Parlamento europeo
2014-2019

TESTI APPROVATI

P8_TA(2017)0366

Lotta alla criminalità informatica

Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068(INI))

Il Parlamento europeo,

– visti gli articoli 2, 3 e 6 del trattato sull'Unione europea (TUE),

– visti gli articoli 16, 67, 70, 72, 73, 75, 82, 83, 84, 87 e 88 del trattato sul funzionamento dell'Unione europea (TFUE),

– visti gli articoli 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 e 52 della Carta dei diritti fondamentali dell'Unione europea,

– vista la Convenzione delle Nazioni Unite sui diritti del fanciullo, del 20 novembre 1989,

– visto il protocollo opzionale alla convenzione sui diritti del fanciullo sulla vendita di bambini, la prostituzione dei bambini e la pornografia rappresentante bambini, del 25 maggio 2000,

– visti la dichiarazione e il piano d'azione di Stoccolma, adottati in occasione del primo Congresso mondiale contro lo sfruttamento sessuale dei minori a fini commerciali, l'impegno globale di Yokohama, adottato in occasione del secondo Congresso mondiale contro lo sfruttamento sessuale dei minori a fini commerciali, nonché l'impegno e il piano d'azione di Budapest, adottati in occasione della conferenza preparatoria in vista del secondo Congresso mondiale contro lo sfruttamento sessuale dei minori a fini commerciali,

– vista la convenzione del Consiglio d'Europa per la protezione dei bambini contro lo sfruttamento e gli abusi sessuali, del 25 ottobre 2007,

– vista la sua risoluzione del 20 novembre 2012 sulla tutela dei minori nel mondo digitale[1],

[1] GU C 419 del 16.12.2015, pag. 33.

– vista la sua risoluzione dell'11 marzo 2015 sull'abuso sessuale dei minori online[1],

– vista la decisione quadro del Consiglio 2001/413/GAI del 28 maggio 2001 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti[2],

– vista la convenzione del Consiglio d'Europa sulla criminalità informatica (convenzione di Budapest), del 23 novembre 2001[3], e il relativo protocollo aggiuntivo,

– visto il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione[4],

– vista la direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione[5],

– vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[6],

– vista la direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio[7],

– vista la comunicazione congiunta del 7 febbraio 2013 della Commissione e del vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dal titolo "Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro" (JOIN(2013)0001),

– vista la direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio[8],

– vista la direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, sull'ordine europeo di indagine penale[9] ("direttiva OEI"),

– vista la sentenza della Corte di giustizia dell'Unione europea (CGUE) dell'8 aprile 2014[10], che ha dichiarato invalida la direttiva sulla conservazione dei dati,

– vista la sua risoluzione del 12 settembre 2013 sulla strategia dell'Unione europea per la

---

1 GU C 316 del 30.8.2016, pag. 109.
2 GU L 149 del 2.6.2001, pag. 1.
3 Consiglio d'Europa, Serie Trattati europei n. 185, del 23.11.2001.
4 GU L 77 del 13.3.2004, pag. 1.
5 GU L 345 del 23.12.2008, pag. 75.
6 GU L 201 del 31.7.2002, pag. 37.
7 GU L 335 del 17.12.2011, pag. 1.
8 GU L 218 del 14.8.2013, pag. 8.
9 GU L 130 dell'1.5.2014, pag. 1.
10 ECLI:EU:C:2014:238.

cibersicurezza: un ciberspazio aperto e sicuro[1],

– vista la comunicazione della Commissione del 6 maggio 2015 intitolata "Strategia per il mercato unico digitale in Europa" (COM(2015)0192),

– vista la comunicazione della Commissione del 28 aprile 2015 dal titolo "Agenda europea sulla sicurezza" (COM(2015)0185) e la successiva relazione di verifica sullo stato di avanzamento dei lavori, dal titolo "Verso un'autentica ed efficace Unione della sicurezza",

– vista la relazione della conferenza sulla competenza nel ciberspazio tenutasi il 7 e 8 marzo 2016 ad Amsterdam,

– visto il 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)[2],

– vista la 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[3],

– visto il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (Europol)[4],

– vista la decisione della Commissione, del 5 luglio 2016, relativa alla firma di un accordo contrattuale per un partenariato pubblico-privato per la ricerca e l'innovazione industriale in materia di cibersicurezza tra l'Unione europea, rappresentata dalla Commissione, e l'organizzazione delle parti interessate (C(2016)4400),

– vista la comunicazione congiunta, del 6 aprile 2016, della Commissione e del vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio dal titolo "Quadro congiunto per contrastare le minacce ibride: la risposta dell'Unione europea" (JOIN(2016)0018),

– viste la comunicazione della Commissione dal titolo "Strategia europea per un'internet migliore per i ragazzi" (COM(2012)0196) e la relazione della Commissione, del 6 giugno 2016, dal titolo "Valutazione finale del programma pluriennale dell'UE per la protezione dei bambini che usano internet e altre tecnologie di comunicazione (programma Safer Internet)" (COM(2016)0364),

– vista la dichiarazione congiunta di Europol e dell'ENISA del 20 maggio 2016 sulle

---

1 GU C 93 del 9.3.2016, pag. 112.
2 GU L 119 del 4.5.2016, pag. 1.
3 GU L 119 del 4.5.2016, pag. 89.
4 GU L 135 del 24.5.2016, pag. 53.

indagini penali legittime che rispettano la protezione dei dati del XXI secolo,

– viste le conclusioni del Consiglio, del 9 giugno 2016, sulla rete giudiziaria europea per la criminalità informatica,

– vista la 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[1],

– visto il parere dell'ENISA del dicembre 2016 sulla cifratura e sulle garanzie che una cifratura forte offre alla nostra identità digitale,

– vista la relazione finale del T-CY Cloud Evidence Group del Consiglio d'Europa dal titolo "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY" (Accesso della giustizia penale alle prove elettroniche nel cloud: raccomandazioni per l'esame da parte del T-CY) del 16 settembre 2016,

– visto il lavoro della task force di azione congiunta contro la criminalità informatica (J-CAT),

– viste la valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA dell'UE), del 28 febbraio 2017, e la valutazione della minaccia della criminalità organizzata su Internet (IOCTA), del 28 settembre 2016, elaborate da Europol,

– vista la sentenza della CGUE nella causa C-203/15 (sentenza TELE2) del 21 dicembre 2016[2],

– vista la direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio[3],

– visto l'articolo 52 del suo regolamento,

– visti la relazione della commissione per le libertà civili, la giustizia e gli affari interni e il parere della commissione per il mercato interno e la protezione dei consumatori (A8-0272/2017),

A. considerando che la criminalità informatica provoca sempre più spesso notevoli danni sociali ed economici che interessano i diritti fondamentali delle persone fisiche, rappresenta una minaccia per lo Stato di diritto nel ciberspazio e mette a repentaglio la stabilità delle società democratiche;

B. considerando che la criminalità informatica è un problema in crescita negli Stati membri;

---

1 GU L 194 del 19.7.2016, pag. 1.

2 Sentenza della Corte di giustizia del 21 dicembre 2016, *Tele2 Sverige AB/Post- och telestyrelsen* e *Secretary of State for the Home Department/Tom Watson e a.*, C-203/15, ECLI:EU:C:2016:970.

