



PARLAMENTUL EUROPEAN

2009 - 2014

Comisia pentru libertăți civile, justiție și afaceri interne

2013/2063(INI)

19.9.2013

AVIZ

al Comisiei pentru libertăți civile, justiție și afaceri interne

destinat Comisiei pentru industrie, cercetare și energie

referitor la valorificarea potențialului cloud computingului în Europa
2013/2063 (INI)

Raportoare pentru aviz (*): Judith Sargentini

(*): Procedura comisiilor asociate – articolul 50 din Regulamentul de procedură

PA_NonLeg

SUGESTII

Comisia pentru libertăți civile, justiție și afaceri interne recomandă Comisiei pentru industrie, cercetare și energie, competentă în fond, includerea următoarelor sugestii în propunerea de rezoluție ce urmează a fi adoptată:

1. afirmă că, în afară de potențialul și de beneficiile cloud computingului pentru întreprinderi, cetățeni, sectorul public și mediu, în special în ceea ce privește reducerea costurilor, acesta implică riscuri și provocări majore, în special pentru drepturile fundamentale (inclusiv în materie de confidențialitate și protecția datelor) și prin creșterea impactului în cazul unor perturbări, indiferent dacă acestea sunt cauzate de funcționări defectuoase, de practici incorecte, de acțiuni infracționale sau de acțiuni ostile din partea altei țări;
2. consideră că accesul la un internet sigur este un drept fundamental al fiecărui cetățean și că cloud computingul va juca în continuare un rol important în această privință; reiterează, prin urmare, solicitarea sa adresată Comisiei și Consiliului să recunoască, fără echivoc, libertățile digitale ca drepturi fundamentale și ca premise indispensabile pentru exercitarea drepturilor universale ale omului;
3. reiterează că, în general, nivelul de protecție a datelor într-un mediu de „cloud computing” nu trebuie să fie inferior celui impus în orice alt context al prelucrării datelor;
4. subliniază că dreptul Uniunii privind protecția datelor, fiind neutru din punct de vedere tehnologic, se aplică deja în totalitate în cazul serviciilor de cloud computing din UE și trebuie, prin urmare, respectat pe deplin; subliniază că ar trebui luat în considerare avizul Grupului de lucru constituit în temeiul articolului 29 referitor la cloud computing¹, deoarece acesta conține orientări clare pentru aplicarea principiilor dreptului Uniunii privind protecția datelor și a normelor referitoare la serviciile de cloud computing, precum conceptele de responsabil/operator de prelucrare, limitarea domeniului de aplicare și proporționalitatea, integritatea și securitatea datelor, folosirea subcontractanților, alocarea responsabilităților, încălcarea securității datelor și transferurile internaționale; subliniază că este necesar ca prin revizuirea în curs a cadrului juridic al Uniunii privind protecția datelor să se elimine toate lacunele în materie de protecție legate de cloud computing pe baza unor orientări suplimentare elaborate de Autoritatea Europeană pentru Protecția Datelor și de WP29; consideră că nu toate datele sensibile sunt date cu caracter personal și îndeamnă, prin urmare, Comisia să propună orientări pentru protejarea datelor sensibile fără caracter personal într-un context de cloud computing, în special în cazul datelor guvernamentale și al datelor furnizate de organizații precum băncile, societățile de asigurări, fondurile de pensii, școlile și spitalele;
5. amintește că, în cazul în care un furnizor de servicii de cloud utilizează datele pentru un alt scop decât cel agreat în acordul privind serviciile sau le comunică sau le utilizează într-un mod care contravine clauzelor contractuale, acesta ar trebui considerat responsabil

¹ Avizul 5/2012, WP 196, disponibil la http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-1.

de date și ar trebui tras la răspundere pentru încălcările și abuzurile comise;

