



TESTI APPROVATI

Edizione provvisoria

P8_TA-PROV(2015)0388

Seguito dato alla risoluzione del Parlamento europeo del 12 marzo 2014 sulla sorveglianza elettronica di massa dei cittadini dell'UE

Risoluzione del Parlamento europeo del 29 ottobre 2015 sul seguito dato alla risoluzione del Parlamento europeo del 12 marzo 2014 sulla sorveglianza elettronica di massa dei cittadini dell'Unione (2015/2635(RSP))

Il Parlamento europeo,

- visti il quadro giuridico stabilito dal trattato sull'Unione europea (TUE), in particolare gli articoli 2, 3, 4, 5, 6, 7, 10 e 21, la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 e 52, la Convenzione europea dei diritti dell'uomo, in particolare gli articoli 6, 8, 9, 10 e 13, nonché la giurisprudenza degli organi giurisdizionali europei in materia di sicurezza, rispetto della vita privata e libertà di espressione,
- 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 interni¹ (in appresso "la risoluzione"),
- visto il documento di lavoro, del 19 gennaio 2015, dal titolo "Seguito dato all'inchiesta della commissione LIBE sulla sorveglianza elettronica di massa dei cittadini dell'Unione"²,
- vista la risoluzione dell'Assemblea parlamentare del Consiglio d'Europa del 21 aprile 2015 sulla sorveglianza di massa,
- viste le interrogazioni al Consiglio e alla Commissione sul seguito dato alla risoluzione del Parlamento europeo del 12 marzo 2014 sulla sorveglianza elettronica di massa dei cittadini dell'Unione (O-000114/2015 – B8-0769/2015 e O-000115/2015 – B8-0770/2015),
- vista la proposta di risoluzione della commissione per le libertà civili, la giustizia e gli

¹ Testi approvati, P7_TA(2014)0230.

² PE546.737v01-00.

affari interni,

- visti l'articolo 128, paragrafo 5, e l'articolo 123, paragrafo 2, del suo regolamento,
- A. considerando che, nella risoluzione, il Parlamento europeo ha invitato le autorità degli Stati Uniti e gli Stati membri dell'Unione a vietare le attività di sorveglianza di massa indiscriminata e il trattamento massiccio dei dati personali dei cittadini, oltre ad aver denunciato le azioni dei servizi di intelligence segnalate che hanno avuto gravi ripercussioni sulla fiducia e sui diritti fondamentali dei cittadini dell'Unione; che la risoluzione indica la possibile esistenza di altre motivazioni, come ad esempio lo spionaggio politico ed economico, in considerazione della capacità dei programmi di sorveglianza di massa segnalati;
- B. considerando che la risoluzione ha varato un "Habeas Corpus digitale europeo – Protezione dei diritti fondamentali nell'era digitale" corredato di otto azioni specifiche e ha incaricato la commissione per le libertà civili, la giustizia e gli affari interni di riferire al Parlamento nell'arco di un anno al fine di valutare in che misura siano state seguite le raccomandazioni formulate;
- C. considerando che il documento di lavoro del 19 gennaio 2015 illustra gli sviluppi registrati successivamente all'approvazione della risoluzione, contiene una serie di rivelazioni che lasciano intendere il proseguimento delle presunte attività di sorveglianza elettronica di massa e presenta inoltre lo stato di attuazione della proposta di "Habeas Corpus digitale europeo", mettendo in evidenza la risposta limitata da parte delle istituzioni, degli Stati membri e dei soggetti interessati chiamati a intervenire;
- D. considerando che, nella risoluzione, il Parlamento europeo ha invitato la Commissione e altre istituzioni, organi, uffici e agenzie dell'UE a dar seguito alle raccomandazioni in conformità dell'articolo 265 TFUE ("carezza");
- E. considerando che di recente Wikileaks ha rivelato che le comunicazioni degli ultimi tre presidenti francesi, dei ministri del governo francese e dell'ambasciatore di Francia negli Stati Uniti sono state sottoposte a sorveglianza mirata; che un simile spionaggio strategico e industriale ad opera dell'NSA è stato un fenomeno su vasta scala che si è protratto negli ultimi dieci anni e ha interessato tutte le strutture statali e le più grandi aziende francesi;
- F. considerando che, stando alla relazione a cura del relatore speciale sulla promozione e la protezione del diritto alla libertà di opinione e di espressione, la crittografia e l'anonimato garantiscono la riservatezza e la sicurezza necessarie per l'esercizio del diritto alla libertà di opinione e di espressione nell'era digitale; che la relazione afferma inoltre che eventuali restrizioni alla crittografia o all'anonimato devono essere strettamente limitate in virtù dei principi di legalità, necessità, proporzionalità e legittimità degli obiettivi;
- 1. valuta positivamente le inchieste del Bundestag tedesco, del Consiglio d'Europa, delle Nazioni Unite e del Senato brasiliano, i dibattiti in seno a molti altri parlamenti nazionali nonché l'operato di numerosi attori della società civile, in quanto hanno contribuito ad accrescere il livello di consapevolezza generale circa la sorveglianza elettronica di massa;
- 2. invita gli Stati membri dell'UE a ritirare ogni imputazione penale nei confronti di

