PARLAMENTO EUROPEO 2014 - 2019

Documento di seduta

A8-0178/2015

3.6.2015

RELAZIONE

su "Diritti umani e tecnologia: impatto dei sistemi di sorveglianza e di individuazione delle intrusioni sui diritti umani nei paesi terzi"
(2014/2232(INI))

Commissione per gli affari esteri

Relatore: Marietje Schaake

PR_INI

INDICE

Pagina

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO

su "Diritti umani e tecnologia: impatto dei sistemi di sorveglianza e di individuazione delle intrusioni sui diritti umani nei paesi terzi"
(2014/2232(INI))

Il Parlamento europeo,

– visti la Dichiarazione universale dei diritti dell'uomo e il Patto internazionale relativo ai diritti civili e politici, in particolare l'articolo 19,

– visto il quadro strategico dell'Unione europea sui diritti umani e la democrazia, adottato dal Consiglio il 25 giugno 2012[1],

– visti gli orientamenti dell'UE in materia di diritti umani per la libertà di espressione online e offline, adottati dal Consiglio "Affari esteri" il 12 maggio 2014[2],

– vista la guida del settore delle TIC sull'attuazione dei principi guida su imprese e diritti umani delle Nazioni Unite, pubblicata dalla Commissione nel giugno 2013,

– viste la relazione dell'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) del 15 dicembre 2011 dal titolo "La libertà di espressione su Internet"[3] e la relazione periodica del rappresentante speciale dell'OSCE per la libertà dei mezzi di informazione, del 27 novembre 2014, destinata al Consiglio permanente dell'OSCE[4],

– vista la relazione del relatore speciale delle Nazioni Unite sulla promozione e la tutela dei diritti umani e delle libertà fondamentali nella lotta al terrorismo (A/69/397) del 23 settembre 2014[5],

– vista la relazione dell'Alto Commissariato delle Nazioni Unite per i diritti umani del 30 giugno 2014 dal titolo "The right to privacy in the digital age" (Il diritto alla privacy nell'era digitale)[6],

– vista la relazione del relatore speciale delle Nazioni Unite, del 17 aprile 2013, sul diritto alla libertà di espressione e di opinione (A/HRC/23/40), in cui sono analizzate le implicazioni della sorveglianza delle comunicazioni da parte degli Stati sull'esercizio dei diritti umani alla riservatezza e alla libertà di opinione e di espressione,

– vista la relazione della commissione per gli affari giuridici e i diritti umani dell'Assemblea parlamentare del Consiglio d'Europa del 26 gennaio 2015 sulla

[1] http://eeas.europa.eu/delegations/un_geneva/press_corner/focus/events/2012/20120625_en.htm.
[2] http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.
[3] http://www.osce.org/fom/80723?download=true.
[4] http://www.osce.org/fom/127656?download=true.
[5] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.
[6] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.

sorveglianza di massa[1],

– vista la sua risoluzione del 12 marzo 2014 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni[2],

– vista la relazione del rappresentante speciale del Segretario generale delle Nazioni Unite per i diritti umani e le imprese transnazionali e altri tipi di impresa, del 21 marzo 2011, dal titolo:"Guiding Principles on Business and Human Rights: Implementing the United Nations «Protect, Respect and Remedy» Framework" (Principi guida su imprese e diritti umani: attuare il quadro delle Nazioni Unite «Proteggere, rispettare e rimediare»)[3],

– viste le linee guida dell'OCSE destinate alle imprese multinazionali[4] e la relazione annuale 2014 sulle linee guida dell'OCSE destinate alle imprese multinazionali[5],

– vista la relazione annuale 2013 dell'Internet Corporation for Assigned Names and Numbers (ICANN)[6],

– vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, del 12 febbraio 2014, dal titolo "Governance e politica di Internet: Il ruolo dell'Europa nel forgiare il futuro della governance di Internet"[7],

– vista la dichiarazione del vertice multipartecipativo NetMundial, approvata il 24 aprile 2014[8],

– vista la sintesi del Presidente relativa al nono forum sulla governance di Internet, tenutosi a Istanbul dal 2 al 5 settembre 2014,

– viste le misure restrittive dell'Unione europea in atto, alcune delle quali includono l'embargo sulle attrezzature di telecomunicazione, sulle tecnologie dell'informazione e della comunicazione (TIC) e sugli strumenti di monitoraggio,

– visto il regolamento (UE) n. 599/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, che modifica il regolamento (CE) n. 428/2009 del Consiglio che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento,

---

[1] http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2.
[2] Testi approvati, P7_TA(2014)0230.
[3] http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf?v=1392752313000/_/jcr:system/jcr:versionstorage/12/52/13/125213a0-e4bc-4a15-bb96-9930bb8fb6a1/1.3/jcr:frozennode
[4] http://www.oecd.org/daf/inv/mne/48004323.pdf
[5] http://www.oecd-ilibrary.org/docserver/download/2014091e.pdf?expires=1423160236&id=id&accname=ocid194994&checksum=D1FC664FBCEA28FC856AE63932715B3C
[6] https://www.icann.org/en/system/files/files/annual-report-2013-en.pdf
[7] COM(2014)0072.
[8] http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

dell'intermediazione e del transito di prodotti a duplice uso[1],

– vista la dichiarazione comune del Parlamento europeo, del Consiglio e della Commissione del 16 aprile 2014 sul riesame del sistema di controllo delle esportazioni di prodotti a duplice uso[2],