6. subliniază că acordurile privind serviciile de cloud trebuie să prevadă în mod clar și transparent obligațiile și drepturile părților cu privire la activitățile de prelucrare a datelor de către furnizorii de servicii de cloud; dispozițiile contractuale nu conțin nicio exonerare de la garanțiile, drepturile și măsurile de protecție prevăzute de dreptul Uniunii privind protecția datelor; îndeamnă Comisia să prezinte propuneri pentru a restabili echilibrul între furnizorii de servicii de cloud și clienții lor în ceea ce privește clauzele și condițiile utilizate de serviciile de cloud, inclusiv dispoziții:
 - care asigură protecție împotriva anulării arbitrare a serviciilor și a ștergerii datelor;
 - care garantează o șansă rezonabilă pentru clienți de a-și recupera datele stocate în cazul anulării serviciului și/sau al eliminării datelor;
 - care furnizează orientări clare pentru furnizorii de servicii de cloud cu scopul de a facilita migrarea simplă a clienților lor către alte servicii;
7. subliniază că rolul furnizorului de servicii de cloud în temeiul actualei legislații a Uniunii trebuie stabilit de la caz la caz, deoarece furnizorii pot fi atât responsabili de date, cât și operatori de prelucrare de date; solicită îmbunătățirea clauzelor și a condițiilor pentru toți utilizatorii, prin dezvoltarea unor modele internaționale de bune practici pentru contracte și prin clarificarea locului în care furnizorii de servicii stochează datele și în cadrul cărui domeniu juridic din UE;
8. subliniază că trebuie acordată o atenție deosebită acelor situații în care dezechilibrul în ceea ce privește situația contractuală între client și furnizorul de servicii de cloud conduce la contractarea de către client a unor angajamente care impun servicii standard și la semnarea unui contract în care furnizorul definește scopurile, condițiile și mijloacele de prelucrare¹; subliniază că, în astfel de circumstanțe, furnizorul de servicii de cloud ar trebui considerat „responsabil de date” și ar trebui să poarte și el, împreună cu clientul, răspunderea;
9. subliniază că statele membre trebuie să acorde o atenție deosebită utilizării de servicii de cloud de către autoritățile publice, inclusiv de către autoritățile de punere în aplicare a legii și de instituțiile UE, și să se coordoneze foarte bine unele cu celelalte; amintește că trebuie garantate integritatea și securitatea datelor, iar accesul neautorizat, inclusiv al guvernelor străine și al serviciilor de informații ale acestora, fără un temei juridic în baza dreptului Uniunii sau al unui stat membru, trebuie împiedicat; subliniază că acest lucru este valabil și în cazul activităților de prelucrare specifice ale anumitor servicii neguvernamentale de bază, în special în cazul prelucrării anumitor categorii de date cu caracter personal, cum ar fi băncile, societățile de asigurării, fondurile de pensii, școlile și spitalele; îndeamnă Comisia să elaboreze orientări pe care aceste organizații să le urmeze atunci când utilizează servicii de cloud pentru a prelucra, a transmite sau a stoca datele lor, inclusiv adoptarea unor standarde deschise pentru a se evita dependența de un anumit furnizor și o preferință pentru software-urile cu sursă deschisă în vederea creșterii

¹ În special în cazul clienților și al IMM-urilor care utilizează servicii de cloud.

transparenței și a răspunderii serviciilor utilizate; subliniază, în plus, că toate chestiunile menționate anterior prezintă o importanță deosebită în cazul în care sunt transferate date (în afara Uniunii Europene între diferite jurisdicții); consideră, prin urmare, că autoritățile publice, precum și serviciile neguvernamentale și sectorul privat ar trebui, în măsura posibilului, să se bazeze pe furnizorii de servicii de cloud din UE atunci când prelucrează date și informații sensibile, până când se introduc norme globale satisfăcătoare referitoare la protecția datelor, asigurând securitatea datelor sensibile și a bazelor de date deținute de organismele publice;