Edward Snowden, a offrirgli protezione e, di conseguenza, a evitare la sua estradizione o consegna da parte di terzi, riconoscendo il suo statuto di informatore e di difensore internazionale dei diritti umani;

3. esprime tuttavia profondo rammarico per la generale mancanza di un senso di urgenza e di volontà da parte della maggioranza degli Stati membri e delle istituzioni dell'UE nell'affrontare seriamente le questioni sollevate nella risoluzione e nel dar seguito alle raccomandazioni concrete ivi contenute; si rammarica altresì profondamente per l'assenza di trasparenza e di dialogo con il Parlamento europeo;
4. esprime preoccupazione per le recenti leggi approvate in alcuni Stati membri che ampliano i poteri di sorveglianza degli organismi di intelligence, tra cui figurano, in Francia, la nuova legge sull'intelligence approvata dall'Assemblea nazionale il 24 giugno 2015, la quale contiene diverse disposizioni che, secondo la Commissione, sollevano importanti questioni giuridiche, nel Regno Unito, l'adozione della legge sulla conservazione dei dati e i poteri investigativi (*Data Retention and Investigatory Powers Act*) del 2014 e la successiva decisione giudiziale secondo cui taluni articoli della legge sono illegittimi e vanno disapplicati, e, nei Paesi Bassi, le proposte a favore di una nuova normativa intesa ad aggiornare la legge sull'intelligence e la sicurezza del 2002; ribadisce il suo invito a tutti gli Stati membri affinché assicurino che i loro attuali o futuri quadri normativi e meccanismi di controllo che disciplinano le attività delle agenzie di intelligence siano in linea con le norme della Convenzione europea sui diritti dell'uomo e con la pertinente legislazione dell'Unione;
5. valuta positivamente l'inchiesta del Bundestag tedesco sulla sorveglianza di massa; è estremamente preoccupato per le rivelazioni concernenti la sorveglianza di massa delle telecomunicazioni e del traffico Internet in seno all'Unione da parte dell'agenzia tedesca di intelligence esterna BND in cooperazione con l'NSA; ritiene che si tratti di una violazione del principio di leale cooperazione sancito all'articolo 4, paragrafo 3, TUE;
6. chiede al suo Presidente di invitare il Segretario generale del Consiglio d'Europa ad avviare la procedura dell'articolo 52 della CEDU, in base al quale "ogni Alta Parte Contraente, alla domanda del Segretario generale del Consiglio d'Europa, fornirà le spiegazioni richieste sul modo in cui il proprio diritto interno assicura l'effettiva applicazione di tutte le disposizioni della presente Convenzione";
7. ritiene che la risposta della Commissione alla risoluzione sia stata finora assai insufficiente vista la portata delle rivelazioni; invita la Commissione a dare seguito alle richieste avanzate nella risoluzione entro dicembre 2015 al più tardi; si riserva il diritto di presentare un ricorso per carenza o di iscrivere in riserva determinate risorse di bilancio destinate alla Commissione finché non verrà dato un seguito adeguato a tutte le raccomandazioni;
8. sottolinea l'importanza della sentenza della Corte di giustizia dell'Unione europea dell'8 aprile 2014 che dichiara invalida la direttiva 2006/24/CE sulla conservazione dei dati; ricorda che la Corte ha stabilito che l'ingerenza dello strumento in questione nel diritto fondamentale al rispetto della vita privata deve essere limitata allo stretto necessario; sottolinea che tale sentenza presenta un aspetto nuovo nella misura in cui la Corte di giustizia fa specifico riferimento a una particolare giurisprudenza della Corte europea dei diritti dell'uomo relativa alla questione dei "programmi generali di sorveglianza" e ha ormai effettivamente integrato gli stessi principi, provenienti da tale particolare giurisprudenza della Corte europea dei diritti dell'uomo, nel diritto dell'Unione nello

