Parlamentul European
2014-2019

Document de ședință

B8-0153/2019

6.3.2019

PROPUNERE DE REZOLUȚIE

depusă pe baza declarațiilor Consiliului și Comisiei

în conformitate cu articolul 123 alineatul (2) din Regulamentul de procedură

referitoare la amenințările la adresa securității în legătură cu prezența tehnologică în creștere a Chinei în UE și posibilele acțiuni la nivelul UE de reducere a acestora
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
în numele Grupului EFDD

B8-0153/2019

Rezoluția Parlamentului European referitoare la amenințările la adresa securității în legătură cu prezența tehnologică în creștere a Chinei în UE și posibilele acțiuni la nivelul UE de reducere a acestora
(2019/2575(RSP))

Parlamentul European,

– având în vedere comunicările Comisiei din 14 septembrie 2016 intitulate „Conectivitate pentru o piață unică digitală competitivă – către o societate europeană a gigabiților” (COM(2016)0587) și „Un plan de acțiune privind 5G în Europa” (COM(2016)0588),

– având în vedere propunerea modificată a Comisiei din 29 ianuarie 2016 de regulament al Parlamentului European și al Consiliului privind accesul bunurilor și al serviciilor din țări terțe pe piața internă a achizițiilor publice a Uniunii și procedurile de sprijinire a negocierilor referitoare la accesul bunurilor și al serviciilor din Uniune pe piețele achizițiilor publice din țări terțe (COM(2016)0034),

– având în vedere Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune[1] (Directiva NIS),

– având în vedere propunerea de regulament al Parlamentului European și al Consiliului din 13 septembrie 2017 privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”) (COM(2017)0477),

– având în vedere Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice[2],

– având în vedere propunerea Comisiei din 12 septembrie 2018 de regulament al Parlamentului European și al Consiliului de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare (COM(2018)0630),

– având în vedere procedura OMC de soluționare a litigiului (WT/DS549/6) din 1 iunie 2018 privind anumite măsuri impuse de China referitoare la transferul de tehnologie străină în China,

– având în vedere poziția sa adoptată în primă lectură la 14 februarie 2019 referitoare la propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniunea Europeană[3],

[1] JO L 194, 19.7.2016, p. 1.
[2] JO L 321, 17.12.2018, p. 36.
[3] Texte adoptate, P8_TA(2019)0121.

– având în vedere negocierile actuale dintre UE și China referitoare la un acord global privind investițiile,

– având în vedere articolul 123 alineatul (2) din Regulamentul său de procedură,

A. întrucât recentele progrese din domeniul TIC, inclusiv al telecomunicațiilor de a cincea generație (5G), au făcut posibile noi modalități de producție, distribuție și valorificare a bunurilor și serviciilor, precum și interacțiunea între dispozitive și între cetățeni, administrațiile publice și alți actori socioeconomici și, prin urmare, au potențialul de a stimula economia europeană;

B. întrucât securitatea cibernetică în domeniul TIC, protecția informațiilor sensibile, respectarea drepturilor individuale și protejarea împotriva amenințărilor cibernetice externe sunt condiții prealabile pentru asigurarea suveranității tehnologice a cetățenilor UE și, în cele din urmă, pentru a aduce prosperitate și a sprijini democrația în UE;

C. întrucât cercetarea și testarea tehnologiei 5G abia țin pasul cu presiunea exercitată la nivel internațional pentru a implementa și comercializa tehnologia 5G, în timp ce o serie de studii științifice au generat preocupări și incertitudini cu privire atât la securitatea, cât și la siguranța sa, în special în ceea ce privește riscurile de poluare electromagnetică pentru sănătatea umană și mediu;

D. întrucât garantarea securității cibernetice pentru rețelele 5G este o provocare nouă și complexă din cauza caracterului virtual și descentralizat al tehnologiei 5G și a lanțului său valoric fragmentat și foarte specializat, de la producție până la expediere, instalare, configurare, operațiuni, întreținere și actualizări ale software-ului; întrucât UE trebuie să acopere, printre altele, deficitul de securitate cibernetică din infrastructura sa critică din sectoarele telecomunicațiilor, energiei, transporturilor, sănătății, apărării și securității, printre altele;

E. întrucât garantarea unor rețele 5G sigure și securizate este o sarcină care nu poate fi realizată de producătorii sau de operatorii de sistem individuali, ci necesită o acțiune coordonată și eficientă din partea tuturor autorităților naționale și internaționale relevante;

F. întrucât UE are potențialul de a coordona dezvoltarea tehnologiilor din domeniul securității cibernetice prin sprijinirea întreprinderilor europene în acest sector și prin promovarea tuturor schimbărilor din lanțul valoric care ar putea reduce dependența UE de tehnologia străină;

G. întrucât UE a elaborat un set de măsuri pentru a asigura securitatea cibernetică, inclusiv Directiva privind securitatea rețelelor și a informațiilor și Legea privind securitatea cibernetică, care ar trebui să fie puse rapid în aplicare și monitorizate în permanență pentru a se asigura că acestea rămân în vigoare pe parcursul tuturor actualizărilor și revizuirilor necesare;

H. întrucât a devenit evidentă prezența crescută a furnizorilor chinezi și ai altor țări terțe de tehnologie pe piața tehnologiei 5G a UE, în special a întreprinderilor de stat sau a întreprinderilor lipsite de transparență;

I. întrucât reciprocitatea este una dintre cele mai eficiente modalități de a încuraja crearea unor condiții de concurență echitabile la nivel mondial;