– viste le decisioni adottate in occasione della 19ª riunione plenaria dell'Intesa di Wassenaar per il controllo delle esportazioni di armi convenzionali e di beni e tecnologie a duplice uso tenutasi a Vienna il 3 e 4 dicembre 2013,

– vista la comunicazione della Commissione al Consiglio e al Parlamento europeo del 24 aprile 2014 dal titolo "Revisione della politica di controllo delle esportazioni: garantire la sicurezza e la competitività in un mondo che cambia"[3],

– viste le conclusioni del Consiglio del 21 novembre 2014 sul riesame della politica sul controllo delle esportazioni,

– vista la sua risoluzione dell'11 dicembre 2012 su una strategia di libertà digitale nella politica estera dell'UE[4],

– vista la sua risoluzione del 13 giugno 2013 sulla libertà della stampa e dei media nel mondo[5],

– viste le sue risoluzioni su casi urgenti di violazione dei diritti umani, della democrazia e dello Stato di diritto, in cui si sollevano preoccupazioni relative alle libertà digitali,

– vista la sua risoluzione del 12 marzo 2015 sulle priorità dell'UE per il Consiglio delle Nazioni Unite per i diritti umani nel 2015[6],

– vista la sua risoluzione dell'11 febbraio 2015 sul rinnovo del mandato del Forum sulla Governance di Internet[7],

– vista la sua risoluzione del 12 marzo 2014 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE[8],

– vista la sua risoluzione sulla relazione annuale sui diritti umani e la democrazia nel mondo nel 2013 e sulla politica dell'Unione europea in materia[9],

– vista la dichiarazione scritta di Edward Snowden destinata alla commissione LIBE del

[1] GU L 173 del 12.6.2014.
[2] GU L 173 del 12.6.2014.
[3] COM(2014)0244.
[4] Testi approvati, P7_TA(2012)0470.
[5] Testi approvati, P7_TA(2013)0274.
[6] Testi approvati, P8_TA(2015)0079.
[7] Testi approvati, P8_TA(2015)0033.
[8] Testi approvati, P7_TA(2014)0230.
[9] Testi approvati, P8_TA(2015)0076.

marzo 2014[1],

– visti la Convenzione europea dei diritti dell'uomo e i negoziati in corso per l'adesione dell'Unione europea alla Convenzione,

– vista la Carta dei diritti fondamentali dell'Unione europea,

– visto l'articolo 52 del suo regolamento,

– vista la relazione della commissione per gli affari esteri (A8-0178/2015),

A. considerando che gli sviluppi tecnologici e l'accesso a un Internet aperto svolgono un ruolo sempre più importante nel consentire e garantire l'esercizio e il pieno rispetto dei diritti umani e delle libertà fondamentali, esercitando un effetto positivo grazie all'estensione della portata della libertà di espressione, dell'accesso all'informazione, del diritto alla riservatezza e della libertà di riunione e di associazione in tutto il mondo;

B. considerando che i sistemi tecnologici possono essere usati in modo improprio per compiere violazioni dei diritti umani attraverso la censura, la sorveglianza, l'accesso non autorizzato alle attrezzature, attività di disturbo, intercettazioni nonché il rilevamento e la localizzazione di informazioni e individui;

C. considerando che tali atti sono compiuti da attori pubblici e privati, compresi i governi e le autorità preposte all'applicazione della legge, come pure da organizzazioni criminali e reti terroristiche, per violare i diritti dell'uomo;

D. considerando che il contesto in cui le TIC sono progettate e utilizzate determina in larga misura l'impatto che possono avere in termini di promozione o violazione dei diritti umani; che le tecnologie dell'informazione, in particolare i software, sono raramente a uso unico e sono solitamente beni a duplice uso per quanto riguarda il loro potenziale di violazione dei diritti umani, mentre il software è anche una forma di comunicazione;

E. considerando che le TIC hanno svolto un ruolo essenziale nell'aiutare gli individui a organizzare i movimenti sociali e le proteste in vari paesi, in particolare sotto regimi autoritari;

F. considerando che la valutazione delle implicazioni per i diritti umani derivanti dal contesto di utilizzo delle tecnologie è determinata dalla forza dei quadri giuridici nazionali e regionali nel disciplinare l'utilizzo di tali tecnologie e dalla capacità delle istituzioni politiche e giudiziarie di controllare detto utilizzo;