3 GU L 88 del 31.3.2017, pag. 6.

C. considerando che la relazione IOCTA 2016 rivela che la criminalità informatica è in aumento per intensità, complessità e ampiezza, che in alcuni paesi dell'UE la criminalità informatica denunciata supera i reati tradizionali, che si estende ad altre sfere della criminalità quali la tratta di esseri umani, che l'uso degli strumenti di crittografia e anonimato a scopi criminali è in aumento e che gli attacchi di tipo ransomware superano le minacce legate ai malware tradizionali quali i trojan;

D. considerando che si registra un aumento del 20 % negli attacchi ai server della Commissione europea nel 2016 rispetto al 2015;

E. considerando che la vulnerabilità dei computer agli attacchi deriva dalle modalità uniche di sviluppo, nel corso degli anni, della tecnologia dell'informazione, dalla velocità di crescita delle aziende online e dalla mancata azione del governo;

F. considerando il costante aumento del mercato nero nell'estorsione informatica, l'uso di botner affittate e la pirateria e il furto di beni digitali;

G. considerando che gli attacchi informatici continuano a concentrarsi principalmente su malware, ad esempio i trojan bancari, ma si registra anche un aumento del numero e dell'impatto di attacchi contro i sistemi di controllo industriali e le reti mirati a distruggere infrastrutture cruciali e strutture economiche nonché a destabilizzare le società, come nel caso dell'attacco di tipo ransomware "WannaCry" del maggio 2017, che rappresentano pertanto una grave minaccia per la sicurezza, la difesa e altri settori importanti; che la maggior parte delle richieste internazionali di dati da parte delle autorità di contrasto riguardano le frodi e la criminalità finanziaria, seguite dalle forme gravi e violente di criminalità;

H. considerando che, sebbene la sempre crescente interconnessione di persone, luoghi e oggetti presenti molti benefici, aumenta il rischio di criminalità informatica; che i dispositivi collegati all'Internet delle cose (Internet of Things - IoT), tra cui reti intelligenti, frigoriferi connessi, automobili, strumenti o dispositivi medici, spesso non sono ben protetti come i dispositivi tradizionali connessi a Internet e costituiscono pertanto un obiettivo ideale per i criminali informatici, in particolare poiché il regime previsto per gli aggiornamenti di sicurezza dei dispositivi connessi è spesso frammentario o manca completamente; che i dispositivi oggetto di attacchi collegati all'IoT, i quali hanno o possono controllare attuatori fisici, possono rappresentare una minaccia concreta alla vita di esseri umani;

I. considerando che un quadro giuridico efficace per la protezione dei dati è fondamentale per rafforzare il senso di sicurezza e di fiducia nel mondo online, consentendo ai consumatori e alle imprese di sfruttare appieno i vantaggi del mercato unico digitale e di affrontare la criminalità informatica;

J. considerando che le aziende non possono affrontare da sole la sfida di rendere più sicuro il mondo connesso e che le amministrazioni pubbliche dovrebbero contribuire alla sicurezza informatica attraverso la regolamentazione e l'offerta di incentivi che incoraggino comportamenti più sicuri da parte degli utenti;

K. considerando che i confini tra reati informatici, spionaggio informatico, guerra informatica, sabotaggio informatico e terrorismo informatico diventano sempre più labili; che i crimini informatici possono prendere di mira persone, enti pubblici o privati

e coprono un'ampia gamma di reati, compresi la violazione della privacy, l'abuso sessuale di minori online, l'incitamento pubblico alla violenza e all'odio, il sabotaggio, lo spionaggio, i reati finanziari e la frode, ad esempio i pagamenti fraudolenti, i furti, anche di identità, nonché i sistemi di interferenza illecita;

L. considerando che la relazione sui rischi globali del Forum economico mondiale del 2017 elenca episodi su vasta scala di frode e furto di dati come uno dei cinque principali rischi globali in termini di probabilità;

M. considerando che un numero notevole di crimini informatici resta non perseguito o impunito; che vi sono ancora un numero significativo di reati non denunciati, lunghi periodi di rilevamento che permettono ai criminali informatici di sviluppare molteplici strategie di ingresso/uscita o backdoor, difficoltà di accesso alle prove elettroniche, problemi nell'ottenerle e nel farle ammettere in tribunale, come pure procedure complesse e sfide giurisdizionali connesse al carattere transfrontaliero della criminalità informatica;

N. considerando che il Consiglio, nelle sue conclusioni del giugno 2016, ha sottolineato che, dato il carattere transfrontaliero della criminalità informatica e le minacce comuni alla cibersicurezza cui deve far fronte l'UE, la cooperazione rafforzata e lo scambio di informazioni tra le autorità giudiziarie e di polizia ed esperti in materia di criminalità informatica sono essenziali per lo svolgimento di indagini efficaci nel ciberspazio e l'ottenimento di prove elettroniche;

O. considerando che l'annullamento della direttiva sulla conservazione dei dati da parte della CGUE nella sua sentenza dell'8 aprile 2014, nonché il divieto di conservazione generalizzata, indifferenziata e non mirata dei dati, confermato dalla decisione della CGUE nella sentenza TELE2 del 21 dicembre 2016, prevedono limiti rigorosi in materia di elaborazione in blocco di dati relativi a telecomunicazioni nonché di accesso delle autorità competenti a tali dati;

P. considerando che la sentenza Maximillian Schrems della CGUE[1] sottolinea che la sorveglianza di massa costituisce una violazione dei diritti fondamentali;

Q. considerando che la lotta alla criminalità informatica deve rispettare le stesse garanzie procedurali e sostanziali e gli stessi diritti fondamentali della lotta a qualsiasi altra sfera della criminalità, in particolare in merito alla protezione dei dati e alla libertà di espressione;

R. considerando che i minori utilizzano Internet ad un'età sempre più precoce e sono particolarmente vulnerabili a cadere vittime di adescamenti e altre forme di sfruttamento sessuale online (cyberbullismo, abuso sessuale, coercizione ed estorsione sessuale), appropriazione indebita di dati personali nonché pericolose campagne intese a promuovere vari atti di autolesionismo, come nel caso del "blue whale", e necessitano pertanto di una protezione speciale; che gli autori dei reati online possono trovare e adescare le vittime più rapidamente tramite chat, e-mail, giochi online e siti di social network, e le reti peer-to-peer (P2P) nascoste rimangono le piattaforme centrali utilizzate dai pedofili per trovare, trasmettere, conservare e condividere il materiale concernente lo sfruttamento sessuale dei minori e monitorare nuove vittime senza

