto nel ciberspazio e ottenere prove elettroniche nei procedimenti penali:

- le soluzioni pratiche volte a migliorare l'efficace svolgimento dei procedimenti penali nel ciberspazio dovrebbero rispettare pienamente i quadri relativi alla protezione dei dati e ai diritti fondamentali;
- dovrebbero essere presi in considerazione il rafforzamento della cooperazione con i fornitori di servizi o qualsiasi altra soluzione analoga che consenta la rapida comunicazione dei dati; potrebbero essere previste procedure giuridiche meno rigorose per l'ottenimento di specifiche categorie di dati, in particolare i dati relativi agli abbonati, con possibili vantaggi per tutte le parti interessate;
- dovrebbero essere accelerate e semplificate le procedure di assistenza giudiziaria relative ai dati elettronici; il volume delle richieste di assistenza giudiziaria tra le autorità competenti potrebbe essere ridotto rafforzando la cooperazione con i fornitori di servizi, o attraverso qualsiasi altra soluzione analoga;

- le procedure di riconoscimento reciproco dovrebbero essere utilizzate in maniera efficiente per garantire l'assicurazione e l'ottenimento efficaci di prove elettroniche;
- dovrebbero essere prese in considerazione altre misure, sulla base di un esame dei criteri di collegamento per la competenza di esecuzione[7] nel ciberspazio, anche nei casi in cui l'ubicazione dei dati non sia (ancora) nota o sia mutevole.

RITIENE necessario cooperare con i paesi terzi e le parti private interessati ai fini dell'esplicazione degli effetti combinati di varie misure per un'efficace attività di contrasto nel ciberspazio.

RITIENE che lo sviluppo di un approccio comune dell'UE al miglioramento della giustizia penale nel ciberspazio debba essere considerato una priorità. I pertinenti lavori dovrebbero essere coerenti con quelli in corso nel quadro della convenzione di Budapest del Consiglio d'Europa.

CONCLUDE, PERTANTO, CHE:

I. LA COOPERAZIONE CON I FORNITORI DI SERVIZI DEVE ESSERE RAFFORZATA.

A tal fine,

1. si invita la COMMISSIONE a elaborare un quadro comune per la cooperazione con i fornitori di servizi allo scopo di ottenere specifiche categorie di dati, in particolare i dati relativi agli abbonati, se consentito dalla legislazione dei paesi terzi, o qualsiasi altra soluzione analoga che consenta una comunicazione rapida e legittima di tali dati[8]. La Commissione è invitata a procedere in tal senso in associazione con gli Stati membri e i paesi terzi interessati e in cooperazione con il settore privato.

---

[7] Ai fini delle presenti conclusioni, per "competenza di esecuzione" e "competenza esecutiva" s'intende la competenza delle autorità pertinenti a compiere un atto di indagine. Conformemente alle presenti conclusioni deve essere esplorato un approccio comune dell'UE volto a migliorare le indagini nel ciberspazio per situazioni specifiche in cui i quadri esistenti non sono sufficienti.

[8] Qualora una richiesta di dati comporti un trasferimento di dati personali da parte di un'autorità di uno Stato membro, deve essere rispettata la pertinente normativa sulla protezione dei dati.

2. Tali soluzioni dovrebbero enunciare requisiti stabiliti di comune accordo, compresi requisiti di necessità e proporzionalità per le richieste rivolte ai fornitori di servizi ai fini dell'accesso legittimo ai dati in loro possesso. Dovrebbero mirare a prevenire interpretazioni contrastanti e conflitti tra normative esistenti e affrontare la questione della mancata comunicazione dei dati richiesti. Le soluzioni proposte non devono essere di ostacolo a disposizioni a livello nazionale.

3. A tal fine, si invita la COMMISSIONE, in associazione con gli Stati membri, ad esplorare con i fornitori di servizi la possibilità di utilizzare moduli e strumenti armonizzati come quelli di cui alla sezione II al fine di agevolare l'autenticazione, garantire la rapidità delle procedure e aumentare la trasparenza del processo volto ad assicurare ed ottenere prove elettroniche nonché dell'assunzione di responsabilità per tale processo.

Si invita LA COMMISSIONE a presentare una relazione di valutazione sui progressi compiuti in materia entro dicembre 2016 e a presentare risultati entro giugno 2017.

II. LE PROCEDURE DI ASSISTENZA GIUDIZIARIA (E, SE DEL CASO, DI RICONOSCIMENTO RECIPROCO) DEVONO ESSERE SEMPLIFICATE.

A tal fine,

4. si invita la COMMISSIONE, in associazione con gli STATI MEMBRI e, se necessario, i paesi terzi, a trovare in via prioritaria modalità per assicurare ed ottenere prove elettroniche in modo più rapido ed efficace, semplificando l'uso delle procedure di assistenza giudiziaria e, se del caso, di riconoscimento reciproco.
5. A tale scopo, si invita la COMMISSIONE, in associazione con gli STATI MEMBRI, EUROJUST e i paesi terzi, a valutare e formulare raccomandazioni su come adeguare, se del caso, i moduli e le procedure standardizzati esistenti per chiedere di assicurare e ottenere prove elettroniche.
6. Per rendere più efficiente l'uso di tali moduli e procedure standardizzati per ottenere prove elettroniche, si invita la COMMISSIONE, in associazione con gli STATI MEMBRI, EUROJUST, la CEPOL e, se necessario, i paesi terzi, a sviluppare, utilizzando se del caso gli strumenti elettronici esistenti e rispettando le competenze e i canali di comunicazione previsti nell'ambito dei quadri giuridici esistenti:
    - un portale online protetto per le richieste e le risposte elettroniche riguardanti prove elettroniche e le corrispondenti procedure, incluso l'uso facoltativo della traduzione automatica di tali richieste, nonché per il loro tracciamento e monitoraggio;
    - orientamenti e moduli di formazione dedicati, in cooperazione con la rete europea di formazione giudiziaria, la rete giudiziaria europea per la criminalità informatica e, se necessario, le autorità dei paesi terzi , sull'uso efficiente dei quadri attuali utilizzati per assicurare ed ottenere prove elettroniche, inclusi orientamenti volti a chiarire quando, secondo le norme vigenti, non è richiesto il ricorso all'assistenza giudiziaria reciproca o a strumenti di riconoscimento reciproco.