stesso ambito; sottolinea pertanto che si può prevedere che la Corte di giustizia applicherà in futuro lo stesso ragionamento nella valutazione della validità, rispetto alla Carta, di altri atti legislativi dell'UE e degli Stati membri nell'ambito dei "programmi generali di sorveglianza";

Pacchetto sulla protezione dei dati

9. accoglie con favore l'avvio di negoziati informali a livello interistituzionale sul progetto di regolamento generale sulla protezione dei dati nonché l'adozione, da parte del Consiglio, di un orientamento generale sul progetto di direttiva sulla protezione dei dati; ribadisce la propria intenzione di concludere nel 2015 i negoziati concernenti il pacchetto sulla protezione dei dati;
10. rammenta al Consiglio il suo impegno a rispettare la Carta dei diritti fondamentali dell'Unione europea in sede di presentazione di emendamenti alle proposte della Commissione; ribadisce in particolare che il livello di protezione offerto non dovrebbe essere inferiore a quello già previsto dalla direttiva 95/46/CE;
11. sottolinea che sia il regolamento sulla protezione dei dati sia la direttiva sulla protezione dei dati sono necessari per tutelare i diritti fondamentali delle persone e che, pertanto, i due atti legislativi devono essere trattati come un pacchetto da adottare contemporaneamente, al fine di garantire che tutte le attività di trattamento dei dati nell'UE offrano un elevato livello di protezione in tutte le circostanze; sottolinea che, in sede di adozione del pacchetto, occorre rispettare l'obiettivo di rafforzare i diritti e le tutele degli individui per quanto concerne il trattamento dei loro dati personali;

Accordo quadro UE-USA

12. osserva che, dall'approvazione della risoluzione, i negoziati con gli Stati Uniti relativi all'accordo quadro UE-USA sulla protezione dei dati personali trasferiti e trattati ai fini dell'applicazione della legge (nel prosieguo "accordo quadro") sono giunti a conclusione e che il progetto di accordo è stato siglato;
13. si compiace degli sforzi profusi dall'amministrazione statunitense per ripristinare la fiducia attraverso l'accordo quadro e accoglie con particolare favore il fatto che, il 20 ottobre 2015, la Camera dei rappresentanti abbia approvato la legge sul ricorso in sede giudiziaria (Judicial Redress Act) del 2015, ponendo in evidenza i passi sostanziali e positivi compiuti dagli Stati Uniti per venire incontro alle preoccupazioni dell'UE; ritiene che sia di fondamentale importanza garantire nelle medesime circostanze gli stessi diritti a un ricorso effettivo in sede giudiziaria ai cittadini e/o alle persone fisiche dell'UE i cui dati personali vengono trattati nell'Unione e trasferiti negli Stati Uniti, senza operare alcuna discriminazione tra i cittadini europei e quelli statunitensi; invita il Senato degli Stati Uniti ad approvare atti legislativi a garanzia di quanto sopra; evidenzia che l'approvazione, in seno al Congresso degli Stati Uniti, della legge sul ricorso in sede giudiziaria costituisce un presupposto per la conclusione e la firma dell'accordo quadro;

Approdo sicuro (Safe Harbour)

14. ricorda che la risoluzione chiede la sospensione immediata della decisione "Approdo sicuro", dal momento che non prevede un'adeguata protezione dei dati personali dei cittadini dell'Unione;

15. ricorda che ogni accordo internazionale concluso dall'UE prevale sul suo diritto derivato e sottolinea pertanto la necessità di garantire che l'accordo quadro non limiti i diritti e le garanzie degli interessati che si applicano al trasferimento dei dati in conformità del diritto unionale; sollecita, pertanto, la Commissione, a valutare esattamente nel dettaglio il modo in cui l'accordo quadro potrebbe interagire, e quali effetti potrebbe avere, sul quadro giuridico dell'UE in materia di protezione dei dati, rispettivamente l'attuale decisione quadro del Consiglio, la direttiva sulla protezione dei dati (95/46/CE) e la direttiva e il regolamento futuri sulla protezione dei dati; invita la Commissione a presentare al Parlamento, prima di avviare la procedura di ratifica, una relazione di valutazione giuridica in materia;
16. rammenta che la Commissione ha rivolto 13 raccomandazioni agli Stati Uniti nelle comunicazioni del 27 novembre 2013 sul funzionamento del regime "Approdo sicuro" onde garantire un livello di protezione adeguato;
17. si compiace che la sentenza del 6 ottobre 2015 della Corte di giustizia dell'Unione europea dichiara invalida la decisione della Commissione 2000/520 che attesta che gli Stati Uniti garantiscono un adeguato livello di protezione dei dati personali trasferiti; sottolinea che la sentenza ha confermato la posizione di lunga data del Parlamento riguardante l'assenza di un livello adeguato di protezione in virtù di tale strumento; invita la Commissione ad adottare immediatamente le misure necessarie per far sì che tutti i dati personali trasferiti negli Stati Uniti siano soggetti a un livello efficace di protezione, sostanzialmente equivalente a quello garantito nell'Unione;
18. obietta al fatto che il Parlamento non abbia ricevuto alcuna comunicazione ufficiale dalla Commissione per quanto concerne lo stato di attuazione delle 13 raccomandazioni, nonostante quest'ultima abbia annunciato l'intenzione procedere in tal senso entro l'estate del 2014; sottolinea che, a seguito della decisione della Corte di giustizia dell'Unione europea di dichiarare invalida la decisione 2000/520/CE, è ormai imperativo che la Commissione fornisca un aggiornamento dettagliato in merito allo stato attuale dei negoziati e all'impatto della sentenza sugli ulteriori negoziati annunciati; chiede alla Commissione di pensare senza indugio ad alternative alla decisione "Approdo sicuro", di riflettere sull'impatto della sentenza su tutti gli altri strumenti previsti ai fini del trasferimento di dati personali negli Stati Uniti e di riferire in merito entro la fine del 2015;
19. esorta la Commissione a valutare l'impatto e le conseguenze sotto il profilo giuridico della sentenza della Corte di giustizia del 6 ottobre 2015 in relazione alla causa Schrems (C-362/14) nei confronti di eventuali accordi con paesi terzi che consentono il trasferimento di dati personali, come ad esempio il programma di controllo delle transazioni finanziarie dei terroristi UE-USA (TFTP), gli accordi relativi ai codici di prenotazione PNR (Passenger Name Record), l'accordo quadro UE-USA ed altri strumenti di diritto unionale che prevedono la raccolta e il trattamento di dati personali;

Controllo democratico

20. pur rispettando totalmente la piena competenza di cui dispongono i parlamenti nazionali nel controllo dei servizi di intelligence nazionali, invita tutti i parlamenti nazionali che non hanno ancora proceduto in tal senso a valutare attentamente e predisporre un controllo incisivo delle attività di intelligence e a garantire che i comitati o gli organismi di controllo dispongano di sufficienti risorse, competenze tecniche e strumenti giuridici e godano dell'accesso a tutti i documenti del caso per poter esercitare un controllo

efficace e indipendente sui servizi di intelligence e sullo scambio di informazioni con altri servizi d'intelligence esteri; ribadisce il proprio impegno a cooperare strettamente con i parlamenti nazionali al fine di assicurare che siano posti in essere meccanismi di controllo efficaci, anche attraverso la condivisione delle migliori prassi e delle norme comuni;

21. intende dare seguito alla conferenza del 28 e 29 maggio 2015 sul controllo democratico dei servizi di intelligence nell'Unione europea, nonché proseguire gli sforzi volti a garantire la condivisione delle migliori prassi in materia di controllo dell'intelligence, in stretta collaborazione con i parlamenti nazionali; accoglie con favore le osservazioni conclusive congiunte dei copresidenti di detta conferenza, in cui essi esprimono l'intenzione di convocare una conferenza di follow-up a distanza di due anni;
22. ritiene che gli strumenti esistenti per la cooperazione tra gli organismi di controllo, ad esempio la rete europea degli organi nazionali di controllo dell'intelligence (*European Network of National Intelligence Reviewers – ENNIR*), dovrebbero essere sostenuti e maggiormente utilizzati, eventualmente sfruttando le potenzialità dell'IPEX (*InterParliamentary EU information EXchange*) per lo scambio di informazioni tra i parlamenti nazionali, entro il suo ambito d'azione e secondo le sue capacità tecniche;
23. ribadisce il suo appello per la sospensione del programma di controllo delle transazioni finanziarie dei terroristi (TFTP);
24. sottolinea che, affinché l'UE e i suoi Stati membri garantiscano la certezza del diritto, è necessaria una definizione comune di "sicurezza nazionale"; rileva che l'assenza di una definizione chiara consente arbitrarietà e violazioni dei diritti fondamentali e dello Stato di diritto da parte degli organismi esecutivi e di intelligence nell'UE;
25. esorta la Commissione e gli Stati membri a introdurre clausole di temporaneità e di proroga nella legislazione che consente la raccolta di dati personali o la sorveglianza dei cittadini europei; sottolinea che siffatte disposizioni rappresentano salvaguardie essenziali per garantire, in una società democratica, che siano periodicamente verificate la necessità e la proporzionalità di uno strumento che è invasivo per la privacy;

Ripristino della fiducia

26. evidenzia che una sana relazione tra l'Unione europea e gli Stati Uniti resta di vitale importanza per entrambe le parti; osserva che le rivelazioni sulla sorveglianza hanno compromesso il sostegno pubblico a favore di tale relazione e sottolinea che occorre adottare provvedimenti per garantire il ripristino della fiducia, specialmente alla luce dell'attuale e urgente necessità di cooperare su tutta una serie di questioni geopolitiche di interesse comune; sottolinea in tale contesto che occorre trovare una soluzione negoziata globale tra gli Stati Uniti e l'Unione europea, nel rispetto dei diritti fondamentali;
27. valuta positivamente le recenti decisioni legislative e giudiziarie adottate negli Stati Uniti per limitare la sorveglianza di massa da parte dell'NSA, quali l'adozione al Congresso dello "*USA Freedom Act*", senza modifiche e in seguito a un compromesso bipartisan tra le due camere, nonché la sentenza della Corte d'appello del Secondo circuito sul programma dell'NSA di raccolta delle intercettazioni telefoniche; si rammarica, tuttavia, che tali decisioni riguardino principalmente i cittadini e residenti USA, mentre la situazione per i cittadini dell'UE rimane immutata;

28. ritiene che qualsiasi decisione di ricorrere a tecnologie di sorveglianza dovrebbe essere basata su una valutazione approfondita della necessità e della proporzionalità; apprezza i risultati del progetto di ricerca SURVEILLE, che offre una metodologia per valutare le tecnologie di sorveglianza tenendo conto di considerazioni giuridiche, etiche e tecnologiche;
29. evidenzia che l'Unione dovrebbe contribuire all'elaborazione di norme e principi internazionali, a livello di Nazioni Unite, in linea con il Patto internazionale dell'ONU relativo ai diritti civili e politici, nell'ottica di creare un quadro globale per la protezione dei dati, che preveda, tra l'altro, limiti specifici per la raccolta di dati a fini di sicurezza nazionale;
30. è convinto che solo quando verranno stabilite norme credibili a livello mondiale sarà possibile evitare una "corsa agli armamenti" per la sorveglianza;