[1] ECLI:EU:C:2015:650.

rischiare di essere scoperti;

S. considerando che la crescente tendenza ad atti di coercizione ed estorsione sessuale non è ancora sufficientemente studiata o denunciata, principalmente a causa della natura del reato, che causa sentimenti di vergogna e di colpa nella vittima;

T. considerando che l'abuso di minori a distanza in diretta è denunciato come una minaccia crescente; che l'abuso di minori a distanza in diretta presenta i legami più evidenti con la distribuzione a fini commerciali dei materiali concernenti lo sfruttamento sessuale di minori;

U. considerando che da un recente studio dell'agenzia nazionale per la lotta alla criminalità del Regno Unito è emerso che i più giovani coinvolti in attività di pirateria sono meno spinti da fini di lucro e spesso attaccano le reti informatiche per suscitare un'impressione positiva sugli amici o per sfidare un sistema politico;

V. considerando che è aumentata la consapevolezza dei rischi posti dai reati informatici, ma che le misure precauzionali prese dalle imprese, dalle istituzioni pubbliche e dai singoli utenti restano totalmente inadeguate, essenzialmente a causa della mancanza di conoscenza e di risorse;

W. considerando che la lotta alla criminalità informatica e alle attività illecite online non dovrebbe oscurare gli aspetti positivi derivanti da un ciberspazio libero e aperto, in grado di offrire nuove possibilità per la condivisione di conoscenze e la promozione dell'inclusione politica e sociale a livello mondiale;

Considerazioni generali

1. sottolinea che il netto aumento di ransomware, botnet e la manomissione non autorizzata di sistemi informatici ha un impatto sulla sicurezza dei singoli utenti, sulla disponibilità e sull'integrità dei loro dati personali, nonché sulla tutela della privacy e delle libertà fondamentali e sull'integrità delle infrastrutture critiche, ivi comprese, tra l'altro, le strutture di approvvigionamento di energia ed elettricità e le strutture finanziarie come la borsa; ricorda in tale contesto che la lotta alla criminalità informatica è una priorità riconosciuta nel quadro dell'Agenda europea sulla sicurezza del 28 aprile 2015;

2. sottolinea la necessità di semplificare le definizioni comuni di criminalità informatica, guerra informatica, sicurezza informatica, molestie online e attacchi informatici per garantire che le istituzioni e gli Stati membri dell'UE condividano una definizione giuridica comune;

3. sottolinea che la lotta alla criminalità informatica dovrebbe riguardare innanzitutto la tutela e il rafforzamento delle infrastrutture critiche e di altri dispositivi in rete e non solo l'attuazione di misure repressive;

4. ribadisce l'importanza delle misure giuridiche adottate a livello europeo per armonizzare la definizione dei reati connessi agli attacchi contro i sistemi d'informazione nonché allo sfruttamento e all'abuso sessuale di minori online e per obbligare gli Stati membri a istituire un sistema di registrazione, produzione e fornitura di dati statistici su tali reati onde accrescere l'efficienza delle azioni volte a contrastarli;

5. esorta vivamente gli Stati membri che non lo abbiano ancora fatto a recepire in modo tempestivo e adeguato la direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile; invita la Commissione a controllare e garantire attentamente la piena ed efficace attuazione della direttiva e a riferire senza indugio al Parlamento e alla sua commissione competente in merito ai risultati di tali controlli, sostituendo nel contempo la decisione quadro 2004/68/GAI del Consiglio; sottolinea che Eurojust ed Europol devono ricevere le risorse adeguate per migliorare l'identificazione delle vittime, per lottare contro le reti organizzate di autori di reati di abuso sessuale e per accelerare il rilevamento, l'analisi e la segnalazione di materiale pedopornografico online e offline;

6. deplora che l'80 % delle imprese in Europa abbia subito almeno un incidente di sicurezza informatica e che gli attacchi informatici contro le imprese spesso non siano individuati né denunciati; ricorda che diversi studi stimano il costo annuo degli attacchi informatici come significativo per l'economia mondiale; ritiene che l'obbligo di comunicare le violazioni di sicurezza e condividere le informazioni sui rischi, introdotto dal regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati) e la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva sulla sicurezza delle reti e dei sistemi informativi), contribuirà ad affrontare tale problema, fornendo sostegno per le imprese, in particolare le PMI;

7. sottolinea che il costante mutare del panorama delle minacce informatiche pone per tutte le parti interessate gravi sfide di ordine giuridico e tecnologico; ritiene che le nuove tecnologie non dovrebbero essere viste come una minaccia e riconosce che i progressi tecnologici in materia di crittografia miglioreranno la sicurezza complessiva dei nostri sistemi d'informazione, anche consentendo agli utenti finali di tutelare meglio i dati e le comunicazioni; rileva, tuttavia, che sussistono ancora notevoli lacune nel garantire la sicurezza delle comunicazioni e che tecniche quali onion routing e reti nascoste possono essere utilizzate da utenti malintenzionati, compresi terroristi e pedofili, hacker appoggiati da Stati stranieri ostili o organizzazioni politiche o religiose estremiste per scopi criminali, in particolare per nascondere la loro identità o le attività criminali, causando gravi problemi alle indagini;

8. è profondamente preoccupato per il recente attacco globale di tipo ransomware, che avrebbe colpito decine di migliaia di computer in circa 100 paesi e numerose organizzazioni, tra cui il servizio sanitario nazionale del Regno Unito, la vittima di più alto profilo di questo ampio attacco di tipo malware; riconosce, in questo contesto, l'importante lavoro dell'iniziativa No More Ransom (NMR) che offre oltre 40 strumenti gratuiti di decrittografia che consentono alle vittime di ransomware in tutto il mondo di decifrare i loro dispositivi colpiti;

9. sottolinea che le reti nascoste e l'onion routing offrono altresì uno spazio libero che consente ai giornalisti, ai sostenitori politici e ai difensori dei diritti umani in alcuni paesi di evitare di essere individuati dalle autorità statali repressive;

10. osserva che il ricorso, da parte delle reti criminali e terroristiche, a strumenti e servizi informatici è ancora limitato; sottolinea, tuttavia, che è probabile che questa situazione cambi alla luce dei crescenti legami tra terrorismo e criminalità organizzata e l'ampia disponibilità di armi da fuoco e di precursori per esplosivi nelle reti nascoste;

11. condanna fermamente qualsiasi interferenza del sistema intrapresa o guidata da una nazione straniera o dai suoi rappresentanti per arrestare il processo democratico di un altro paese;

