Parlamento europeo
2014-2019

Documento di seduta

B8-0153/2019

6.3.2019

PROPOSTA DI RISOLUZIONE

presentata a seguito di dichiarazioni del Consiglio e della Commissione

a norma dell'articolo 123, paragrafo 2, del regolamento

sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'UE e sulla possibile azione a livello di UE per ridurre tali minacce (2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
a nome del gruppo EFDD

B8-0153/2019

Risoluzione del Parlamento europeo sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'UE e sulla possibile azione a livello di UE per ridurre tali minacce
(2019/2575(RSP))

Il Parlamento europeo,

– viste le comunicazioni della Commissione del 14 settembre 2016 dal titolo "Connettività per un mercato unico digitale competitivo: verso una società dei Gigabit europea" (COM(2016)0587) e "Il 5G per l'Europa: un piano d'azione" (COM(2016)0588),

– vista la proposta modificata della Commissione di regolamento del Parlamento europeo e del Consiglio, del 29 gennaio, relativo all'accesso di beni e servizi di paesi terzi al mercato interno degli appalti pubblici dell'Unione europea e alle procedure a sostegno dei negoziati sull'accesso di beni e servizi dell'Unione europea ai mercati degli appalti pubblici dei paesi terzi (COM(2016)0034),

– 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] (direttiva SRI),

– vista la proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza"), presentata dalla Commissione il 13 settembre 2017 (COM(2017)0477),

– vista la direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche[2],

– vista la proposta di regolamento del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento, presentata dalla Commissione (COM(2018)0630),

– visto il procedimento di risoluzione delle controversie dell'OMC (WT/DS549/6) del 1º giugno 2018 relativo a talune misure imposte dalla Cina in relazione al trasferimento di tecnologia estera in Cina,

– vista la sua posizione approvata in prima lettura il 14 febbraio 2019 sulla proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per il

[1] GU L 194 del 19.7.2016, pag. 1.
[2] GU L 321 del 17.12.2018, pag. 36.

controllo degli investimenti esteri diretti nell'Unione europea[3],

– visti i negoziati in corso tra l'UE e la Cina in merito all'accordo globale in materia di investimenti,

– visto l'articolo 123, paragrafo 2, del suo regolamento,

A. considerando che i recenti progressi nel settore delle TIC, comprese le telecomunicazioni di quinta generazione (5G), hanno aperto nuove strade per la produzione, la distribuzione e la fruizione dei beni e dei servizi, nonché per l'interazione tra i dispositivi e tra i cittadini, le amministrazioni pubbliche e altri attori socioeconomici, e hanno quindi il potenziale per stimolare l'economia europea;

B. considerando che la cibersicurezza nelle TIC, la protezione delle informazioni sensibili, il rispetto dei diritti individuali e la tutela dalle minacce informatiche esterne sono condizioni preliminari per garantire la sovranità tecnologica dei cittadini dell'UE e, in ultima analisi, portare prosperità e sostenere la democrazia nell'UE;

C. considerando che la ricerca e la sperimentazione in materia di 5G stentano a tenere il ritmo della pressione internazionale per la diffusione e la commercializzazione delle 5G, mentre una serie di studi scientifici hanno sollevato preoccupazioni e incertezze circa la loro sicurezza, in particolare per quanto riguarda i rischi di inquinamento elettromagnetico per la salute umana e per l'ambiente;

D. considerando che garantire la cibersicurezza per le reti 5G costituisce una sfida nuova e complessa dato il loro carattere virtualizzato e decentrato e la loro catena di valore frammentata e altamente specializzata, dalla produzione alla distribuzione, all'installazione, alla configurazione, alle operazioni, alla manutenzione e agli aggiornamenti dei software; che l'UE deve colmare il divario in materia di cibersicurezza nelle sue infrastrutture critiche, segnatamente nei settori delle telecomunicazioni, dell'energia, dei trasporti, della sanità, della difesa e della sicurezza;

E. considerando che garantire la sicurezza e la protezione delle reti 5G è un compito che non può essere realizzato da singoli costruttori o gestori dei sistemi, ma richiede un'efficace azione coordinata da parte di tutte le pertinenti autorità nazionali e internazionali;

F. considerando che l'UE ha il potenziale per guidare lo sviluppo di tecnologie di cibersicurezza attraverso il sostegno alle imprese europee in questo settore e la promozione di tutti i cambiamenti nella catena di valore che potrebbero ridurre la dipendenza dell'UE dalla tecnologia estera;

G. considerando che l'UE ha sviluppato una serie di misure per garantire la cibersicurezza, tra cui la direttiva SRI e il regolamento sulla cibersicurezza, che dovrebbero essere attuate rapidamente e monitorate costantemente, al fine di garantire che restino efficaci nel corso di tutti i necessari aggiornamenti e riesami;

H. considerando che una maggiore presenza di fornitori di tecnologie cinesi e di altri paesi

[3] Testi approvati, P8_TA(2019)0121.

terzi è diventata evidente nel mercato 5G dell'UE, in particolare di imprese statali o di imprese prive di trasparenza;

I. considerando che la reciprocità è uno dei modi più efficaci per progredire verso condizioni di parità a livello globale;

J. considerando che le imprese estere devono affrontare l'attuale divario nelle norme dell'UE in materia di protezione dei dati tra il regolamento generale sulla protezione dei dati e i diversi requisiti previsti dalle normative nazionali;

K. considerando che l'UE e la Cina stanno negoziando un accordo globale in materia di investimenti dal 2013; che l'accordo proposto contribuirebbe a risolvere le questioni relative all'accesso al mercato, a stabilire un quadro per la protezione degli investimenti e a fissare norme fondamentali in materia di lavoro e ambiente;

L. considerando che sono emersi elementi di prova, seppure non decisivi, per quanto riguarda lacune in ordine alla sicurezza del materiale proposto da fornitori di paesi terzi, tra cui la Cina, che potrebbero mettere a repentaglio i diritti individuali alla vita privata e la protezione delle informazioni sensibili nell'UE;

1. sottolinea che la diffusione e la commercializzazione delle 5G dovrebbero essere realizzate nel rispetto del principio di precauzione, esortando tutti gli attori socioeconomici a prevedere i potenziali effetti sulla sicurezza e la protezione e ad adottare misure precauzionali proporzionate, compresa la tempestiva divulgazione di fattori che potrebbero mettere a rischio la salute pubblica o l'ambiente;

2. sottolinea che gli impatti sociali ed economici della rete 5G e delle tecnologie che essa consente, dall'Internet delle cose all'intelligenza artificiale, dovrebbero essere attentamente valutati, e che dovrebbero essere adottate misure affinché la transizione verso la società europea dei Gigabit avvenga in modo giusto ed equo per tutti e sulla base della responsabilità etica;

3. invita la Commissione e gli Stati membri a creare un ambiente favorevole all'innovazione per i venditori dell'UE al fine di sviluppare nuovi prodotti, servizi e tecnologie e di sostenere l'imprenditorialità dell'UE nella diffusione e nella commercializzazione di prodotti 5G sicuri, garantendo nel contempo che il suo potenziale sia accessibile a tutte le imprese dell'economia digitale dell'UE, comprese le piccole e medie imprese;

4. ricorda che la sicurezza informatica è una delle principali sfide che l'UE si trova attualmente ad affrontare e che eventuali carenze in questo ambito potrebbero violare la vita privata e i diritti fondamentali dei consumatori e dei produttori dell'UE, compromettere seriamente la fiducia dei cittadini nei prodotti e nei servizi TIC e, in ultima analisi, provocare gravi danni economici; chiede una rete che sia sicura fin dalla progettazione e per impostazione predefinita;

5. invita la Commissione e gli Stati membri a cooperare strettamente nell'attuazione della strategia dell'UE in materia di cibersicurezza e a riunire le misure dell'UE con quelle nazionali al fine di ridurre al minimo il rischio di frodi in merito alla sicurezza e di violazioni dei dati lungo l'intera catena del valore; ritiene che tali misure potrebbero

includere la certificazione dell'UE sulla cibersicurezza, i requisiti di configurazione e le procedure e prassi operative, nonché la promozione dell'igiene informatica e dell'istruzione digitale;

6. ritiene che l'agenzia per la sicurezza informatica dell'UE (l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione – ENISA) svolga un ruolo fondamentale nell'analisi delle possibili minacce derivanti da interventi di fornitori esteri, tra cui la Cina, e nel coordinamento di un approccio comune tra gli Stati membri per affrontare le minacce e gli attacchi in materia di cibersicurezza;

7. invita la Commissione e gli Stati membri ad attuare rapidamente il pacchetto sull'economia circolare e a potenziare la gestione delle materie prime in tutto il loro ciclo di vita, nonché il riciclaggio dei rifiuti, in modo tale da migliorare l'accesso dell'UE alle materie prime critiche, che sono fondamentali per i prodotti ad alta tecnologia e le innovazioni emergenti;

8. ritiene urgente affrontare le possibili minacce alla sicurezza tecnologica poste dall'attuale penetrazione sul mercato dell'UE di venditori stranieri, tra cui la Cina, adottando un approccio comune in materia di sicurezza e protezione dei dati tra gli Stati membri;

9. invita la Commissione e gli Stati membri ad analizzare e a monitorare la sicurezza dei sistemi TIC in cui le tecnologie dei paesi terzi sono fortemente presenti, anche attraverso stress test;

10. sottolinea che i fornitori di paesi terzi non dovrebbero essere discriminati sulla base del loro paese di origine, ma che si dovrebbe tener conto della trasparenza di tali imprese, dei loro standard di cibersicurezza e dell'esistenza di condizioni di reciprocità per le imprese europee nel paese di origine, al fine di garantire condizioni di parità;

11. sottolinea che i fornitori e gli operatori cinesi o di paesi terzi non dovrebbero in alcun caso compromettere i diritti individuali garantiti dal diritto dell'UE, anche ove il diritto nazionale del loro paese preveda requisiti diversi;

12. chiede al Consiglio di valutare positivamente la riapertura delle discussioni sulla nuova proposta rivista della Commissione in relazione alla procedura che limita l'accesso di prodotti esteri al mercato degli appalti dell'UE in assenza di un accesso reciproco;

13. ricorda l'importanza di migliorare ulteriormente i negoziati sulla cooperazione normativa con i paesi terzi in materia di tecnologia digitale e di garantire un maggiore impegno da parte loro in seno agli organismi internazionali di normazione;

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