Imprese private

31. accoglie con favore le iniziative del settore TIC privato per lo sviluppo di soluzioni di sicurezza crittografica e di servizi Internet che migliorano la privacy; incoraggia il continuo sviluppo di impostazioni di facile utilizzo per le applicazioni che aiutano i clienti a gestire la condivisione delle informazioni scegliendo quali informazioni condividere, con chi e in che modo; osserva che varie società hanno altresì annunciato l'intenzione di applicare la crittografia end-to-end in risposta alle rivelazioni sulla sorveglianza di massa;
32. ricorda che, ai sensi dell'articolo 15, paragrafo 1, della direttiva 2000/31/CE, gli Stati membri non devono imporre ai prestatori, per la fornitura di servizi di trasmissione, memorizzazione e "hosting", un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite; rammenta, in particolare, che la Corte di giustizia dell'Unione europea, nelle sentenze C-360/10 e C-70/10, ha respinto le misure di "sorveglianza attiva" della quasi totalità degli utenti dei servizi interessati (fornitori d'accesso a Internet in un caso, rete sociale nell'altro) e ha precisato che è vietata qualsiasi ingiunzione che imponga al prestatore di servizi di hosting una sorveglianza generale;
33. valuta positivamente la pubblicazione, da parte delle aziende di informatica e telecomunicazione, di relazioni di trasparenza sulle richieste di dati degli utenti da parte dei governi; invita gli Stati membri a pubblicare statistiche sulle loro richieste alle imprese private di fornire informazioni private degli utenti;

Accordo TFTP

34. si rammarica che la Commissione non abbia tenuto conto della chiara richiesta del Parlamento di sospendere l'accordo TFTP dato che non sono state fornite informazioni precise in merito alla possibilità che qualsiasi altro ente governativo statunitense abbia avuto accesso ai dati SWIFT al di fuori dell'accordo TFTP; intende tenere conto di tale circostanza nel valutare l'opportunità di dare l'approvazione a futuri accordi internazionali;

Altri scambi di dati personali con paesi terzi

35. sottolinea la sua posizione secondo cui tutti gli accordi, i meccanismi e le decisioni di

adeguatezza per gli scambi di dati personali con paesi terzi richiedono un rigoroso monitoraggio e azioni immediate di follow-up da parte della Commissione in quanto custode dei trattati;

36. plaude alla dichiarazione UE-USA di Riga, del 3 giugno 2015, sul rafforzamento della cooperazione transatlantica nello spazio di libertà, sicurezza e giustizia, in cui i firmatari si impegnano a migliorare l'attuazione dell'accordo USA-UE di mutua assistenza giudiziaria (MLAT), a concluderne il riesame come previsto dall'accordo stesso e a tenere una serie d'incontri per discutere tali questioni con le autorità nazionali competenti; sottolinea che i trattati di mutua assistenza giudiziaria sono lo strumento grazie al quale le autorità di contrasto degli Stati membri dovrebbero cooperare con le autorità dei paesi terzi; invita a tale riguardo gli Stati membri e il governo degli Stati Uniti ad attenersi agli impegni di cui sopra per una rapida conclusione del riesame del MLAT Stati Uniti-Unione europea;
37. invita la Commissione a riferire al Parlamento entro la fine del 2015 in merito alle lacune, individuate nei diversi strumenti per i trasferimenti internazionali di dati, in relazione all'accesso da parte dei servizi di contrasto e di intelligence di paesi terzi, nonché in merito agli strumenti atti a colmare tali lacune, onde garantire che i dati personali dell'UE trasferiti in paesi terzi continuino ad essere adeguatamente e opportunamente protetti;

Tutela dello Stato di diritto e dei diritti fondamentali dei cittadini dell'Unione / maggiore protezione degli informatori e dei giornalisti

38. ritiene che i diritti fondamentali dei cittadini dell'UE siano tuttora in pericolo e che sia stato fatto troppo poco per garantire la loro totale protezione in caso di sorveglianza elettronica di massa; si rammarica per i limitati progressi registrati sul fronte della protezione degli informatori e dei giornalisti;
39. deplora il fatto che numerosi programmi d'intelligence di massa e su vasta scala sembrino essere dettati anche dagli interessi economici delle aziende che li sviluppano e li gestiscono, come è avvenuto in relazione alla fine del programma mirato dell'NSA "Thinthread" e alla sua sostituzione con il programma di sorveglianza su vasta scala "Trailblazer", appaltato alla SAIC nel 2001;
40. ribadisce la propria grave preoccupazione circa il lavoro svolto in seno alla commissione per la Convenzione sulla criminalità informatica del Consiglio d'Europa, sull'interpretazione dell'articolo 32 della Convenzione europea sulla criminalità informatica del 23 novembre 2001 (Convenzione di Budapest), concernente l'accesso transfrontaliero ai dati informatici memorizzati previo consenso o qualora pubblicamente disponibili; si oppone all'eventuale conclusione di un protocollo aggiuntivo o ad 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 delle autorità di contrasto a server e computer situati in altre giurisdizioni senza il ricorso ad accordi di mutua assistenza giudiziaria (MLA) 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; sottolinea che l'UE ha esercitato la sua competenza in materia di criminalità informatica e che le prerogative sia della Commissione che del Parlamento andrebbero pertanto rispettate;

41. deplora che la Commissione non abbia risposto alla richiesta del Parlamento di condurre un esame sul programma globale europeo per la protezione degli informatori e la invita a presentare una comunicazione sull'argomento, al più tardi entro il 2016;
42. accoglie con favore la risoluzione adottata il 23 giugno 2015 dall'Assemblea parlamentare del Consiglio d'Europa dal titolo "Migliorare la protezione degli informatori", e, in particolare, il punto 9, sull'importanza della segnalazione degli illeciti da parte dei dipendenti per assicurare il rispetto dei limiti legali imposti alla sorveglianza, e il punto 10, che invita l'UE ad adottare norme per la protezione dei dipendenti che segnalano illeciti valide anche per il personale dei servizi di sicurezza o d'intelligence nazionali e per quelli delle imprese private che operano in questo campo, e a concedere l'asilo, nella misura resa possibile dal diritto nazionale, ai dipendenti autori di tali segnalazioni minacciati di misure di ritorsione nei loro paesi d'origine, a condizione che le loro rivelazioni integrino i requisiti richiesti per la protezione in base ai principi enunciati dall'Assemblea;
43. sottolinea che la sorveglianza di massa minaccia gravemente il segreto professionale delle professioni regolamentate, compresi i medici, i giornalisti e gli avvocati; evidenzia segnatamente il diritto dei cittadini dell'UE di essere protetti contro qualsiasi tipo di sorveglianza delle comunicazioni riservate con i loro avvocati, che violerebbe la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 6, 47 e 48, e la direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore; invita la Commissione a presentare una comunicazione sulla protezione delle comunicazioni riservate nelle professioni soggette al segreto professionale, al più tardi entro la fine del 2016;
44. invita la Commissione a elaborare linee guida per gli Stati membri su come conformare gli strumenti di raccolta di dati personali a fini di prevenzione, accertamento, indagine e perseguimento dei reati, compreso quelli di terrorismo, alle sentenze della Corte di giustizia dell'Unione europea dell'8 aprile 2014 sulla conservazione dei dati (cause C-293/12 e C-594/12) e del 6 ottobre 2015 sull'approdo sicuro (causa C 362/14); fa riferimento in particolare ai punti 58 e 59 della sentenza sulla conservazione dei dati e ai punti 93 e 94 della sentenza sull'approdo sicuro, che pongono chiaramente l'esigenza, per la raccolta dei dati, di un approccio mirato piuttosto che di una raccolta indiscriminata;
45. sottolinea il fatto che la giurisprudenza più recente, e in particolare la sentenza della Corte di giustizia dell'Unione europea dell'8 aprile 2014 sulla conservazione dei dati, stabilisce chiaramente come un obbligo di legge la dimostrazione della necessità e della proporzionalità di eventuali misure che prevedono la raccolta e l'utilizzo dei dati personali che potenzialmente interferiscono con il diritto al rispetto della vita privata e familiare e il diritto alla protezione dei dati; si rammarica del fatto che le considerazioni politiche spesso pregiudicano il rispetto di tali principi giuridici nel processo decisionale; invita la Commissione a garantire, nel quadro del suo programma di miglioramento della regolamentazione, che tutta la legislazione dell'UE sia di qualità elevata, conforme a tutte le norme giuridiche e alla giurisprudenza ed in linea con la Carta dei diritti fondamentali dell'UE; raccomanda che la valutazione d'impatto di tutte le misure di contrasto e di sicurezza che prevedono l'uso e la raccolta di dati personali comprenda sempre una verifica della necessità e della proporzionalità;