J. întrucât întreprinderile străine trebuie să facă față actualei lacune de standarde UE privind protecția datelor dintre Regulamentul general privind protecția datelor și diferitele cerințe prevăzute de legislația națională;

K. întrucât UE și China au negociat, din 2013 până în prezent, un acord cuprinzător privind investițiile; întrucât acordul propus ar contribui la soluționarea problemelor privind accesul pe piață, la crearea unui cadru pentru protecția investițiilor și la stabilirea unor standarde de bază în domeniul muncii și al mediului;

L. întrucât au apărut dovezi, deși neconcludente, în ceea ce privește deficiențele în materie de securitate prezentate de echipamentele propuse de furnizorii din țări terțe, inclusiv China, care ar putea pune în pericol drepturile individuale la viață privată și la protecția informațiilor sensibile în UE;

1. subliniază faptul că implementarea și comercializarea tehnologiei 5G ar trebui să se desfășoare în conformitate cu principiul precauției, toți actorii socioeconomici având sarcina de a anticipa impacturile potențiale asupra siguranței și securității și de a lua măsuri proporționale, inclusiv comunicarea rapidă a factorilor care ar putea pune în pericol sănătatea publică sau mediul;

2. subliniază faptul că impactul social și economic al tehnologiei 5G și al tehnologiilor potențate de aceasta, de la internetul obiectelor la inteligența artificială, ar trebui evaluat în mod minuțios și că ar trebui luate măsuri pentru ca tranziția către o societate europeană a gigabiților să aibă loc într-un mod echitabil și egal pentru toți și având la bază responsabilitatea etică;

3. invită Comisia și statele membre să creeze un mediu favorabil inovării pentru ca furnizorii din UE să dezvolte noi produse, servicii și tehnologii și să sprijine întreprinderile din UE în implementarea și comercializarea unei tehnologii 5G sigure și securizate, garantând în același timp că potențialul său este accesibil tuturor întreprinderilor din economia digitală a UE, inclusiv întreprinderilor mici și mijlocii;

4. reamintește că securitatea cibernetică este una dintre principalele provocări cu care se confruntă în prezent UE și că un eșec în această privință ar putea implica încălcarea vieții private și a drepturilor fundamentale ale consumatorilor și producătorilor din UE, ar putea submina în mod grav încrederea cetățenilor în produsele și serviciile TIC și, în cele din urmă, ar putea cauza prejudicii economice grave; solicită o rețea securizată intrinsec și din momentul conceperii;

5. invită Comisia și statele membre să coopereze îndeaproape la punerea în aplicare a strategiei UE în materie de securitate cibernetică și să combine măsurile UE cu cele naționale pentru a reduce la minimum riscul de crize în materie de securitate și de încălcare a securității datelor de-a lungul întregului lanț valoric; consideră că astfel de măsuri ar putea include certificarea de securitate cibernetică la nivelul UE, cerințele de configurare și procedurile și practicile operaționale, precum și promovarea igienei cibernetice și a educației digitale;

6. consideră că agenția UE pentru securitate cibernetică (Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor - ENISA) trebuie să joace un rol esențial în analizarea posibilelor amenințări generate de vânzătorii străini, inclusiv China, și în coordonarea unei abordări comune între statele membre pentru a combate amenințările și atacurile la adresa securității cibernetice;

7. invită Comisia și statele membre să pună rapid în aplicare pachetul privind economia circulară și să stimuleze gestionarea materiilor prime pe parcursul ciclului de viață al acestora, precum și reciclarea deșeurilor, pentru a îmbunătăți accesul UE la materii prime critice, care sunt fundamentale pentru produsele de înaltă tehnologie și pentru inovațiile emergente;

8. consideră că este urgent să se abordeze posibilele amenințări tehnologice la adresa securității pe care le reprezintă pătrunderea actuală pe piața UE a vânzătorilor străini, inclusiv a Chinei, adoptând o abordare comună în materie de securitate și de protecție a datelor între statele membre;

9. invită Comisia și statele membre să analizeze și să monitorizeze securitatea acelor sisteme TIC în care sunt puternic prezente tehnologiile din țările terțe, inclusiv prin efectuarea unor teste de rezistență;

10. subliniază că furnizorii din țările terțe nu ar trebui să fie discriminați din cauza țării lor de origine, dar că ar trebui să se țină seama de transparența acestor societăți, de standardele lor de securitate cibernetică și de existența unor condiții reciproce pentru întreprinderile europene în țara de origine, pentru a asigura condiții de concurență echitabile;

11. subliniază că furnizorii și operatorii din China sau din alte țări terțe nu ar trebui, în nici un caz, să pună în pericol drepturile individuale garantate de legislația UE, chiar și în cazul în care legislația națională prevede cerințe diferite în țara lor de origine;

12. solicită Consiliului să ia în considerare în mod favorabil redeschiderea discuțiilor referitoare la noua propunere revizuită a Comisiei privind procedura de restricționare a accesului produselor străine pe piața achizițiilor publice a UE în cazul în care nu există un acces reciproc;

13. reamintește importanța îmbunătățirii în continuare a negocierilor privind cooperarea în materie de reglementare a tehnologiilor digitale cu țările terțe și a asigurării unui angajament mai puternic din partea acestora în cadrul organismelor internaționale de standardizare;

14. îi încredințează Președintelui sarcina de a transmite prezenta rezoluție Consiliului și Comisiei.