G. considerando che nel mondo digitale i soggetti privati svolgono un ruolo sempre più significativo in tutte le sfere delle attività sociali, ma non sono ancora in vigore garanzie per impedire loro di imporre eccessive restrizioni ai diritti e alle libertà fondamentali; che, di conseguenza, i soggetti privati svolgono un ruolo più attivo nella valutazione della legittimità del contenuto e nello sviluppo di sistemi di sicurezza informatica e di

[1] http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

sorveglianza, e ciò può avere un impatto negativo sui diritti umani in tutto il mondo;

H. considerando che Internet rappresenta una rivoluzione in termini di possibilità offerte per lo scambio di dati, informazioni e conoscenze di qualsiasi tipo;

I. considerando che la crittografia rappresenta un mezzo importante che contribuisce alla sicurezza delle comunicazioni e dei soggetti che ne fanno uso;

J. considerando che la governance di Internet ha beneficiato di un modello decisionale multilaterale, ovvero di un processo in grado di garantire la partecipazione significativa, inclusiva e responsabile di tutte le parti, tra cui i governi, la società civile, le comunità tecniche e accademiche, il settore privato e gli utenti;

K. considerando che le agenzie di intelligence hanno sistematicamente messo a rischio i protocolli e i prodotti crittografici per poter intercettare comunicazioni e dati; che l'Agenzia per la sicurezza nazionale degli Stati Uniti ha raccolto un numero elevato di cosiddetti "exploit zero-day", ossia quelle vulnerabilità in materia di sicurezza informatica non ancora note al pubblico o al fornitore del prodotto; che tali attività mettono a rischio gli sforzi globali finalizzati al miglioramento della sicurezza informatica;

L. considerando che i servizi di intelligence con sede nell'UE hanno svolto attività che ledono i diritti umani;

M. considerando che, alla luce dei rapidi sviluppi tecnologici in corso, le garanzie e il controllo giudiziario e democratico sono ampiamente sottosviluppati;

N. considerando che la sicurezza informatica e le misure antiterrorismo che prevedono l'uso di TIC, nonché il monitoraggio di Internet possono avere un grave effetto negativo sui diritti umani e sulle libertà fondamentali delle persone in tutto il mondo, compresi i cittadini dell'Unione che risiedono o viaggiano all'estero, soprattutto in mancanza di una base giuridica fondata sui principi di necessità, proporzionalità e controllo democratico e giudiziario;

O. considerando che i filtri per Internet e la sorveglianza delle comunicazioni compromettono la capacità dei difensori dei diritti umani di trarre vantaggio da Internet e di comunicare informazioni sensibili e violano vari articoli della dichiarazione universale dei diritti dell'uomo (UDHR) che garantisce il diritto di ogni individuo alla riservatezza e alla libertà di espressione;

P. considerando che la sicurezza digitale e la libertà digitale sono entrambe fondamentali e l'una non può sostituire l'altra ma dovrebbero rafforzarsi a vicenda;

Q. considerando che, per quanto riguarda le libertà digitali, l'Unione europea può dare il buon esempio soltanto se tali libertà sono tutelate all'interno dell'UE stessa e pertanto è essenziale adottare il pacchetto dell'UE sulla protezione dei dati;

R. considerando che sono in gioco importanti interessi sociali, come la protezione dei diritti fondamentali, che non dovrebbero essere determinati esclusivamente dal mercato

ma richiedono una regolamentazione;

S. considerando che il rispetto dei diritti fondamentali e dello Stato di diritto e l'efficace controllo parlamentare dei servizi di intelligence che utilizzano la tecnologia di sorveglianza digitale sono elementi importanti della cooperazione internazionale;

T. considerando che le aziende con sede nell'UE rappresentano una parte importante del mercato globale nel settore delle TIC, soprattutto in riferimento all'esportazione delle tecnologie di sorveglianza, localizzazione, individuazione delle intrusioni e controllo;

U. considerando che l'introduzione dei controlli delle esportazioni non dovrebbe danneggiare la legittima ricerca in merito alle questioni relative alla sicurezza informatica né lo sviluppo degli strumenti di sicurezza informatica laddove non vi siano intenti criminali;

1. riconosce che i diritti umani e le libertà fondamentali sono universali e vanno difesi a livello globale in ogni aspetto della loro espressione; sottolinea che la sorveglianza delle comunicazioni, in quanto tale, interferisce con i diritti alla riservatezza e all'espressione, se esercitata al di fuori di un adeguato quadro giuridico;

2. invita la Commissione a garantire la coerenza tra le azioni esterne dell'UE e le sue politiche interne correlate alle TIC;

3. ritiene che la complicità attiva di alcuni Stati membri dell'UE nell'ambito della sorveglianza di massa dei cittadini e dello spionaggio di leader politici da parte dell'Agenzia per la sicurezza nazionale degli Stati Uniti, come rivelato da Edward Snowden, abbia causato gravi danni alla credibilità della politica dell'UE in materia di diritti umani e abbia minato la fiducia globale nei benefici derivanti dalle TIC;