12. sottolinea che le richieste transfrontaliere di confische del dominio, rimozioni di contenuti e accesso ai dati degli utenti implicano gravi sfide per le quali è necessaria un'azione urgente, dal momento che la posta in gioco è alta; sottolinea, in questo contesto, che i quadri internazionali in materia di diritti umani che si applicano online e offline rappresentano un importante parametro di riferimento a livello mondiale;

13. invita gli Stati membri a garantire che le vittime di attacchi informatici possano beneficiare pienamente di tutti i diritti sanciti dalla direttiva 2012/29/UE, e a intensificare i loro sforzi in relazione all'identificazione delle vittime e ai servizi incentrati sulle vittime, anche mediante un sostegno continuo alla task force di Europol per l'identificazione delle vittime; invita gli Stati membri, in cooperazione con Europol, ad istituire urgentemente piattaforme correlate con l'obiettivo di garantire che tutti gli utenti di Internet sappiano come chiedere aiuto quando sono vittime di attività illegali online; invita la Commissione a pubblicare uno studio sulle implicazioni della criminalità informatica transfrontaliera sulla base della direttiva 2012/29/UE;

14. sottolinea che la relazione IOCTA 2014 di Europol descrive la necessità di strumenti giuridici più efficaci ed efficienti, che tengano conto delle attuali limitazioni del processo del trattato di mutua assistenza giudiziaria (Mutual Legal Assistance Treaty – MLAT), e auspica un'ulteriore armonizzazione della legislazione nell'UE, se del caso;

15. sottolinea che la criminalità informatica minaccia gravemente il funzionamento del mercato unico digitale, riducendo la fiducia nei fornitori di servizi digitali, mettendo a rischio le transazioni transfrontaliere e compromettendo seriamente gli interessi dei consumatori di servizi digitali;

16. sottolinea che le strategie e le misure di sicurezza informatica possono essere valide ed efficaci solo se si basano sui diritti e sulle libertà fondamentali sanciti nella Carta dei diritti fondamentali dell'Unione europea e sui valori fondamentali dell'UE;

17. sottolinea la legittima e urgente necessità di proteggere le comunicazioni tra le persone e tra queste ultime e le organizzazioni pubbliche e private al fine di prevenire la criminalità informatica; sottolinea che una forte crittografia può contribuire a soddisfare tale necessità; sottolinea inoltre che la limitazione dell'utilizzo degli strumenti crittografici o l'indebolimento della loro forza creerà vulnerabilità che possono essere sfruttate per fini criminali e ridurrà la fiducia nei servizi elettronici, il che, a sua volta, danneggerà la società civile e l'industria;

18. chiede un piano d'azione per tutelare i diritti dei minori online e offline nel ciberspazio e rammenta che le autorità preposte all'applicazione della legge devono prestare particolare attenzione ai reati contro i minori nelle loro attività di lotta alla criminalità informatica; sottolinea, a tale proposito, che è necessario rafforzare la cooperazione giudiziaria e di polizia tra gli Stati membri nonché con Europol e il suo Centro europeo per la lotta alla criminalità informatica (EC3), allo scopo di prevenire e combattere la criminalità informatica e in particolare lo sfruttamento sessuale dei minori online;

19. esorta la Commissione e gli Stati membri a mettere in atto tutte le misure giuridiche per

contrastare il fenomeno online della violenza contro le donne e del bullismo; chiede in particolare all'UE e agli Stati membri di unire le forze per creare un quadro di illeciti penali che obblighi le imprese online a cancellare o bloccare la diffusione di contenuti degradanti, offensivi e umilianti; chiede altresì di offrire sostegno psicologico alle donne vittime della violenza online e alle ragazze oggetto di bullismo online;

20. sottolinea che è opportuno eliminare immediatamente i contenuti illeciti online sulla base di una regolare procedura legale; pone l'accento sul ruolo delle tecnologie dell'informazione e della comunicazione, dei fornitori di servizi Internet e dei fornitori di Internet hosting nel garantire la celere ed efficace eliminazione dei contenuti illeciti online, su richiesta della competente autorità di contrasto;

Prevenzione

21. invita la Commissione, nel contesto della revisione della strategia europea della sicurezza informatica, a continuare a individuare le vulnerabilità, sul piano della sicurezza delle reti e dell'informazione, delle infrastrutture critiche europee, a incentivare l'elaborazione di sistemi resilienti e a valutare la situazione relativa alla lotta alla criminalità informatica nell'UE e negli Stati membri per acquisire una migliore comprensione delle tendenze e degli sviluppi in relazione ai reati nel ciberspazio;

22. sottolinea che la resilienza informatica è essenziale per la prevenzione della criminalità informatica e che occorre pertanto darvi la massima priorità; invita gli Stati membri ad adottare politiche e azioni proattive volte alla difesa delle reti e delle infrastrutture critiche e chiede un approccio globale europeo alla lotta alla criminalità informatica che sia compatibile con i diritti fondamentali, la protezione dei dati, la sicurezza informatica, la protezione dei consumatori e il commercio elettronico;

23. accoglie con favore, a tale riguardo, l'investimento di fondi dell'UE in progetti di ricerca quali il partenariato pubblico-privato (PPP) sulla sicurezza informatica inteso a promuovere la resilienza informatica attraverso l'innovazione e lo sviluppo di capacità; riconosce in particolare gli sforzi compiuti dal PPP sulla sicurezza informatica per elaborare risposte adeguate alla gestione delle vulnerabilità "zero-day";

24. sottolinea, al riguardo, l'importanza del software libero e open source; chiede di mettere a disposizione maggiori fondi dell'UE in particolare per la ricerca basata sul software libero e open source a favore della sicurezza informatica;

25. rileva con preoccupazione l'assenza di professionisti informatici qualificati che operano nel settore della sicurezza informatica; esorta gli Stati membri a investire nell'istruzione;

26. ritiene che la regolamentazione debba svolgere un ruolo maggiore nella gestione dei rischi legati alla sicurezza informatica attraverso il miglioramento delle norme di prodotto e software sulla progettazione e sui successivi aggiornamenti, nonché norme minime sui nomi utente e sulle password predefiniti;

27. esorta gli Stati membri a intensificare lo scambio di informazioni tramite Eurojust, Europol ed ENISA, nonché la condivisione delle prassi eccellenti attraverso la rete europea per la sicurezza informatica in caso di incidente (CSIRT) e i gruppi di pronto intervento informatico (*Computer Emergency Response Teams* – CERT) riguardo alle sfide con cui devono misurarsi nella lotta alla criminalità informatica, nonché alle

soluzioni giuridiche e tecniche concrete per affrontarle e rafforzare la resilienza informatica; invita, al riguardo, la Commissione a promuovere la cooperazione efficace e ad agevolare lo scambio di informazioni al fine di anticipare e gestire eventuali rischi, secondo quanto previsto dalla direttiva SRI;