Si invita la COMMISSIONE a presentare una relazione intermedia sui progressi di tali attività entro dicembre 2016 e a presentare risultati al più tardi entro giugno 2017. Si invita la COMMISSIONE a presentare il portale online entro dicembre 2017.

7. Si invita la COMMISSIONE, in associazione con gli STATI MEMBRI e, se necessario, i paesi terzi, a valutare ulteriori misure per assicurare ed ottenere prove elettroniche in modo più efficace, tramite il ricorso, tra l'altro, al quadro di assistenza giuridica UE-USA.
8. Si invita la COMMISSIONE, al fine di utilizzare appieno la direttiva 2014/41/UE relativa all'ordine europeo di indagine penale ("direttiva OEI") per assicurare ed ottenere prove elettroniche nell'UE, a continuare a monitorare e sostenere gli Stati membri nel processo di recepimento di detta direttiva da effettuare entro il 22 maggio 2017.
9. Gli STATI MEMBRI sono invitati a:
    - ratificare ed attuare pienamente la Convenzione sulla criminalità informatica del 23 novembre 2001;
    - recepire rapidamente la direttiva OEI, al più tardi entro il 22 maggio 2017;
    - garantire una capacità sufficiente per il trattamento delle richieste di assistenza giudiziaria relative a indagini nel ciberspazio e fornire al personale una formazione adeguata su come trattare tali richieste;
    - ottimizzare l'uso dei punti di contatto esistenti disponibili h 24 - 7/7 e aumentare il ricorso alle squadre investigative comuni, al fine di facilitare la condivisione delle informazioni e/o accelerare le procedure di assistenza giudiziaria.

III. È OPPORTUNO RIESAMINARE LE NORME SULLA COMPETENZA ESECUTIVA NEL CIBERSPAZIO.

A tal fine,

10. si invita la COMMISSIONE, alla luce degli orientamenti politici forniti dai ministri della giustizia nel Consiglio di giugno 2016 e in associazione con gli STATI MEMBRI, EUROJUST ed EUROPOL, a esaminare le possibilità di un approccio comune dell'UE in materia di competenza esecutiva nel ciberspazio in situazioni in cui i quadri esistenti non sono sufficienti, ad esempio situazioni in cui diversi sistemi di informazione sono utilizzati simultaneamente in più giurisdizioni per commettere un unico reato, situazioni in cui le pertinenti prove elettroniche si spostano tra giurisdizioni in brevi frazioni di tempo, o in cui sono usati metodi sofisticati per nascondere l'ubicazione di prove elettroniche o l'attività criminale, con conseguente "delocalizzazione".[9]
11. Tenendo conto delle specificità di ogni situazione, l'approccio dovrebbe determinare:

    - quali fattori di collegamento possano costituire criteri di competenza esecutiva nel ciberspazio;
    - se, ed eventualmente quali, atti d'indagine possano essere usati indipendentemente da frontiere fisiche.

12. È necessario prestare attenzione a quanto segue:

    - la natura e la gravità dei reati che potrebbero altrimenti restare impuniti;
    - i possibili criteri di competenza esecutiva, in particolare sulla base di fattori di collegamento quali, ad esempio, l'ubicazione della sede di un fornitore di servizi, l'attività economica di un fornitore di servizi nello stato che procede alle indagini, ossia quando il fornitore di servizi offre prodotti o servizi nel territorio dello Stato che procede alle indagini ("nesso economico"), la residenza abituale e/o la cittadinanza dell'indagato o dell'imputato, e/o il luogo in cui si trova la vittima;

[9] Si tratta di meri esempi. Si invita la Commissione ad esaminare soluzioni per affrontare situazioni di questo tipo o di pari gravità in grado di giustificare un tale approccio.

- l'uso e l'efficacia di ordini interni di produzione di dati basati su tali possibili criteri di collegamento per la competenza esecutiva nel ciberspazio;
- una soluzione di cooperazione per un accesso transfrontaliero diretto ai dati senza assistenza tecnica;
- le opportune salvaguardie, come la protezione dei diritti e delle libertà fondamentali e dei dati personali, e la proporzionalità e la sussidiarietà quali principi guida per l'uso di atti d'indagine volti a garantirne la legittimità;
- le possibili analogie con altri regimi giuridici transfrontalieri, ad es. il trattato sui cieli aperti e la convenzione sul diritto del mare, le norme dell'UE sulla protezione dei dati e il diritto UE in materia di concorrenza;
- gli effetti di un tale approccio sul quadro giuridico vigente.

Si invita LA COMMISSIONE a riferire sul processo di sviluppo di tale approccio entro dicembre 2016 e a presentare i risultati di detta valutazione entro giugno 2017. La valutazione dovrebbe includere elementi specifici per un approccio comune dell'UE e proposte per la sua realizzazione, inclusa la possibilità di promuovere un'iniziativa legislativa al riguardo.