10. amintește de preocuparea sa profundă referitoare la dezvăluirea recentă a programelor de supraveghere ale Agenției Naționale de Securitate a SUA, și a unor programe similare ale serviciilor de informații din diferite state membre, recunoscând că, dacă informațiile disponibile până în acest moment se confirmă, aceste programe constituie o încălcare gravă a dreptului fundamental al cetățenilor și rezidenților UE la confidențialitate și la protecția datelor, precum și a dreptului la viața privată și de familie, a confidențialității comunicațiilor, a prezumției de nevinovăție, a libertății de exprimare, a libertății de informare și a libertății de a desfășura o activitate comercială;
11. își exprimă din nou îngrijorările serioase cu privire la divulgarea directă obligatorie a datelor și a informațiilor cu caracter personal din UE, prelucrate în temeiul unor acorduri privind serviciile de cloud, către autorități din țări terțe de către furnizorii de servicii de cloud sub rezerva legislației din țara terță sau prin utilizarea unor servere de stocare localizate în țări terțe și la accesul de la distanță direct la datele și informațiile prelucrate de autoritățile de aplicare a legii și de serviciile de informații din țările terțe;
12. regretă faptul că acest tip de acces este obținut în mod normal prin aplicarea directă de către autoritățile din țările terțe a propriilor norme de drept, fără a se utiliza instrumentele internaționale destinate cooperării judiciare, cum ar fi acordurile de asistență judiciară reciprocă sau alte forme de cooperare judiciară;
13. subliniază că aceste practici ridică probleme legate de încredere cu privire la furnizorii de servicii de cloud și online din afara UE și la țările terțe care nu folosesc instrumentele internaționale destinate cooperării juridice și judiciare;
14. se așteaptă ca Comisia și Consiliul să ia măsurile necesare pentru soluționarea acestei situații și pentru asigurarea respectării drepturilor fundamentale ale cetățenilor UE;
15. subliniază că toate societățile care furnizează servicii în UE trebuie să respecte, fără excepție, dreptul UE și sunt răspunzătoare pentru orice încălcări ale acestuia;
16. subliniază că serviciile de cloud care sunt de competența țărilor terțe ar trebui să ofere utilizatorilor situați în UE un avertisment clar și distinct cu privire la posibilitatea ca datele lor cu caracter personal să facă obiectul supravegherii din partea serviciilor de informații și a autorităților de aplicare a legii din țările terțe pe baza unor ordine sau a unor ordonanțe secrete, urmat, dacă e cazul, de o solicitare a acordului explicit al persoanei vizate pentru prelucrarea datelor cu caracter personal;
17. îndeamnă Comisia ca, în cazul în care negociază acorduri internaționale care implică prelucrarea datelor cu caracter personal, să acorde o atenție deosebită riscurilor și

provocărilor pe care cloud computingul le reprezintă pentru drepturile fundamentale, în special, dar nu numai, pentru dreptul la viață privată și la protecția datelor cu caracter personal, astfel cum se prevede la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene; îndeamnă, de asemenea, Comisia să ia act de normele interne ale partenerilor de negociere care guvernează accesul autorităților de aplicare a legii și al serviciilor de informații la datele cu caracter personal prelucrate prin servicii de cloud computing, în special solicitând ca accesul autorităților de aplicare a legii și al serviciilor de informații să fie acordat numai cu condiția ca acestea să respecte pe deplin legislația și să existe un temei juridic lipsit de ambiguități care să permită accesul, precum și cerința de a specifica condițiile exacte de acordare a accesului, scopul obținerii accesului, măsurile de securitate instituite cu privire la transmiterea datelor și drepturile cetățenilor, precum și normele în materie de supraveghere și un mecanism eficient de soluționare a litigiilor;

18. subliniază îngrijorările sale serioase cu privire la activitățile desfășurate de Comisia pentru Convenția privind criminalitatea informatică din cadrul Consiliului Europei în scopul elaborării unui protocol suplimentar privind interpretarea articolului 32 din Convenția privind criminalitatea informatică din 23 noiembrie 2001 referitor la „accesarea transfrontalieră a datelor stocate pe calculator, cu consimțământ sau în cazul în care acestea sunt accesibile publicului”¹ pentru „a facilita utilizarea și punerea sa în aplicare eficace, în lumina evoluțiilor legale, politice și tehnologice”; invită Comisia și statele membre, având în vedere viitoarea analizare a dispozițiilor de la articolul 32 din Convenția privind criminalitatea informatică de către Comitetul de Miniștri al Consiliului Europei, să asigure compatibilitatea acestora, și a modului în care sunt interpretate de statele membre, cu drepturile fundamentale, care includ protecția datelor și, în special dispozițiile privind fluxurile transfrontaliere de date cu caracter personal, astfel cum sunt prevăzute în Carta drepturilor fundamentale a UE, cu acquis-ul UE privind protecția datelor, cu Convenția europeană a drepturilor omului și cu Convenția Consiliului Europei privind protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (Convenția nr. 108), a căror respectare este obligatorie din punct de vedere juridic pentru statele membre; invită Comisia și statele membre să respingă cu tărie orice măsură care ar periclita exercitarea acestor drepturi; își exprimă îngrijorarea cu privire la faptul că, în cazul în care acest protocol suplimentar va fi adoptat, punerea sa în aplicare ar putea duce la un acces la distanță neîngrădit al autorităților de aplicare a legii la serverele și la sistemele informatice aflate în alte jurisdicții, fără ca acestea să recurgă la acordurile de asistență judiciară reciprocă și la alte instrumente de cooperare judiciară introduse pentru a garanta drepturile fundamentale ale cetățenilor, care se referă inclusiv la protecția datelor și la respectarea procedurilor;
19. subliniază că trebuie acordată o atenție deosebită întreprinderilor mici și mijlocii care se bazează tot mai mult pe tehnologia de cloud computing atunci când prelucrează date cu caracter personal și care ar putea să nu aibă întotdeauna resursele sau cunoștințele de specialitate necesare pentru a aborda în mod adecvat provocările în materie de securitate;

1

[http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T%20CY\(2013\)14transb_elements_protocol_V2.pdf%20h](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T%20CY(2013)14transb_elements_protocol_V2.pdf%20h)
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

20. subliniază că nivelul real de control asupra metodelor de prelucrare trebuie să reflecte în mod corespunzător calificarea responsabilului de date și a operatorului de prelucrare de date, cu scopul de a stabili în mod clar responsabilitățile pentru protecția datelor cu caracter personal în ceea ce privește utilizarea cloud computingului;
21. subliniază importanța competențelor în mediul digital în rândul tuturor cetățenilor și îndeamnă statele membre să elaboreze concepte cu privire la modul de promovare a utilizării în condiții de siguranță a internetului, inclusiv a serviciilor de cloud computing;
22. subliniază că toate principiile prevăzute de dreptul UE privind protecția datelor, precum corectitudinea și legalitatea, limitarea domeniului de aplicare, proporționalitatea, acuratețea, perioadele limitate de păstrare a datelor, trebuie luate în considerare pe deplin de către furnizorii de servicii de cloud computing atunci când prelucrează date cu caracter personal;
23. subliniază importanța sancțiunilor administrative eficace, proporționale și disuasive care pot fi aplicate în cazul în care serviciile de cloud computing nu respectă standardele UE în domeniul protecției datelor;
24. subliniază că, pentru a defini cele mai adecvate standarde ce trebuie puse în aplicare, trebuie analizat ad hoc impactul fiecărui serviciu de cloud computing asupra protecției datelor;
25. subliniază că un furnizor european de servicii de cloud ar trebui să acționeze întotdeauna în conformitate cu dreptul UE privind protecția datelor, chiar dacă acest lucru intră în conflict cu instrucțiunile unui client sau ale unui responsabil de date dintr-o țară terță sau atunci când persoanele vizate sunt (doar) rezidente ale unor țări terțe;
26. subliniază nevoia de a aborda provocările generate de cloud computing la nivel internațional, în special în ceea ce privește supravegherea informațiilor de către guverne și garanțiile necesare;
27. subliniază că cetățenii UE care fac obiectul supravegherii informațiilor de către autoritățile unor țări terțe ar trebui să beneficieze cel puțin de aceleași garanții și măsuri reparatorii ca și cetățenii țării terțe în cauză;
28. regretă abordarea din comunicarea Comisiei, deoarece nu se menționează riscurile și provocările aferente cloud computingului și îndeamnă Comisia să-și continue activitatea referitoare la cloud computing, dezvoltând o comunicare mai holistică cu privire la cloud computing, care să țină seama de interesele tuturor părților interesate și care să conțină, pe lângă o referire standard la protecția drepturilor fundamentale și la respectarea cerințelor în materie de protecție a datelor, cel puțin următoarele:
 - orientări în vederea asigurării respectării depline a obligațiilor stabilite la nivelul UE cu privire la drepturile fundamentale și la protecția datelor;
 - condiții restrictive în care datele de pe cloud pot fi sau nu pot fi accesate, în scopul aplicării legii, în conformitate cu Carta drepturilor fundamentale a UE și cu dreptul UE;

- măsuri de protecție împotriva accesării ilegale de către entități străine și naționale, de exemplu prin modificarea cerințelor în materie de achiziții și prin aplicarea Regulamentului (CE) nr. 2271/96 al Consiliului¹ cu scopul de a contracara legislația străină care poate rezulta în transferuri ilegale masive de date de pe cloud ale cetățenilor și ale rezidenților UE;
- propuneri de garantare a neutralității rețelelor și a serviciilor pentru a împiedica discriminarea din motive comerciale a anumitor servicii de cloud;
- propuneri de garantare a faptului că prin măsurile îndreptate împotriva conținutului ilegal nu va fi afectat accesul la conținutul legal;
- propuneri privind definiția termenului „transfer” de date cu caracter personal și modul în care trebuie actualizate clauzele contractuale standard care sunt adaptate mediului cloud, deoarece cloud computingul implică adesea fluxuri masive de date de la clienții serviciilor de cloud către serverele și centrele de date ale furnizorilor de servicii de cloud, implicând numeroase părți diferite și traversând frontierele dintre statele membre ale UE și țări din afara acesteia;
- măsuri de abordare a dezechilibrului actual de pe piața serviciilor de cloud dintre furnizorii de servicii și majoritatea utilizatorilor serviciilor lor;
- măsuri de promovare a cercetării privind modul în care actualele cadre legislative și acorduri internaționale ale UE sunt adaptate la anumite scenarii privind serviciile de cloud, analizând atât impactul economic, cât și pe cel de mediu ale cloud computingului, având în vedere că, până acum, au fost realizate puține studii cu privire la aceste aspecte.

¹ Regulamentul (CE) nr. 2271/96 al Consiliului din 22 noiembrie 1996 de protecție împotriva efectelor aplicării extraterritoriale a unei legislații adoptate de către o țară terță, precum și a acțiunilor întemeiate pe aceasta sau care rezultă din aceasta (JO L 309, 29.11.1996, p. 1-6; URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML>)

REZULTATUL VOTULUI FINAL ÎN COMISIE

Data adoptării	18.9.2013
Rezultatul votului final	+: 43 -: 3 0: 1
Membri titulari prezenți la votul final	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Emine Bozkurt, Arkadiusz Tomasz Bratkowski, Salvatore Caronna, Philip Claeys, Carlos Coelho, Ioan Enciu, Cornelia Ernst, Tanja Fajon, Hélène Flautre, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Agnes Hankiss, Anna Hedh, Salvatore Iacolino, Sophia in 't Veld, Livia Járóka, Timothy Kirkhope, Juan Fernando López Aguilar, Svetoslav Hristov Malinov, Clemente Mastella, Véronique Mathieu Houillon, Claude Moraes, Georgios Papanikolaou, Carmen Romero López, Judith Sargentini, Birgit Sippel, Csaba Sógor, Renate Sommer, Rui Tavares, Nils Torvalds, Wim van de Camp, Axel Voss, Renate Weber, Josef Weidenholzer, Tatjana Ždanoka, Auke Zijlstra
Membri supleanți prezenți la votul final	Alexander Alvaro, Cornelis de Jong, Mariya Gabriel, Marian-Jean Marinescu, Salvador Sedó i Alabart, Janusz Wojciechowski
Membri supleanți (articolul 187 alineatul (2)) prezenți la votul final	Nuno Teixeira