28. è preoccupato che Europol abbia riscontrato che la maggior parte degli attacchi riusciti contro le persone sono imputabili alla mancanza di "igiene digitale" e a una scarsa avvedutezza degli utenti o all'attenzione insufficiente prestata alle misure di sicurezza tecnica, quali ad esempio la sicurezza fin dalla progettazione; sottolinea che gli utenti sono le prime vittime della sicurezza inadeguata dell'hardware e del software;

29. invita la Commissione e gli Stati membri ad avviare una campagna di sensibilizzazione che coinvolga tutte le parti interessate e tutti gli attori pertinenti e miri a responsabilizzare i minori e a sostenere i genitori, i tutori e gli educatori nella comprensione e nella gestione dei rischi online nonché nella tutela della sicurezza dei minori online, a sostenere gli Stati membri nell'istituzione di programmi di prevenzione degli abusi sessuali online, a promuovere campagne di sensibilizzazione per un comportamento responsabile sui social media e a incoraggiare i principali motori di ricerca e le reti di social media ad adottare un approccio proattivo in termini di tutela della sicurezza dei minori online;

30. invita la Commissione e gli Stati membri ad avviare campagne di sensibilizzazione, di informazione e di prevenzione e a promuovere le buone pratiche per garantire che i cittadini, in particolare i minori e gli altri utenti vulnerabili, ma anche le amministrazioni centrali e le collettività territoriali, gli operatori di importanza fondamentale e gli attori del settore privato, in particolare le PMI, siano consapevoli dei rischi posti dalla criminalità informatica e sappiano navigare su internet in tutta sicurezza e proteggere i propri dispositivi; invita la Commissione e gli Stati membri a promuovere misure pratiche di sicurezza, quali la cifratura o altre tecnologie a sostegno della sicurezza e della vita privata;

31. sottolinea che le campagne di sensibilizzazione debbono essere accompagnate da programmi educativi in merito a un "utilizzo consapevole" degli strumenti informatici; incoraggia gli Stati membri a includere la sicurezza informatica, nonché i rischi e le conseguenze dell'utilizzo dei dati personali online, nei programmi scolastici di informatica; sottolinea, in tale contesto, gli sforzi compiuti nell'ambito della Strategia europea per un'internet migliore per i ragazzi (strategia BIK 2012);

32. sottolinea l'urgente necessità, nella lotta alla criminalità informatica, di prevedere maggiori sforzi nel campo dell'istruzione e della formazione in materia di sicurezza delle reti e dell'informazione, introducendo corsi di formazione sulla sicurezza delle reti e dell'informazione, sullo sviluppo di software sicuro e sulla protezione dei dati personali per gli studenti di informatica, nonché corsi di formazione di base in materia di sicurezza delle reti e dell'informazione per il personale della pubblica amministrazione;

33. ritiene che l'assicurazione contro la pirateria informatica possa essere uno degli strumenti che incentivano l'azione in materia di sicurezza sia da parte delle aziende ritenute responsabili della progettazione del software sia da parte degli utenti indotti a utilizzare il software adeguatamente;

34. sottolinea che le imprese dovrebbero individuare le vulnerabilità e i rischi tramite valutazioni periodiche, tutelare i loro prodotti e servizi eliminando senza indugio le vulnerabilità rilevate, anche attraverso politiche di gestione dei patch e aggiornamenti per la protezione dei dati, attenuare gli effetti degli attacchi perpetrati per mezzo di ransomware provvedendo alla messa a punto di robusti sistemi di backup, e denunciare in modo coerente gli attacchi informatici;

35. esorta gli Stati membri a istituire CERT cui le imprese e i consumatori possono denunciare i messaggi di posta elettronica e i siti web malintenzionati, come previsto dalla direttiva sulla sicurezza delle reti e dell'informazione, in modo che gli Stati membri siano regolarmente informati degli incidenti di sicurezza e delle misure volte contrastare e attenuare il rischio per i loro sistemi; incoraggia gli Stati membri a valutare la possibilità di creare una banca dati per registrare tutte le tipologie di criminalità informatica e monitorare l'andamento dei pertinenti fenomeni;

36. esorta gli Stati membri a investire per rendere le loro infrastrutture critiche e i relativi dati più sicuri per poter resistere ad attacchi informatici;

Maggiore responsabilità dei fornitori di servizi

37. ritiene che una maggiore cooperazione tra le autorità competenti e i fornitori di servizi sia un fattore chiave per accelerare e razionalizzare l'assistenza giuridica reciproca e le procedure di riconoscimento reciproco, nell'ambito del mandato previsto dal quadro giuridico europeo; invita i fornitori di servizi di comunicazione elettronica non stabiliti nell'Unione a designare per iscritto rappresentanti nell'Unione;

38. ribadisce che, per quanto riguarda l'Internet degli oggetti (IoT), i produttori rappresentano il punto di partenza fondamentale per rafforzare i regimi di responsabilità, il che condurrà a una migliore qualità dei prodotti e garantirà un ambiente più sicuro in termini di accesso esterno e un servizio documentato di aggiornamento;

39. ritiene che, alla luce delle tendenze innovative e della crescente accessibilità dei dispositivi per l'internet degli oggetti, occorra prestare particolare attenzione alla sicurezza di tutti i dispositivi, anche di quelli più semplici; ritiene che sia nell'interesse dei produttori e degli sviluppatori di software innovativo di investire in soluzioni volte a prevenire la criminalità informatica e a scambiare informazioni in materia di minacce alla sicurezza informatica; esorta la Commissione e gli Stati membri a promuovere l'approccio della sicurezza fin dalla progettazione ed esorta le imprese del settore a includere soluzioni basate su tale approccio in tutti i dispositivi in questione; incoraggia, in tale contesto, il settore privato ad attuare misure volontarie definite sulla base della legislazione dell'UE in materia quale la direttiva SRI e allineate alle norme riconosciute a livello internazionale onde rafforzare la fiducia nella sicurezza dei software e dei dispositivi, come il marchio di fiducia IoT;

40. incoraggia i fornitori di servizi ad aderire al Codice di condotta per contrastare l'illecito incitamento all'odio online e invita la Commissione e le aziende partecipanti a continuare la cooperazione in materia;

41. ricorda che la direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società

dell'informazione, in particolare il commercio elettronico, nel mercato interno[1] (direttiva sul commercio elettronico), esonera gli intermediari dalla responsabilità per il contenuto soltanto se svolgono un ruolo neutro e passivo in relazione al contenuto trasmesso e/o ospitato ma esige altresì una reazione celere per rimuovere o disabilitare l'accesso ai contenuti qualora un intermediario sia realmente a conoscenza di una violazione o di un'attività o informazione illecita;

42. sottolinea l'assoluta necessità di proteggere le banche dati delle autorità di contrasto dagli incidenti di sicurezza e dall'accesso illecito, dal momento che tale questione desta preoccupazione tra i cittadini; esprime preoccupazione per la portata extraterritoriale dell'accesso ai dati da parte delle autorità di contrasto nel contesto delle indagini penali e sottolinea la necessità di attuare norme rigorose in materia;