Strategia europea per una maggiore indipendenza informatica

46. si rammarica per il fatto che la Commissione non abbia intrapreso azioni per dare seguito alle raccomandazioni dettagliate formulate nella risoluzione e volte a potenziare la sicurezza informatica e la privacy online nell'UE;
47. plaude ai provvedimenti sinora adottati per potenziare la sicurezza informatica in seno al Parlamento, quali illustrati nel piano d'azione sulla sicurezza delle TIC al PE elaborato dalla DG ITEC; chiede che tali sforzi siano costanti e che venga dato un seguito tempestivo e completo alle raccomandazioni contenute nella risoluzione; chiede nuove idee e, se necessario, modifiche di natura legislativa nel settore degli appalti al fine di potenziare la sicurezza informatica delle istituzioni dell'UE; chiede la sostituzione sistematica del software proprietario con un software open-source controllabile e verificabile in tutte le istituzioni dell'UE, l'introduzione di criteri di selezione "open-source" obbligatori in tutte le future procedure d'appalto relative alle TIC nonché la messa a disposizione efficiente di strumenti di crittografia;
48. ribadisce fermamente il suo invito a sviluppare, nel quadro di nuove iniziative come il mercato unico digitale, una strategia europea per una maggiore indipendenza informatica e una maggiore privacy online che promuova l'industria informatica dell'UE;
49. intende formulare ulteriori raccomandazioni sull'argomento in seguito alla conferenza in programma per la fine del 2015 sul tema "Protezione della privacy online attraverso il potenziamento della sicurezza e dell'autonomia dell'Unione nel settore informatico", avvalendosi dei risultati del recente studio STOA sulla sorveglianza di massa degli utenti delle tecnologie informatiche;

Governance democratica e neutrale di Internet

50. valuta positivamente l'intento della Commissione di fare dell'UE un attore di riferimento per la governance di Internet nonché la sua visione di un modello multipartecipativo della governance di Internet, quale ribadito al summit multipartecipativo sul futuro della governance di Internet (NETMundial) tenutosi in Brasile nell'aprile 2014; guarda con interesse ai risultati dei lavori in corso in questo ambito sul piano internazionale, anche nel quadro del Forum sulla governance di Internet;
51. mette in guardia contro la spirale rovinosa in cui viene chiaramente trascinato il diritto fondamentale alla privacy e alla protezione dei dati personali quando ogni singola informazione sul comportamento umano è considerata potenzialmente utile per contrastare futuri atti criminali, con l'inevitabile risultato di creare una cultura della sorveglianza di massa in cui ogni cittadino è trattato come un potenziale sospetto, e con la conseguente corrosione della fiducia e della coesione sociale;
52. intende tener conto dei risultati della ricerca approfondita svolta dall'Agenzia per i diritti fondamentali sulla tutela dei diritti fondamentali nel contesto della sorveglianza e in particolare sull'attuale situazione giuridica delle persone per quanto riguarda i mezzi di ricorso a loro disposizione in relazione alle pratiche in parola;

Seguito

53. incarica la commissione per le libertà civili, la giustizia e gli affari interni di continuare a monitorare gli sviluppi in questo settore e il seguito dato alle raccomandazioni contenute nella risoluzione;

o

o o

54. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio, alla Commissione nonché ai governi e ai parlamenti degli Stati membri e al Consiglio d'Europa.