4. rammenta agli Stati membri e alle agenzie dell'UE interessate, tra cui Europol ed Eurojust, i loro obblighi derivanti dalla Carta dei diritti fondamentali dell'Unione europea nonché dal rispetto del diritto internazionale dei diritti umani e degli obiettivi della politica esterna dell'UE, che vietano la condivisione di informazioni di intelligence che potrebbero portare a violazioni dei diritti umani in un paese terzo nonché l'utilizzo di informazioni ottenute violando i diritti umani, come la sorveglianza illegale, al di fuori dell'UE;

5. sottolinea che l'impatto delle tecnologie sul miglioramento dei diritti umani dovrebbe essere integrato in tutti i programmi e le politiche dell'UE, ove possibile, al fine di favorire la tutela dei diritti umani e la promozione della democrazia, dello Stato di diritto e della buona governance nonché la risoluzione pacifica delle controversie;

6. invita a uno sviluppo attivo e alla divulgazione di tecnologie che contribuiscono a tutelare i diritti umani e a favorire i diritti e le libertà digitali delle persone nonché la relativa sicurezza, e che promuovono le migliori prassi e adeguati quadri legislativi garantendo al contempo la sicurezza e l'integrità dei dati personali; esorta, in particolare, l'UE e i suoi Stati membri a promuovere l'utilizzo globale e lo sviluppo di norme aperte, come pure di software e tecnologie crittografiche gratuiti e open-source;

7. invita l'UE ad aumentare il proprio sostegno agli operatori che si adoperano per il rafforzamento delle norme in materia di sicurezza e tutela della riservatezza nel settore delle TIC a tutti i livelli, anche per quanto riguarda hardware, software e norme di comunicazione, nonché per lo sviluppo di hardware e software che integrano il principio della tutela della vita privata fin dalla fase di progettazione (privacy-by-design);

8. chiede di istituire un fondo per i diritti umani e la tecnologia nell'ambito dello strumento europeo per la democrazia e i diritti umani;

9. esorta l'UE, e in particolare il Servizio europeo per l'azione esterna (SEAE), a utilizzare la crittografia nelle sue comunicazioni con i difensori dei diritti umani, a evitare di mettere a rischio i difensori e a proteggere dalla sorveglianza le proprie comunicazioni con terzi;

10. invita l'UE ad adottare software gratuiti e open-source e a incoraggiare altri attori a fare altrettanto, giacché tali software garantiscono migliore sicurezza e maggiore rispetto dei diritti umani;

11. richiama l'attenzione sull'importanza dello sviluppo delle TIC nelle zone di conflitto per promuovere attività di consolidamento della pace al fine di fornire una comunicazione protetta tra le parti coinvolte nella risoluzione pacifica dei conflitti;

12. invita all'applicazione di condizioni, valori di riferimento e procedure di segnalazione al fine di garantire che il sostegno finanziario e tecnico dell'UE per lo sviluppo di nuove tecnologie nei paesi terzi non venga utilizzato in violazione dei diritti umani;

13. invita la Commissione e il Consiglio a collaborare attivamente con i governi dei paesi terzi e a utilizzare i meccanismi di sostegno e gli strumenti europei esistenti per sostenere maggiormente, formare e rendere autonomi i difensori dei diritti umani, gli attivisti della società civile e i giornalisti indipendenti che utilizzano le TIC in modo sicuro nell'ambito delle loro attività, come pure a promuovere i diritti fondamentali connessi alla privacy, quali l'accesso privo di restrizioni alle informazioni su Internet, il diritto alla riservatezza e alla protezione dei dati, la libertà di espressione, di riunione, di associazione, di stampa e di pubblicazione online;

14. richiama l'attenzione sulla difficile situazione in cui versano gli informatori e i relativi sostenitori, ivi compresi i giornalisti, a seguito delle loro rivelazioni in merito alle pratiche di sorveglianza abusive nei paesi terzi; ritiene che tali soggetti debbano essere considerati difensori dei diritti umani e che, in quanto tali, meritino la protezione da parte dell'UE secondo quanto disposto dagli orientamenti dell'UE sui difensori dei diritti umani; ribadisce la sua richiesta alla Commissione e agli Stati membri di esaminare approfonditamente la possibilità di concedere agli informatori protezione internazionale dall'azione penale;

15. deplora che le misure di sicurezza, comprese le misure antiterrorismo, siano sempre più spesso utilizzate come pretesto per violare il diritto alla riservatezza e per contrastare le legittime attività dei difensori dei diritti umani, dei giornalisti e degli attivisti politici; ribadisce la propria ferma convinzione che la sicurezza nazionale non possa mai giustificare programmi di sorveglianza di massa, segreti o non mirati; insiste sul fatto

che tali misure devono essere perseguite nel rigoroso rispetto delle norme in materia di Stato di diritto e diritti umani, ivi compreso il diritto alla riservatezza e alla protezione dei dati;

16. invita il SEAE e la Commissione a promuovere il controllo democratico dei servizi di sicurezza e di intelligence nel suo dialogo politico con i paesi terzi nonché nei suoi programmi di cooperazione allo sviluppo; esorta la Commissione a sostenere le organizzazioni della società civile e gli organi legislativi nei paesi terzi che cercano di rafforzare il controllo, la trasparenza e la responsabilità dei servizi di sicurezza nazionale; chiede che siano inclusi impegni specifici a tal fine nel futuro piano di azione dell'UE sui diritti umani e la democratizzazione;

17. sollecita il Consiglio e la Commissione affinché promuovano le libertà digitali e l'accesso privo di restrizioni a Internet in tutte le forme di contatto con i paesi terzi, inclusi i negoziati di adesione e commerciali, i dialoghi sui diritti umani e le relazioni diplomatiche;

18. riconosce che Internet è divenuto un luogo pubblico e un mercato, per il quale la libera circolazione di informazioni e l'accesso alle TIC sono indispensabili; sottolinea pertanto la necessità di promuovere e tutelare contemporaneamente la libertà digitale e il libero scambio;

19. invita all'inclusione, in tutti gli accordi con paesi terzi, di clausole che fanno riferimento in modo esplicito al bisogno di promuovere, garantire e rispettare le libertà digitali, la neutralità della rete, l'accesso privo di censure e restrizioni a Internet, i diritti alla riservatezza e la protezione dei dati;

20. esorta l'UE a contrastare la criminalizzazione dell'utilizzo, da parte dei difensori dei diritti umani, di strumenti di crittografia, elusione della censura delle informazioni e riservatezza, rifiutando di limitare l'utilizzo della crittografia all'interno dell'UE, nonché ad opporsi ai governi dei paesi terzi che lanciano simili accuse nei confronti dei difensori dei diritti umani;

21. esorta l'UE a contrastare la criminalizzazione dell'utilizzo degli strumenti di crittografia, anticensura e riservatezza, rifiutando di limitare l'utilizzo della crittografia all'interno dell'UE e opponendosi ai governi dei paesi terzi che sanzionano penalmente tali strumenti;

22. sottolinea che per garantire un'efficace politica UE in materia di sviluppo e diritti umani sarà necessario integrare le TIC e colmare il divario digitale, fornendo le infrastrutture tecnologiche di base, facilitando l'accesso alle conoscenze e alle informazioni per promuovere le competenze digitali e promuovendo l'utilizzo di norme aperte nei documenti e l'impiego di software gratuiti e open-source, ove possibile, per garantire l'apertura e la trasparenza (soprattutto da parte delle istituzioni pubbliche), compresa la tutela della protezione dei dati nell'ambiente digitale in tutto il mondo, nonché avere una maggiore comprensione dei potenziali rischi e benefici delle TIC;

23. invita la Commissione a sostenere l'abbattimento delle barriere digitali per le persone con disabilità; considera di estrema importanza che le politiche dell'UE in materia di

sviluppo e promozione dei diritti umani nel mondo puntino a mitigare il divario digitale per le persone disabili e a offrire un quadro più ampio di diritti, in particolare per quanto riguarda l'accesso alla conoscenza, la partecipazione digitale e l'inclusione nelle nuove opportunità economiche e sociali fornite da Internet;

24. sottolinea che la raccolta e la diffusione digitali legali di prove relative a violazioni dei diritti umani possono contribuire alla lotta globale contro l'impunità e il terrorismo; ritiene che tale materiale dovrebbe risultare ammissibile, in casi debitamente giustificati ai sensi del diritto (penale) internazionale, quale materiale probatorio nei procedimenti giudiziari, in linea con le garanzie internazionali, regionali e costituzionali; raccomanda di creare meccanismi nel settore del diritto penale internazionale per l'introduzione di procedure mediante le quali tali dati vengono autenticati e raccolti per l'utilizzo quale materiale probatorio nei procedimenti giudiziari;

25. deplora il fatto che alcune tecnologie e servizi dell'informazione e della comunicazione prodotti all'interno dell'UE siano venduti e possano essere utilizzati da privati, imprese e autorità nei paesi terzi con l'intento specifico di violare i diritti umani attraverso la censura, la sorveglianza di massa, attività di disturbo, intercettazioni, controllo, rilevamento e localizzazione dei cittadini e delle loro attività sulle reti telefoniche (mobili) e su Internet; esprime preoccupazione per il fatto che alcune imprese con sede nell'UE possano fornire tecnologie e servizi in grado di consentire tali violazioni dei diritti umani;

26. osserva che le minacce alla sicurezza dell'Unione europea e dei suoi Stati membri e ai paesi terzi spesso provengono da singoli o piccoli gruppi che utilizzano reti di comunicazione digitale per pianificare e condurre attacchi, e che gli strumenti e le tattiche necessari per sconfiggere tali minacce devono essere costantemente rivisti e aggiornati;

27. ritiene che la sorveglianza di massa non giustificata da un maggiore rischio di attacchi e minacce terroristici costituisca una violazione dei principi di necessità e proporzionalità e, di conseguenza, una violazione dei diritti umani;

28. esorta gli Stati membri a promuovere il pieno controllo democratico delle attività dei servizi di intelligence nei paesi terzi, a verificare che tali servizi operino nel pieno rispetto dello Stato di diritto e a far sì che i servizi e gli individui che operano in modo illegale rispondano delle loro azioni;

29. incoraggia gli Stati membri, alla luce del maggior grado di cooperazione e scambio di informazioni tra Stati membri e paesi terzi (anche attraverso l'utilizzo della sorveglianza digitale), a garantire il controllo democratico di tali servizi e delle loro attività grazie a un'opportuna sorveglianza parlamentare interna, esecutiva, giudiziaria e indipendente;

30. sottolinea che i principi della responsabilità sociale delle imprese e i criteri che tengono conto dei diritti umani nella concezione stessa dei sistemi ("human rights by design"), che costituiscono soluzioni e innovazioni tecnologiche a tutela dei diritti umani, dovrebbero essere integrati nel diritto dell'Unione per garantire che i provider di Internet, gli sviluppatori di software, i produttori di hardware, i media e i servizi di social networking, gli operatori di telefonia mobile e altri considerino i diritti umani

degli utenti finali a livello globale;

31. esorta l'UE a garantire maggiore trasparenza nei rapporti tra operatori di telefonia mobile o provider di Internet e governi e a richiederla nelle sue relazioni con i paesi terzi, chiedendo che gli operatori e i provider di Internet pubblichino annualmente relazioni dettagliate sulla trasparenza, ivi comprese relazioni sulle azioni richieste dalle autorità, nonché sui legami finanziari tra autorità pubbliche e operatori/provider di Internet;

32. ricorda agli attori societari la loro responsabilità di rispettare i diritti umani nelle loro operazioni a livello mondiale, indipendentemente dalla localizzazione degli utenti e dal rispetto da parte dello Stato ospitante dei propri obblighi in materia di diritti umani; invita le imprese del settore delle TIC, in particolare quelle con sede nell'UE, ad attuare i principi guida su imprese e diritti umani delle Nazioni Unite, anche definendo politiche di dovuta diligenza e garanzie di gestione dei rischi e fornendo mezzi di ricorso efficaci qualora le loro attività abbiano provocato un impatto negativo sui diritti umani o vi abbiano contribuito;

33. sottolinea la necessità di attuare e monitorare in modo più efficace regolamenti e sanzioni UE correlati alle TIC, incluso il ricorso a meccanismi con validità generale, al fine di garantire che tutte le parti, compresi gli Stati membri, rispettino la normativa e che siano mantenute condizioni di parità;

34. sottolinea che il rispetto dei diritti fondamentali è un elemento essenziale per il successo delle politiche antiterrorismo, ivi compreso l'utilizzo delle tecnologie di sorveglianza digitale;

35. accoglie con favore la decisione adottata nell'ambito dell'Intesa di Wassenaar del dicembre 2013 in merito al controllo delle esportazioni per quanto riguarda gli strumenti di sorveglianza, applicazione della legge e raccolta delle informazioni di intelligence, nonché i sistemi di sorveglianza delle reti; ricorda il carattere ancora molto incompleto del regime UE sul duplice uso, vale a dire il regolamento dell'UE sui prodotti a duplice uso, in relazione al controllo efficace e sistematico delle esportazioni delle tecnologie TIC pericolose verso paesi non democratici;

36. esorta la Commissione, nel quadro dell'imminente riesame e rinnovo della politica in materia di duplice uso, a presentare in tempi brevi una proposta per politiche intelligenti ed efficaci volte a limitare e disciplinare le esportazioni commerciali di servizi relativi all'attuazione e all'utilizzo delle cosiddette tecnologie a duplice uso, affrontando il problema delle esportazioni potenzialmente pericolose di prodotti e servizi legati alle TIC verso paesi terzi, come convenuto nella dichiarazione comune del Parlamento europeo, del Consiglio e della Commissione dell'aprile 2014; invita la Commissione a includere efficaci garanzie per impedire eventuali ripercussioni negative da parte di tali controlli delle esportazioni sulla ricerca, ivi compresa la ricerca scientifica e nel campo della sicurezza informatica;

37. sottolinea che la Commissione dovrebbe riuscire a fornire tempestivamente alle aziende che sono in dubbio se richiedere o meno una licenza di esportazione informazioni accurate e aggiornate in merito alla legittimità o agli effetti potenzialmente nocivi delle

eventuali transazioni;

38. invita la Commissione a presentare proposte per un riesame delle possibili modalità di utilizzo delle norme UE sulle TIC per la prevenzione delle ripercussioni potenzialmente nocive dell'esportazione di tali tecnologie o di altri servizi verso paesi terzi in cui concetti come l'"intercettazione legale" non possono essere considerati equivalenti a quelli dell'Unione europea o in cui, ad esempio, la situazione dei diritti umani è carente o lo Stato di diritto non esiste;

39. ribadisce che le norme dell'Unione, in particolare la Carta dei diritti fondamentali dell'Unione europea, dovrebbero prevalere nella valutazione dei casi in cui le tecnologie a duplice uso vengono utilizzate secondo modalità che potrebbero limitare i diritti umani;

40. chiede lo sviluppo di politiche per la regolamentazione della vendita di exploit zero-day e di vulnerabilità onde impedirne l'utilizzo per attacchi informatici o per l'accesso non autorizzato ai dispositivi dando origine a violazioni dei diritti umani, senza che tali regolamentazioni abbiano un impatto significativo sulla ricerca accademica e comunque in materia di sicurezza in buona fede;

41. deplora la cooperazione attiva di alcune imprese europee, come pure di imprese internazionali, che commerciano tecnologie a duplice uso con potenziali effetti negativi sui diritti umani e che operano nell'UE, con governi che violano i diritti umani;

42. sollecita la Commissione a escludere pubblicamente le imprese che svolgono tali attività dalle procedure di aggiudicazione degli appalti UE, dai finanziamenti alla ricerca e allo sviluppo e da qualunque altra forma di sostegno finanziario;

43. invita la Commissione a prestare particolare attenzione agli aspetti relativi ai diritti umani nelle procedure di aggiudicazione degli appalti pubblici per attrezzature tecnologiche, in particolare nei paesi con pratiche inaffidabili in questo settore;

44. invita la Commissione e il Consiglio a difendere attivamente l'Internet aperto, le procedure decisionali multilaterali, la neutralità della rete, le libertà digitali e le garanzie in materia di protezione dei dati nei paesi terzi tramite i forum sulla governance di Internet;

45. condanna l'indebolimento e la compromissione dei protocolli e dei prodotti di crittografia, in particolare da parte dei servizi di intelligence che cercano di intercettare le comunicazioni crittografate;

46. mette in guardia dalla privatizzazione delle attività di contrasto attraverso le aziende Internet e i provider di Internet;

47. chiede un chiarimento delle norme e degli standard utilizzati dai soggetti privati per sviluppare i propri sistemi;

48. ricorda l'importanza di valutare il contesto in cui vengono utilizzate le tecnologie, al fine di comprendere appieno il loro impatto sui diritti umani;

49. invita esplicitamente a promuovere strumenti che consentono l'utilizzo anonimo e/o pseudonimo di Internet e contesta la visione unilaterale secondo cui tali strumenti avrebbero come unica funzione quella di consentire le attività criminali, e non di dare maggiore potere agli attivisti dei diritti umani all'interno e all'esterno dell'UE;

50. esorta il Consiglio, la Commissione e il SEAE a elaborare politiche intelligenti ed efficaci volte a disciplinare le esportazioni delle tecnologie a duplice uso, affrontando il problema delle esportazioni potenzialmente pericolose di prodotti e servizi legati alle TIC, a livello internazionale e nell'ambito di regimi di controllo delle esportazioni multilaterali e altri organismi internazionali;

51. sottolinea che eventuali modifiche regolamentari volte ad aumentare l'efficacia dei controlli delle esportazioni dei trasferimenti immateriali di tecnologia non devono ostacolare la ricerca legittima o l'accesso alle informazioni e lo scambio delle stesse, e che eventuali misure quale l'utilizzo delle autorizzazioni generali di esportazione dell'UE per la ricerca a duplice uso non dovrebbero avere un "effetto deterrente" sugli individui o sulle PMI;

52. invita gli Stati membri a garantire che le politiche in materia di controllo delle esportazioni vigenti e future non limitino le attività dei legittimi ricercatori nel campo della sicurezza e che i controlli delle esportazioni siano applicati in buona fede e solo a tecnologie chiaramente definite e destinate a essere utilizzate per la sorveglianza di massa, la censura, attività di disturbo, intercettazioni o controllo, oppure per il rilevamento e la localizzazione dei cittadini e delle loro attività sulle reti telefoniche (mobili);

53. ricorda che le tecnologie wireless ad hoc basate su reti a maglie offrono notevoli opportunità per fornire reti di backup in zone in cui Internet non è disponibile o bloccato e possono contribuire alla promozione dei diritti umani;

54. invita la Commissione a nominare un gruppo indipendente di esperti che possa eseguire una valutazione di impatto sui diritti umani delle norme UE vigenti in materia di TIC, con l'obiettivo di formulare raccomandazioni per l'adeguamento in grado di aumentare la protezione dei diritti umani, in particolare quando i sistemi vengono esportati;

55. riconosce che lo sviluppo tecnologico costituisce una sfida per i sistemi giuridici, richiedendone l'adeguamento alle nuove circostanze; sottolinea che è importante che i legislatori prestino maggiore attenzione alle questioni attinenti all'economia digitale;

56. invita la Commissione a coinvolgere la società civile ed esperti indipendenti, ivi compresi i ricercatori nel campo della sicurezza, nell'ambito delle TIC nei paesi terzi, per garantire competenze aggiornate che dovrebbero portare all'elaborazione di politiche adeguate alle esigenze future;

57. sottolinea l'esigenza di evitare conseguenze non intenzionali, quali restrizioni o effetti deterrenti, per ricerca e sviluppo scientifici o di altro genere in buona fede, per lo scambio di informazioni e l'accesso alle stesse, per lo sviluppo di conoscenze in materia di sicurezza o per l'esportazione di tecnologie che favoriscono l'acquisizione delle necessarie competenze digitali e la promozione dei diritti umani;

58. ritiene che la cooperazione tra governi e soggetti privati a livello mondiale in ambito digitale, compreso il forum sulla governance di Internet, richieda un chiaro sistema di controlli e garanzie e non debba portare a un deterioramento del controllo democratico e giudiziario;

59. osserva che l'approccio volontario non è sufficiente e che sono necessarie misure vincolanti che inducano le imprese a tenere conto della situazione dei diritti umani di un paese prima di esportarvi i propri prodotti e a condurre una valutazione degli effetti delle proprie tecnologie sui difensori dei diritti umani e sugli oppositori del governo;

60. è del parere che l'esportazione di prodotti altamente sensibili debba essere oggetto di controlli prima che tali merci lascino l'UE e che occorre prevedere sanzioni in caso di violazioni;

61. chiede che ogni individuo abbia accesso alla crittografia e che siano create le condizioni necessarie per consentirla; ritiene che i controlli spettino all'utente finale, che deve disporre delle capacità necessarie per eseguirli correttamente;

62. sollecita l'introduzione di norme di crittografia "end to end" quale procedura di routine per tutti i servizi di comunicazione, in modo da rendere più difficile l'accesso ai contenuti da parte di governi, servizi di intelligence e organi di sorveglianza;

63. sottolinea la particolare responsabilità dei servizi governativi di intelligence nel creare un clima di fiducia e chiede di porre fine alla sorveglianza di massa; ritiene che la sorveglianza dei cittadini europei da parte dei servizi di intelligence nazionali e stranieri debba essere presa in esame e fermata;

64. si oppone alla vendita e alla distribuzione di tecnologie di sorveglianza e strumenti di censura europei a regimi autoritari dove non vige lo Stato di diritto;

65. invita ad ampliare la portata della protezione internazionale degli informatori ed esorta gli Stati membri a presentare leggi che ne assicurino la tutela;

66. chiede la nomina di un inviato delle Nazioni Unite per le libertà digitali e la protezione dei dati e invita ad ampliare il mandato del commissario UE per i diritti umani, affinché tali tecnologie siano considerate anche sotto il profilo dei diritti umani;

67. chiede l'adozione di misure atte a garantire la protezione della sfera privata di attivisti, giornalisti e cittadini in ogni parte del mondo e che sia loro assicurato l'accesso a Internet;

68. ribadisce che l'accesso a Internet dovrebbe essere riconosciuto quale diritto umano e chiede l'adozione di misure atte a colmare il divario digitale;

69. incarica il suo Presidente di trasmettere la presente relazione al Consiglio, alla Commissione, al vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e al SEAE.

ESITO DELLA VOTAZIONE FINALE IN COMMISSIONE

Approvazione	26.5.2015
Esito della votazione finale	+: 33 –: 6 0: 24
Membri titolari presenti al momento della votazione finale	Lars Adaktusson, Petras Auštrevičius, Amjad Bashir, Goffredo Maria Bettini, Mario Borghezio, Elmar Brok, Klaus Buchner, James Carver, Javier Couso Permuy, Mark Demesmaeker, Georgios Epitideios, Eugen Freund, Michael Gahler, Richard Howitt, Sandra Kalniete, Tunne Kelam, Afzal Khan, Janusz Korwin-Mikke, Andrey Kovatchev, Eduard Kukan, Ilhan Kyuchyuk, Ryszard Antoni Legutko, Arne Lietz, Barbara Lochbihler, Sabine Lösing, Ramona Nicole Mănescu, David McAllister, Francisco José Millán Mon, Javier Nart, Pier Antonio Panzeri, Demetris Papadakis, Vincent Peillon, Alojz Peterle, Tonino Picula, Andrej Plenković, Cristian Dan Preda, Jozo Radoš, Sofia Sakorafa, Jacek Saryusz-Wolski, Alyn Smith, Jaromír Štětina, Charles Tannock, Eleni Theocharous, László Tőkés, Ivo Vajgl, Boris Zala
Supplenti presenti al momento della votazione finale	Bodil Ceballos, Ignazio Corrao, Tanja Fajon, Andrzej Grzyb, Marek Jurek, Jo Leinen, Javi López, Antonio López-Istúriz White, Fernando Maura Barandiarán, Norbert Neuser, Urmas Paet, Godelieve Quisthoudt-Rowohl, Marietje Schaake, György Schöpflin
Supplenti (art. 200, par. 2) presenti al momento della votazione finale	Damian Drăghici, Maria Grapini, Josef Weidenholzer