43. ritiene che le questioni legate alle attività illegali online vadano affrontate in maniera rapida ed efficace, anche mediante procedure di rimozione se il contenuto non risulta o non risulta più necessario ai fini di accertamento, indagine e perseguimento; ricorda che gli Stati membri possono, allorché la rimozione risulta impossibile, adottare misure necessarie e proporzionate per bloccare l'accesso a tali contenuti a partire dal territorio dell'Unione; sottolinea la necessità che tali misure siano conformi alle procedure legislative e giudiziarie vigenti, nonché con la Carta, e siano soggette a garanzie adeguate, tra cui la possibilità di ricorso giudiziario;

44. sottolinea il ruolo dei fornitori di servizi della società dell'informazione digitale nel garantire la celere ed efficiente rimozione dei contenuti illeciti online, su richiesta della competente autorità di contrasto, e si compiace dei progressi compiuti al riguardo, anche attraverso il contributo del Forum dell'UE su Internet; sottolinea la necessità di un maggiore impegno e cooperazione delle autorità competenti e dei fornitori di servizi della società dell'informazione ai fini della rimozione rapida ed efficace da parte delle imprese del settore ed evitare il blocco dei contenuti illeciti in virtù di misure governative; invita gli Stati membri a obbligare le piattaforme non conformi a risponderne dinanzi alla legge; ribadisce che eventuali misure per rimuovere contenuti illeciti online che prevedono termini e condizioni debbano essere autorizzate soltanto se le norme procedurali nazionali prevedono la possibilità per gli utenti di far valere i propri diritti dinanzi a un tribunale dopo essere venuti a conoscenza di tali misure;

45. sottolinea che, conformemente alla propria risoluzione del 19 gennaio 2016 sul tema "Verso un atto sul mercato unico digitale"[2], la responsabilità limitata degli intermediari è essenziale per la protezione dell'apertura di Internet, i diritti fondamentali, la certezza del diritto e l'innovazione; plaude all'intenzione della Commissione di fornire orientamenti sulle procedure di notifica e di rimozione, per aiutare le piattaforme online a rispettare le loro responsabilità e le norme in materia di responsabilità definite dalla direttiva sul commercio elettronico (2000/31/CE), al fine di rafforzare la certezza del diritto e rafforzare la fiducia degli utenti; esorta la Commissione a presentare una proposta legislativa in materia;

46. chiede l'applicazione dell'approccio "segui il denaro", come indicato nella propria risoluzione del 9 giugno 2015 sul tema "Verso un rinnovato consenso sul rispetto dei

---

1 GU L 178 del 17.7.2000, pag. 1.
2 Testi approvati, P8_TA(2016)0009.

diritti di proprietà intellettuale: Piano d'azione dell'Unione europea"[1], basato sul quadro normativo della direttiva sul commercio elettronico e la direttiva IPRED;

47. sottolinea l'importanza cruciale di fornire formazione continua e specifica e sostegno psicologico ai moderatori di contenuti in enti pubblici e privati che sono competenti per la valutazione di contenuti contestabili o illeciti online, poiché essi dovrebbero essere considerati i primi rispondenti in questo settore;

48. invita i fornitori di servizi a prevedere chiare modalità di notifica e un'infrastruttura di backoffice ben definita, in grado di garantire un seguito rapido e adeguato alle segnalazioni;

49. invita i fornitori di servizi ad adoperarsi al fine di intensificare le attività di sensibilizzazione dei rischi online, segnatamente per quanto concerne i minori, sviluppando strumenti interattivi e materiale informativo;

Intensificare la cooperazione di polizia e giudiziaria

50. è preoccupato per il fatto che un numero considerevole di crimini informatici restano impuniti; deplora che l'adozione, da parte dei fornitori di accesso a Internet, di tecnologie quali le NAT CGN comprometta seriamente le indagini, rendendo tecnicamente impossibile l'identificazione precisa dell'utente di un indirizzo IP e, di conseguenza, l'attribuzione di reati online; sottolinea la necessità di consentire alle autorità di contrasto di accedere legalmente alle informazioni pertinenti in circostanze limitate laddove tale accesso sia necessario e proporzionato per ragioni di sicurezza e giustizia; sottolinea la necessità che le autorità giudiziarie e di contrasto siano dotate di sufficienti capacità e finanziamenti per condurre indagini legittime;

51. esorta gli Stati membri a non imporre alcun obbligo ai fornitori di servizi di crittografia che indebolisca o comprometta la sicurezza delle loro reti e dei loro servizi quale la creazione o l'agevolazione di backdoor; sottolinea la necessità di offrire soluzioni fattibili sia tramite la legislazione che mediante l'evoluzione tecnica continua, qualora tali soluzioni siano indispensabile per ragioni di giustizia e sicurezza; invita gli Stati membri a cooperare, di concerto con la magistratura ed Eurojust, sul ravvicinamento delle condizioni per l'uso corretto degli strumenti di indagine online;

52. sottolinea che l'intercettazione lecita può essere una misura estremamente efficace per combattere la pirateria illecita, purché sia necessaria, proporzionata, basata sulla regolare procedura legale e nel pieno rispetto dei diritti fondamentali e della normativa e giurisprudenza dell'UE in materia di protezione dei dati; invita tutti gli Stati membri ad avvalersi delle possibilità offerte dall'intercettazione lecita nei confronti di individui sospetti, a definire norme chiare concernenti la procedura di autorizzazione preliminare e giudiziaria per le attività di intercettazione lecite, comprese le restrizioni sull'uso e la durata degli strumenti di pirateria leciti, a istituire un meccanismo di controllo e fornire mezzi di ricorso efficaci per i soggetti interessati da attività di pirateria;

53. incoraggia gli Stati membri a interagire con la comunità della sicurezza delle TIC e di incoraggiarla a svolgere un ruolo più attivo nella cosiddetta "pirateria etica" e la segnalazione di contenuti illegali, come il materiale contenente abusi sessuali su minori;

---

[1] GU C 407 del 4.11.2016, pag. 25.

54. incoraggia Europol a porre in essere un sistema di denuncia anonima dall'interno delle reti nascoste, che consenta alle persone di denunciare alle autorità contenuti illeciti, quali rappresentazioni di materiale contenente violenze sessuali su minori, utilizzando le stesse garanzie tecniche attuate da molti organi di stampa che impiegano sistemi analoghi per agevolare lo scambio di dati sensibili con giornalisti in modo da consentire un maggiore grado di anonimato e sicurezza rispetto a quanto possibile con l'e-mail tradizionale;

55. evidenzia la necessità di ridurre al minimo i rischi per la privacy degli utenti di Internet dovuti alle fughe di exploit o di strumenti impiegati dalle autorità di contrasto nel quadro delle loro legittime indagini;

56. sottolinea che le autorità giudiziarie e di contrasto devono essere dotate di sufficienti capacità e finanziamenti che consenta loro di rispondere efficacemente alla criminalità informatica;

57. sottolinea che il mosaico di giurisdizioni nazionali distinte e definite in base al territorio rende difficile determinare la legge applicabile nelle interazioni transnazionali e dà luogo a incertezza giuridica, impedendo in tal modo la cooperazione transfrontaliera necessaria per gestire in modo efficace la criminalità informatica;

58. sottolinea la necessità di sviluppare elementi concreti per un approccio comune dell'UE in materia di giurisdizione nel ciberspazio, come sottolineato in occasione della riunione informale dei ministri della giustizia e degli affari interni del 26 gennaio 2016;

59. sottolinea, al riguardo, la necessità di sviluppare norme procedurali condivise in grado di determinare i fattori territoriali che giustificano la legislazione applicabile al ciberspazio e definire misure investigative che possano essere utilizzate a prescindere dai confini geografici;

60. riconosce che un approccio europeo comune di questo tipo, che deve rispettare i diritti fondamentali e la privacy, creerà un clima di fiducia tra le parti interessate, ridurrà i ritardi nel trattamento delle richieste transfrontaliere, istituirà l'interoperabilità tra attori eterogenei e offrirà l'opportunità di integrare i requisiti del giusto processo nei quadri operativi;

61. ritiene che, nel lungo periodo, le norme procedurali condivise in materia di competenza esecutiva nel ciberspazio dovranno essere definite a livello mondiale; accoglie con favore, al riguardo, il lavoro svolto dal Cloud Evidence Group del Consiglio d'Europa;

Prove elettroniche

62. sottolinea che un approccio comune europeo alla giustizia penale nel ciberspazio è prioritario, in quanto consentirà di migliorare l'applicazione dello stato di diritto nel ciberspazio e agevolare l'ottenimento di prove elettroniche nei procedimenti penali, oltre a contribuire alla conclusione delle cause molto più velocemente di quanto sia possibile oggi;

63. sottolinea la necessità di trovare le risorse per ottenere prove elettroniche in maniera più rapida, come pure l'importanza di una stretta cooperazione tra le autorità di contrasto, anche mediante un maggiore ricorso alle squadre investigative comuni, i paesi terzi e i fornitori di servizi operanti nel territorio europeo, in conformità del regolamento

generale sulla protezione dei dati (UE) 2016/679, della direttiva (UE) 2016/680 (direttiva di polizia) e degli accordi di mutua assistenza giudiziaria; sottolinea la necessità di istituire sportelli unici in tutti gli Stati membri e di ottimizzare l'uso dei punti di contatto esistenti, in modo da agevolare l'accesso alle prove elettroniche nonché lo scambio di informazioni, migliorare la cooperazione con i fornitori di servizi e accelerare le procedure di mutua assistenza giudiziaria;

64. riconosce che l'attuale quadro giuridico frammentato può creare difficoltà per i prestatori di servizi che intendono soddisfare le richieste dei servizi di contrasto; invita la Commissione a proporre un quadro giuridico europeo in materia di prove elettroniche, tra cui norme armonizzate per determinare se un prestatore di servizi possa considerarsi nazionale o estere, e a imporre ai prestatori di servizi l'obbligo di rispondere a richieste provenienti da altri Stati membri basate su regolare procedura legale e in linea con l'ordine europeo di indagine (OEI), tenendo conto del principio di proporzionalità per evitare effetti negativi sull'esercizio della libertà di stabilimento e la libera prestazione di servizi e garantire adeguate garanzie, al fine di garantire la certezza del diritto e migliorare la capacità dei prestatori di servizi e degli intermediari di rispondere alle richieste dei servizi di contrasto;

65. sottolinea la necessità di un quadro in materia di prove elettroniche che comprenda garanzie sufficienti per i diritti e le libertà di tutti gli interessati; mette in evidenza che ciò dovrebbe comprendere un requisito in base al quale le richieste di prove elettroniche siano trasmesse in primo luogo ai titolari del trattamento dei dati o ai proprietari dei dati, al fine di assicurare il rispetto dei loro diritti, nonché dei diritti di coloro cui i dati fanno riferimento (per esempio il loro diritto di far valere il segreto professionale forense e di presentare ricorso in caso di accesso sproporzionato o altrimenti illecito); sottolinea altresì la necessità di garantire che eventuali quadri giuridici tutelino i prestatori di servizi e tutte le altre parti dalle richieste che possano creare conflitti di leggi o altrimenti pregiudicare la sovranità di altri Stati;

66. invita gli Stati membri ad attuare pienamente la direttiva 2014/41/UE sull'ordine europeo di indagine penale ("direttiva OEI"), al fine di garantita l'efficace messa in sicurezza e l'ottenimento di prove elettroniche nell'UE, nonché a prevedere disposizioni specifiche relative al ciberspazio nei rispettivi codici penali nazionali per agevolare l'ammissibilità delle prove elettroniche nei tribunali e formulare indicazioni più chiare per i giudici per quanto riguarda la punibilità della criminalità informatica;

67. accoglie con favore l'attuale lavoro della Commissione mirato a una piattaforma di cooperazione con un canale di comunicazione sicuro per gli scambi digitali degli OEI per le prove elettroniche e le risposte tra le autorità giudiziarie dell'UE; invita la Commissione, in collaborazione con gli Stati membri, Eurojust e i prestatori di servizi, a esaminare e allineare i moduli, gli strumenti e le procedure per richiedere la conservazione e l'ottenimento di prove elettroniche al fine di agevolare l'autenticazione, assicurare procedure rapide e aumentare la trasparenza e la rendicontabilità del processo di garanzia della conservazione e dell'ottenimento di prove elettroniche; invita l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL) a sviluppare moduli di formazione sull'uso efficace dei quadri attuali utilizzati per conservare e ottenere prove elettroniche; sottolinea, in questo contesto, che la razionalizzazione delle politiche dei prestatori di servizi contribuirà a ridurre l'eterogeneità degli approcci, segnatamente in merito alle procedure e alle condizioni per la concessione dell'accesso ai dati richiesti;

Sviluppo di capacità a livello europeo

68. sottolinea che i recenti episodi hanno dimostrato chiaramente la forte vulnerabilità dell'UE, e in particolare delle istituzioni dell'Unione, dei governi e parlamenti nazionali, delle principali società europee, delle infrastrutture e delle reti informatiche europee, agli attacchi sofisticati che utilizzano software e malware complessi; invita l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) a valutare continuamente il livello di minaccia e la Commissione investire nella capacità informatica nonché nella difesa e resilienza delle infrastrutture critiche delle istituzioni dell'Unione europea, al fine di ridurre il grado di vulnerabilità della stessa di fronte ai gravi attacchi informatici ad opera di grandi organizzazioni criminali, agli attacchi sostenuti dagli Stati o da gruppi terroristici;

69. riconosce l'importante contributo alla lotta contro la criminalità informatica apportato dal Centro europeo per la lotta alla criminalità informatica (EC3) di Europol ed Eurojust, nonché dall'ENISA;

70. invita Europol a sostenere le autorità di contrasto nazionali nella creazione di canali di trasmissione sicuri e adeguati;

71. deplora l'attuale assenza di norme dell'UE in materia di formazione e certificazione; riconosce che le tendenze future della criminalità informatica richiedono un livello crescente di competenze dei professionisti; si compiace del fatto che le iniziative esistenti quali il Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG), il progetto relativo alla formazione dei formatori (TOT) e le attività di formazione nel quadro del ciclo programmatico dell'UE già consentano di colmare il divario in termini di competenze a livello dell'UE;

72. invita la CEPOL e la rete europea di formazione giudiziaria a estendere la loro offerta di corsi di formazione dedicati alle tematiche connesse alla criminalità informatica ai competenti organismi di contrasto e alle autorità giudiziarie in tutta l'Unione;

73. sottolinea che il numero di reati informatici segnalati a Eurojust è aumentato del 30 %; chiede che siano assegnati finanziamenti sufficienti, creando maggiori posti se necessario, per consentire a Eurojust di far fronte al suo crescente carico di lavoro connesso alla criminalità informatica nonché sviluppare e rafforzare ulteriormente il suo sostegno ai procuratori che si occupano di casi transfrontalieri di criminalità informatica, anche tramite la neoistituita rete giudiziaria europea per la criminalità informatica;

74. chiede la revisione del mandato dell'ENISA e il rafforzamento delle agenzie nazionali per la sicurezza informatica; chiede il potenziamento dei compiti, dell'organico e delle risorse dell'ENISA; sottolinea che il nuovo mandato dovrebbe comportare altresì maggiori legami con Europol e le parti interessate del settore, per consentire all'agenzia di sostenere meglio le autorità competenti nella lotta alla criminalità informatica;

75. chiede all'Agenzia dell'Unione europea per i diritti fondamentali (FRA) di elaborare un manuale pratico e dettagliato che offra agli Stati membri orientamenti in merito ai controlli approfonditi e di supervisione;

Migliore cooperazione con i paesi terzi

76. sottolinea l'importanza di una stretta cooperazione con i paesi terzi nella lotta globale contro la criminalità informatica, anche attraverso lo scambio delle migliori prassi, indagini comuni, il rafforzamento delle capacità e l'assistenza giuridica reciproca;

77. invita gli Stati membri che non l'abbiano ancora fatto a ratificare e attuare pienamente la convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001 ("convenzione di Budapest"), nonché i suoi protocolli aggiuntivi e, in collaborazione con la Commissione europea, a promuoverla nelle apposite sedi internazionali;

78. sottolinea la sua profonda preoccupazione circa il lavoro in corso in seno alla commissione per la convenzione sulla criminalità informatica del Consiglio d'Europa, sull'interpretazione dell'articolo 32 della convenzione di Budapest, concernente l'accesso transfrontaliero ai dati informatici memorizzati ("cloud evidence") e si oppone all'eventuale conclusione di un protocollo aggiuntivo o a orientamenti volti ad ampliare la portata di tale disposizione al di là dell'attuale regime stabilito dalla convenzione, che già rappresenta una rilevante eccezione al principio di territorialità, in quanto potrebbe dar luogo al libero accesso a distanza per le autorità di contrasto a server e computer situati in altre giurisdizioni senza il ricorso ad accordi di mutua assistenza giudiziaria o ad altri strumenti di cooperazione giudiziaria istituiti per garantire i diritti fondamentali dell'individuo, tra cui la protezione dei dati e il giusto processo, tra cui la convenzione 108 del Consiglio d'Europa;

79. deplora l'assenza di una normativa internazionale vincolante in materia di criminalità informatica ed esorta gli Stati membri e le istituzioni europee a collaborare all'elaborazione di una convenzione in materia;

80. invita la Commissione a proporre iniziative volte a migliorare l'efficacia e a promuovere il ricorso ai trattati di mutua assistenza giudiziaria (*Mutual Legal Assistance Treaty* – MLAT) al fine di contrastare l'assunzione della competenza extraterritoriale da parte di paesi terzi;

81. invita gli Stati membri a garantire sufficiente capacità di trattamento delle richieste di mutua assistenza giudiziaria relative alle indagini nel ciberspazio e a elaborare programmi di formazione pertinenti per il personale responsabile del trattamento di dette richieste;

82. sottolinea che gli accordi conclusi tra Europol e i paesi terzi in materia di cooperazione strategica e operativa favoriscono sia lo scambio di informazioni che la cooperazione concreta;

83. rileva il fatto che il maggior numero di richieste da parte delle autorità di contrasto è inviato agli Stati Uniti e al Canada; è preoccupato per il fatto che il tasso di comunicazione da parte dei grandi prestatori di servizi statunitensi in risposta alle richieste delle autorità giudiziarie penali europee è inferiore al 60 % e ricorda che il capo V del regolamento generale sulla protezione dei dati, i MLAT e altri accordi internazionali costituiscono il meccanismo privilegiato per consentire l'accesso ai dati personali conservati all'estero;

84. invita la Commissione a presentare misure concrete volte a tutelare i diritti fondamentali della persona sospettata o accusata al momento dello scambio di informazioni tra le autorità di contrasto europee e i paesi terzi, in particolare garanzie in merito al rapido

ottenimento, a seguito di una decisione giudiziaria, di prove pertinenti, informazioni riguardanti l'abbonato o metadati e dati particolareggiati sui contenuti (se non criptati) dalle autorità di contrasto e/o dai fornitori di servizi al fine di migliorare la reciproca assistenza giuridica;

85. invita la Commissione, in collaborazione con gli Stati membri, gli organismi europei associati e, ove necessario, i paesi terzi a considerare nuove modalità per garantire la conservazione e l'ottenimento in modo efficace di prove elettroniche ospitate in paesi terzi, nel pieno rispetto dei diritti fondamentali e della normativa in materia di protezione dei dati dell'UE, accelerando e razionalizzando l'uso delle procedure di mutua assistenza giudiziaria e, se del caso, di riconoscimento reciproco;

86. sottolinea l'importanza del centro di risposta agli incidenti informatici della NATO;

87. invita tutti gli Stati membri a partecipare al forum globale sulle competenze informatiche al fine di agevolare la creazione di partenariati per lo sviluppo di capacità;

88. sostiene l'assistenza allo sviluppo di capacità fornita dall'UE ai paesi del vicinato orientale, dato che molti attacchi informatici provengono da tali paesi;

o

o o

89. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione.