Avizul Comitetului Economic și Social European privind Comunicarea Comisiei către Parlamentul European și Consiliu – Orientări referitoare la Regulamentul privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană

[COM(2019) 250 final]

(2020/C 14/18)

Raportoare: **Laure BATUT**

Sesizare	Comisia Europeană, 22.7.2019
Temei juridic	Articolul 304 din Tratatul privind funcționarea Uniunii Europene
Secțiunea competentă	Secțiunea pentru transporturi, energie, infrastructură și societatea informațională
Data adoptării în secțiune	11.9.2019
Data adoptării în sesiunea plenară	25.9.2019
Sesiunea plenară nr.	546
Rezultatul votului (voturi pentru/voturi împotrivă/abțineri)	162/2/6

1. Recomandări

1.1. CESE recomandă Comisiei:

— să adopte un mod simplu și clar de a comunica pe tema criteriilor de definire a datelor fără caracter personal și a domeniului de aplicare a regulamentului de stabilire a unui cadru pentru libera circulație a datelor fără caracter personal (RDNP), pentru a disipa incertitudinile și a spori încrederea;

— să informeze părțile interesate cu privire la zonele de suprapunere a textelor europene referitoare la date;

— să se asigure – promovând totodată libera circulație – de faptul că datele cu caracter personal (DP) nu ajung, treptat, să fie considerate drept date fără caracter personal (DNP) și că Regulamentul general privind protecția datelor (RGPD) își păstrează în întregime domeniul de aplicare, chiar dacă, pentru aceasta, trebuie contopite cele două regulamente pe termen mediu, în sensul creșterii protecției datelor, și nu a comercializării lor;

— să încurajeze înființarea și dezvoltarea unor federații paneuropene de servicii de tip *cloud computing*;

— să sprijine, pe termen foarte scurt, cetățenii europeni să utilizeze algoritmi capabili să trateze volumele de DNP din cadrul pieței unice a datelor; să încurajeze statele membre să consolideze educația în domeniul tehnologiei informației (TI) și al inteligenței artificiale (IA) la toate nivelurile (școală, universitate, mediul de afaceri) și pe tot parcursul vieții;

— să îndemne părțile interesate la cultivarea unui spirit de responsabilitate, de etică și de solidaritate și nu să lase ca autoreglementarea și soluționarea „pe cale amiabilă”a litigiilor să dea naștere la interpretări divergente ale textelor;

— să nu neglijeze utilizarea instrumentului de reglementare;

— să promoveze sancțiuni pentru nereguli în materie de autoreglementare;

— să elaboreze o foaie de parcurs pentru a verifica dacă securitatea juridică a întreprinderilor este o realitate în contextul utilizării libere a datelor lor, după cum prevede RDNP;

— să facă un bilanț al situației actuale a celor 27 de state membre și să evalueze activitatea punctelor de contact naționale după douăsprezece luni de funcționare;

— să își asume pe deplin rolul său de informare, de comunicare și de avertizare;

— să invite statele membre să comunice cu părțile interesate pe tema criteriilor lor de „siguranță publică”;

— să invite statele membre să își separe zonele de stocare a datelor netransferabile;

— să reexamineze în timp util politica în domeniul concurenței, pentru a verifica dacă este adaptată la libera circulație a datelor în condițiile actuale.

2. **Introducere**

2.1. CESE ia notă de intenția Comisiei de a orienta întreprinderile implicate în transferul de date fără caracter personal înainte de negocierea codurilor de conduită între părțile interesate, care va avea loc în cursul anului 2020. Faptul că datele pot fi adesea mixte, atât cu caracter personal, cât și fără caracter personal, poate crea incertitudini la nivelul întreprinderilor cu privire la măsurile care trebuie luate pentru a le proteja. Ar trebui să se amintească aici principiile de bază ale normelor existente, înainte de examinarea punctelor cu privire la care CESE dorește să facă observații.

2.2. Comisia a observat că lipsa competitivității serviciilor de cloud computing din UE și, prin urmare, lipsa mobilității datelor în contextul oligopolurilor au un impact negativ asupra pieței datelor. RDNP solicită statelor membre să își reducă la minimum cerințele de localizare a datelor și, totodată, fragmentarea legislațiilor în domeniu, pentru a stimula creșterea și pentru a debloca capacitatea de inovare a întreprinderilor.

2.3. Odată cu adoptarea Regulamentului privind libera circulație a datelor fără caracter personal, care este complementar RGPD, se introduce în textele europene ale secolului XXI o „a cincea libertate de circulație”, care se aplică tuturor datelor (afirmația aparține dnei Anna-Maria Corazza Bildt, deputată în Parlamentul European, raportoare). Un astfel de așa-numit „bun necorporal”, trebuie să poată fi transferat și administrat unde doresc proprietarii săi, acolo unde se află furnizorii de servicii de găzduire a datelor, în alte țări decât cea în care au fost create și/sau utilizate, în Uniunea Europeană (articolul 1 din RDNP). Astfel, deținătorii săi au de câștigat sub aspectul facilității și competitivității.

RDNP

2.4. Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului ([1]) promovează libera circulație a datelor fără caracter personal în Uniune pentru a dezvolta inteligența artificială, *cloud computing*-ul și analiza volumelor mari de date. Acesta prevede (articolul 6) că Comisia încurajează și facilitează elaborarea, de către operatorii care lucrează cu aceste date fără caracter personal, a unor coduri de conduită de autoreglementare la nivelul Uniunii.

2.5. Textul supus examinării, care este destinat profesioniștilor din microîntreprinderi și IMM-uri, trebuie să promoveze înțelegerea de către aceștia a interacțiunilor dintre regulamentul sus-menționat și RGPD, prin intermediul unor orientări. În virtutea unei abordări pedagogice, Comisia utilizează numeroase exemple de situații.

2.6. Codurile de conduită aflate în curs de pregătire ar trebui să fie gata între noiembrie 2019 și mai 2020 [considerentele 30 și 31, articolul 6 alineatul (1)]. La elaborarea lor se va ține seama de opiniile tuturor părților. Au avut loc două consultări publice și s-au constituit două grupuri de lucru, alcătuite din specialiști, care sprijină Comisia: unul privind certificarea securității cibernetice în *cloud* (CSPCERT), iar celălalt, privind portarea datelor și schimbarea furnizorilor de servicii (SWIPO). Contribuțiile lor acoperă infrastructura ca serviciu (*Infrastructure-as-a-Service – IaaS*) și software-ul ca serviciu (*Software-as-a-Service – SaaS*). În mai 2020, Comisia va propune ca acest sector să fie încurajat să elaboreze un model de clauze contractuale, iar, în 2022, va transmite Parlamentului European, Consiliului și CESE un raport cu privire la punerea în aplicare a regulamentului, în special cu privire la utilizarea datelor „compuse”sau mixte.

3. **Observații generale**

3.1. *Misiunea Comisiei: concilierea RGPD cu RDNP*

3.1.1. Pentru a concilia cele două regulamente, care sunt complementare, Comisia explică următoarele: 1. cerințele privind localizarea datelor **sunt interzise de acum înainte**; 2. datele rămân accesibile **autorităților competente**; 3. datele devin mobile și astfel pot face obiectul „portării”. RGPD se referă la „portabilitate”, pe când RDNP vorbește despre „portare”. Utilizatorii își pot transfera datele în afara țării în care au fost create, iar apoi le pot recupera fără a fi supuși la (prea multe) constrângeri, în urma schimbării furnizorului de servicii, pentru stocarea, prelucrarea sau analiza lor. Spre deosebire de „portabilitate”, care este un drept al persoanele vizate, „portarea”este structurată în funcție de codurile de conduită, așadar în contextul unui demers de autoreglementare.

([1]) JO L 303, 28.11.2018, p. 59.

3.1.2. Aceasta este o diferență importantă între cele două regulamente, unul fiind bazat pe instrumente juridice obligatorii (***hard law***), iar celălalt – pe instrumente juridice neobligatorii (***soft law***), despre care se știe că oferă mult mai puține garanții. Or, potrivit Comisiei înseși, majoritatea datelor prezintă caracteristici personale și, deopotrivă, nepersonale, **indisolubil legate**, motiv pentru care se poate vorbi despre date „mixte"(DM).

3.1.3. CESE salută acest demers de susținere și nu pune în discuție exemplele alese, nici nu intenționează să propună alte exemple, însă observă că orientările Comisiei destinate operatorilor se rezumă la ilustrarea contextului prin exemple de situații. Pentru a trage un semnal de alarmă, în atenția Comisiei, CESE dorește să sublinieze zonele critice care, în opinia sa, riscă să ridice probleme pentru utilizatori, în pofida îndrumării și a codurilor viitoare.

3.2. *Trecerea în revistă a principiilor – spre aducere aminte*

3.2.1. Principiul libertății de circulație a datelor

Greu de depășit sunt nu atât barierele geografice din calea liberei circulații a DNP, cât cele de natură funcțională și/sau legate de mijloacele de care dispun întreprinderile pentru utilizarea tehnologiilor informatice.

RDNP interzice cerințele de localizare a DNP pe un anumit teritoriu (articolul 4 și solicită statelor membre abrogarea oricărei dispoziții contrare în termen de 24 de luni de la intrarea în vigoare a regulamentului (mai 2021).

Acesta acceptă excepțiile legate de siguranța publică. Statele trebuie să publice online informații detaliate cu privire la cerințele lor de localizare la nivel național. Comisia Europeană poate să formuleze observații și retransmite informații despre site-urile statelor membre.

3.2.2. Excepții de la libertatea de circulație

— Autoritățile statelor membre pot avea **acces la datele transferate**: RDNP instituie o procedură prin care orice autoritate de control dintr-un stat X poate să obțină date prelucrate într-un stat Y. Este prevăzută și o procedură de cooperare între state (articolele 5 și 7). În absența localizării însă, CESE nutrește serioase temeri ca datele (contabile, financiare, contractuale etc.) să nu scape de sub controlul autorităților statelor membre. El amintește Comisiei că, la nevoie, nu trebuie să piardă din vedere recursul la utilizarea instrumentului de reglementare.

— **Punctul unic de contact** din fiecare stat va răspunde cererii prin intermediul autorității naționale de supraveghere, care poate sau nu să furnizeze datele, în cazul în care consideră cererea drept admisibilă. În spiritul RDNP, punctele de contact ar trebui să ajute părțile interesate să își aleagă în cunoștință de cauză transferurile și prestatorii de servicii, din întreaga Uniune, în condiții de concurență.

CESE consideră că doar cu ajutorul orientărilor nu pot fi disipate numeroasele incertitudini legate de punerea în aplicare a acestui principiu. Motivele invocate de state, buna credință a operatorilor sau buna funcționare a punctelor de contact sunt aspecte greu de apreciat. Orice evaluare în această privință va fi greu de realizat.

— Interzicerea cererii directe sau indirecte de localizare a datelor, cu excepția cazurilor justificate de „siguranța publică". CESE consideră că noțiunea de „siguranță publică"invocată în regulament este lipsită de precizie iar sfera ei de cuprindere este neclară atunci când se aplică la fluxul de date și la comercializarea lor. RDNP definește cerințele de localizare a datelor ca „orice obligație, interdicție, condiție, limită sau altă cerință prevăzută în actele cu putere de lege sau actele administrative ale unui stat membru"sau care rezultă din practicile administrative ([2]) care ar obliga operatorii să păstreze datele în perimetrul unui anumit teritoriu din Uniune. Pentru Curtea de Justiție a Uniunii Europene (CJUE) ([3]) (și considerentul 19 din RDNP), siguranța publică cuprinde „atât securitatea internă, cât și cea externă a unui stat membru"și presupune existența „unei amenințări reale și suficient de grave care afectează unul dintre interesele fundamentale ale societății". Această definiție include datele genetice, datele biometrice și datele privind sănătatea. Răspunsul statului membru trebuie să fie proporțional.

([2]) Articolul 3 alineatul (5) din Regulamentul (UE) 2018/1807.

([3]) A se vedea comunicarea COM(2019) 250, notele de subsol de la p. 13 și Hotărârea C-331/16 și C-366/16 K./Staatssecretaris van Veiligheid en Justitie, și H. F./Belgische Staat: „42. În ceea ce privește **noțiunea de «siguranță publică»**, reiese din jurisprudența Curții că această noțiune **acoperă atât securitatea internă a unui stat membru, cât și securitatea sa externă** (Hotărârea din 23 noiembrie 2010, Tsakouridis, C-145/09, EU:C:2010:708, punctul 43). Securitatea internă poate fi afectată, printre altele, printr-o **amenințare directă pentru liniștea și siguranța fizică** ale populației statului membru vizat (a se vedea în acest sens Hotărârea din 22 mai 2012, I, C-348/09, EU:C:2012:300, punctul 28). În ceea ce privește securitatea externă, aceasta poate fi afectată, printre altele, prin **riscul unei perturbări grave a relațiilor externe ale acestui stat membru** sau a conviețuirii în pace a popoarelor (a se vedea în acest sens Hotărârea din 23 noiembrie 2010, Tsakouridis, C-145/09, EU:C:2010:708, punctul 44)".

3.2.3. Comitetul consideră că, în cazul liberei circulații și al localizării datelor:

— criteriile luate în considerare pot fi interpretate în mai multe feluri;

— numai judecătorul va fi în măsură să le clarifice, de la caz la caz, ceea ce poate fi în detrimentul încrederii necesare desfășurării comerțului, în special în cazul datelor sensibile; diferendele ce decurg din codurile de conduită ar putea duce la o fragmentare și mai accentuată a situațiilor;

— ritmul justiției este cu totul altul decât cel al domeniului digital și al circulației datelor.

CESE consideră că incertitudinile și complexitatea situației reprezintă un factor de descurajare pentru microîntreprinderi și IMM-urilor.

3.2.4. CESE regretă că, în cadrul orientărilor, nu se face nicio referire la litigii, nici la modalitățile de verificare a modului în care statele membre vor întruni criteriile de siguranță publică și nici la modul în care ar putea fi sancționate, dacă este cazul. CESE nutrește temeri legate de faptul că textul explicativ al comunicării nu este suficient pentru ca operatorii din microîntreprinderi și din IMM-uri să se poată poziționa între toate capcanele juridice ale textelor și că aceste incertitudini nu lasă să se instaureze climatul de încredere și de securitate juridică necesar pentru dezvoltarea acestui sector.

3.2.5. CESE recunoaște că comunicarea Comisiei are marele merit de a difuza pe scară largă, de la vârf către bază, informații privind situația creată de cele două regulamente, fiind mai mult decât necesară pentru microîntreprinderi și IMM-uri. CESE dorește ca acțiunile punctelor de contact naționale și utilizarea site-ului web al Comisiei de către aceste părți interesate să fie evaluate încă din a șasea lună de funcționare, astfel încât să se poată aplica rapid măsuri de corectare în cazul în care se resimte o lipsă de informare și de comunicare.

4. **Observații specifice**

4.1. *Datele*

4.1.1. Datele fără caracter personal includ, prin definiție, toate datele digitale care nu se înscriu în sfera de cuprindere a datelor cu caracter personal, astfel cum sunt definite în RGPD. Poate fi vorba despre date comerciale, date privind agricultura de precizie, cerințele de întreținere a mașinilor, condițiile meteorologice etc.

4.1.2. Datele colectate de servicii publice precum spitalele, serviciile de asistență socială sau din domeniul fiscal se pot afla în imediata apropiere a datelor cu caracter personal ale pacienților sau contribuabililor. Întreprinderile care vor să le utilizeze trebuie să se asigure că nu există riscul identificării persoanelor și nici, după anonimizarea datelor, riscul dezanonimizării lor. Pentru microîntreprinderi sau IMM-uri, aceasta poate implica proceduri prea îndelungate și prea costisitoare. Întrucât ambele regulamente (RGPD și RDNP) asigură libera circulație a tuturor datelor în UE, atunci când acestea sunt „**legate între ele în mod indisolubil**”, măsurile juridice de protecție prevăzute în RGPD se aplică setului de date mixte [considerentul 8 și articolul 2 alineatul (2) din Regulamentul (UE) 2018/1807]. La prima restricție, privind fluxul liber al datelor fără caracter personal, legată de siguranța publică, se adaugă așadar o restricție legată de însăși natura datelor. Această chestiune se situează în centrul preocupărilor comunicării Comisiei, care se referă în câteva rânduri la strânsa legătură dintre DP și DNP: „[s]eturile de date mixte reprezintă majoritatea seturilor de date”[comunicare, punctul 2.2]; ele pot fi „legate între ele în mod indisolubil”[punctul 2.2], „niciunul dintre cele două regulamente nu obligă întreprinderile să separe seturile de date”(punctul 2.2).

4.1.3. Întreprinderea trebuie să își pună întrebarea dacă datele fără caracter personal pe care le prelucrează sunt „legate în mod indisolubil”de datele cu caracter personal și să le protejeze, în cazul în care se verifică această afirmație. Pentru întreprindere, pregătirea acestei „gestionări”(*out management*) nu este o sarcină ușoară. Formularea unei definiții generale a datelor mixte pare a fi imposibilă, iar suprapunerea celor două regulamente va conduce, probabil, la alte suprapuneri, cu texte referitoare la legislația în materie de date, precum cele referitoare la proprietatea intelectuală: DNP pot circula, dar dacă sunt reutilizate într-o lucrare, nu vor mai face obiectul acelorași norme. În opinia CESE, corelarea diferitelor texte va fi foarte delicată. Jurisprudența a cerut deja ca legătura „indisolubilă”susmenționată să fie analizată prin prisma unui criteriu „rezonabil”. CESE constată că, în mod evident, comunicarea supusă examinării nu poate trece în revistă toate cazurile posibile, pentru a ajuta părțile interesate, și că, în această situație, sunt favorizate mai curând întreprinderile mari. CESE recomandă Comisiei să se asigure că, în practică, DP nu ajung treptat să fie considerate drept DNP și să facă în așa fel încât RGPD să își păstreze în întregime domeniul de aplicare, chiar dacă, pentru aceasta, trebuie contopite cele două regulamente pe termen mediu, în sensul creșterii protecției datelor, și nu al comercializării lor.

4.2. *Portabilitatea, transferul, prelucrarea și stocarea datelor*

RGPD prevede ca portabilitatea să fie pusă în aplicare printr-un regulament (articolul 20, iar RDNP – prin autoreglementare. CESE regretă că se creează astfel, în mare măsură, insecuritate juridică, ceea ce ar fi în detrimentul microîntreprinderilor și întreprinderilor mici și mijlocii, din cauza multiplelor riscuri de litigii. CESE consideră că, în cazul în care DNP sunt bunuri – necorporale, desigur, dar în liberă circulație –, se pot importa și exporta. În contextul actual, ar fi interesantă o dezbatere asupra proprietății asupra acestor date. Or, mai mult decât datele în sine, volumele mari de date sunt de o reală valoare. Astfel, Comitetul ajunge la concluzia că, probabil, politica în domeniul concurenței nu este adaptată la acest tip de piață. CESE se întreabă cum va determina situația creată consolidarea productivității microîntreprinderilor și a IMM-urilor. În această privință, comunicarea Comisiei nu oferă întreprinderilor de acest tip informații relevante.

4.3. *Furnizorii de servicii*

4.3.1. UE nu are operatori de dimensiuni mari, nici cloud „european", aspect regretabil, semnalat ca atare de către CESE, cu mult timp în urmă. Efectul de scară mereu căutat este apanajul marilor întreprinderi americane din domeniul informaticii și al anumitor întreprinderi chineze. Astfel, chiar și marile administrații mari din statele membre sunt tentate să aibă încredere în ele și să le transfere gestionarea datelor lor (cazul Franței).

4.3.2. CESE consideră că europenii ar avea nevoie să creeze ecosisteme partenere și să prevadă transferuri de date între platforme. Dincolo de această comunicare, Comisia ar putea ajuta microîntreprinderile și IMM-urile să dezvolte resurse în acest sens, după cum a procedat și pentru SGI în cadrul proiectului său din 2018 privind „Federația de servicii paneuropene de *cloud*"pentru prestarea de servicii de interes economic și non-economic general (serviciu la cerere, *FaaS*) și după cum prevede să procedeze cu rețeaua de centre de inovare digitală („A *network of Digital Innovation Hubs*", web/Commission/DIHs/ianuarie 2019).

4.4. *Securitatea datelor* ([4])

4.4.1. Pe plan intern, operatorii naționali ([5]) verifică natura datelor lor care urmează să fie transferate și le asigură securitatea. Cerința de localizare corespundea normelor de securitate care puteau fi verificate în conformitate cu legislația națională. În pofida RGPD și a RDNP, standardele de securitate informatică din diferitele țări ale UE nu sunt unificate. Comitetul consideră că ar trebui furnizate informații solide cu privire la acest aspect atât microîntreprinderilor și IMM-urilor, cât și serviciilor publice și private, prin intermediul punctelor naționale de contact și în diferite limbi.

Pe plan extern, CESE consideră că nu prezintă siguranță capacitatea întreprinderilor din afara UE de a respecta codurile de conduită și de a restitui datele după noile transferuri cerute de proprietarii lor. Comitetul se teme că, în timp, separarea responsabilităților va deveni dificilă.

CESE recomandă Comisiei să ajute părțile interesate europene pentru ca, pe termen foarte scurt, să ajungă să utilizeze algoritmi în măsură să prelucreze volumele mari de date fără caracter personal (DNP) de pe piața unică a datelor.

4.4.2. Chestiunea localizării fizice a serverelor și a securității lor va face obiectul unor negocieri de natură comercială și diplomatică purtate de către state. Această chestiune este esențială. În relația cu întreprinderile mari din domeniul informatic și cu statele de referință ale acestora, deși gestionarea datelor este o competență partajată între statele membre și UE, eventualele negocieri purtate de statele membre pe cont propriu nu ar fi scutite de riscuri.

4.4.3. CESE propune Comisiei să își clarifice comunicarea privind obligațiile furnizorilor de servicii în ceea ce privește stocarea PND, metodele utilizate, locațiile fizice, perioada prevăzută sau autorizată de păstrare a datelor și utilizarea lor după prelucrare, deoarece securitatea datelor depinde de aceste elemente, care pot fi importante pentru întreprinderile europene în contextul concurenței globale.

4.5. *Codurile de conduită*

4.5.1. Începând din mai 2019, părțile interesate de RDNP (în principal utilizatorii și furnizorii de servicii de *cloud computing*) sunt încurajate să își elaboreze propriul cod de conduită în termen de 12 de luni. Potrivit Comisiei, este de dorit să se țină seama de cele mai bune practici, de abordările în ceea ce privește sistemele de certificare și de foile de parcurs în materie de comunicare. Grupurile de lucru SWIPO și CSPCERT contribuie cu expertiza lor.

4.5.2. Comisia face referire la ceea ce s-a făcut pentru RGPD (comunicare, pagina 23). Într-adevăr, regulamentul sus-menționat se întemeiază pe avizul AEPD ([6]), care poate servi drept text de referință și pentru RDNP. Asociațiile reprezentanților unui sector de activitate își pot elabora propriul cod de conduită. Autorii trebuie să demonstreze autorităților competente (CompSA) că proiectul lor de cod, fie el național sau transnațional, răspunde unei nevoi sectoriale specifice, facilitează punerea în aplicare a regulamentului și instituie mecanisme eficace de monitorizare a respectării codului.

([4]) JO C 227, 28.6.2018, p. 86.
([5]) JO C 218, 23.7.2011, p. 130.
([6]) AEPD – Autoritatea Europeană pentru Protecția Datelor; linii directoare 1/2019 privind codurile de conduită, 12.2.2019, https://edpb.europa.eu/our-work-tools/our-documents/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

4.5.3. Chiar înainte de intrarea în vigoare a RGPD, principalii furnizori de infrastructură ca serviciu (*IaaS*) și de software ca serviciu (*SaaS*) își elaboraseră propriul cod de conduită pentru a-și defini modalitățile de punere în aplicare, eliminând astfel zonele de incertitudine identificate de specialiștii din domeniu ([7]); ei s-au asociat cu IMM-urile, considerând că, pentru multe dintre ele, autocertificarea era de preferat certificării, al cărei cost este foarte ridicat.

4.5.4. CESE sprijină o abordare sectorială în cazul RDNP, dacă o formulă unică, universal valabilă, nu pare a fi acceptată. În contextul RGPD, a fost stabilită o listă neexhaustivă a elementelor care trebuie incluse în coduri [articolul 40 alineatul (2)], în special în ceea ce privește caracterul echitabil și transparent al procedurilor, securitatea transferului de date și soluționarea litigiilor. În interesul propriu și pentru a consolida încrederea consumatorilor în abordarea europeană, părțile interesate ar trebui încurajate să pornească de la un spirit de responsabilitate, etică și solidaritate, pe care să îl dezvolte, în special prin intermediul unor orientări care să ia în considerare inteligența artificială. Acesta este unul dintre aspectele pe care Comitetul dorește să le scoată în evidență: să recomande Comisiei să nu să lase ca autoreglementarea și soluționarea „pe cale amiabilă"a litigiilor să dea naștere la interpretări divergente ale textelor. Dimpotrivă, ar trebui să se depună toate eforturile pentru a le unifica, astfel încât să devină ulterior norme aplicabile tuturor, și să anunțe acest lucru în foile sale de parcurs privind informarea și comunicarea.

5. **Evaluarea**

Comisia va trece la o evaluare regulată cu privire la impactul liberei circulații, la aplicarea regulamentului, la abrogarea măsurilor restrictive de către statele membre și la eficacitatea codurilor de conduită. CESE consideră că reprezentanții societății civile ar trebui invitați să își exprime opiniile în acest context ([8]). Pentru ca societatea în ansamblu să se simtă în siguranță și astfel să aibă încredere în aceste noi practici digitale, atât Uniunea, cât și statele membre trebuie să disipeze incertitudinile în ceea ce privește legea aplicabilă, confidențialitatea, păstrarea și recuperarea fără pierdere a datelor, garanțiile de fezabilitate și buna-credință a părților interesate, precum și garanțiile financiare. Legătura indisolubilă dintre date care sunt DP și DNP deopotrivă reprezintă o sursă de îngrijorare, iar ponderea acestui tip de date în ansamblul tuturor datelor determină CESE să își pună întrebarea dacă autoreglementarea este cu adevărat singura cale de urmat. Comitetul recomandă ca, pe termen mediu, normele RGPD să se aplice tuturor datelor și întregii circulații a datelor, excepție făcând „adevăratele"DNP.

Bruxelles, 25 septembrie 2019.

Președintele
Comitetului Economic și Social European
Luca JAHIER

([7]) CISPE (*Cloud Infrastructure Services Providers in Europe*).
([8]) JO C 487, 28.12.2016, p. 92; JO C 62, 15.2.2019, p. 292.

ANEXĂ

Următoarele propuneri de amendamente au fost respinse, dar au întrunit cel puțin o pătrime din voturile exprimate [articolul 59 alineatul (3) din Regulamentul de procedură]:

Punctul 4.1.3

Se modifică după cum urmează:

Întreprinderea trebuie să își pună întrebarea dacă datele fără caracter personal pe care le prelucrează sunt „legate în mod indisolubil" de datele cu caracter personal și să le protejeze, în cazul în care se verifică această afirmație. Pentru întreprindere, pregătirea acestei „gestionări" (out management) nu este o sarcină ușoară. Formularea unei definiții generale a datelor mixte pare a fi imposibilă, iar suprapunerea celor două regulamente va conduce, probabil, la alte suprapuneri, cu texte referitoare la legislația în materie de date, precum cele referitoare la proprietatea intelectuală: DNP pot circula, dar dacă sunt reutilizate într-o lucrare, nu vor mai face obiectul acelorași norme. În opinia CESE, corelarea diferitelor texte va fi foarte delicată. Jurisprudența a cerut deja ca legătura „indisolubilă" sus-menționată să fie analizată prin prisma unui criteriu „rezonabil". CESE constată că, în mod evident, comunicarea supusă examinării nu poate trece în revistă toate cazurile posibile, pentru a ajuta părțile interesate, și că, în această situație, sunt favorizate mai curând întreprinderile mari. CESE recomandă Comisiei să se asigure că, în practică, DP nu ajung treptat să fie considerate drept DNP și să facă în așa fel încât RGPD să își păstreze în întregime domeniul de aplicare~~, chiar dacă, pentru aceasta, trebuie contopite cele două regulamente pe termen mediu,~~ în sensul creșterii protecției datelor, și nu al comercializării lor.

Punctul 5

Se modifică după cum urmează:

Comisia va trece la o evaluare regulată cu privire la impactul liberei circulații, la aplicarea regulamentului, la abrogarea măsurilor restrictive de către statele membre și la eficacitatea codurilor de conduită. CESE consideră că reprezentanții societății civile ar trebui invitați să își exprime opiniile în acest context. Pentru ca societatea în ansamblu să se simtă în siguranță și astfel să aibă încredere în aceste noi practici digitale, atât Uniunea, cât și statele membre trebuie să disipeze incertitudinile în ceea ce privește legea aplicabilă, confidențialitatea, păstrarea și recuperarea fără pierdere a datelor, garanțiile de fezabilitate și buna-credință a părților interesate, precum și garanțiile financiare. Legătura indisolubilă dintre date care sunt DP și DNP deopotrivă reprezintă o sursă de îngrijorare, iar ponderea acestui tip de date în ansamblul tuturor datelor determină CESE să își pună întrebarea dacă autoreglementarea este cu adevărat singura cale de urmat. ~~Comitetul recomandă ca, pe termen mediu, normele RGPD să se aplice tuturor datelor și întregii circulații a datelor, excepție făcând „adevăratele" DNP.~~

Punctul 1.1, a treia liniuță

Se modifică după cum urmează:

CESE recomandă Comisiei:

…

— *să se asigure – promovând totodată libera circulație – de faptul că datele cu caracter personal (DP) nu ajung, treptat, să fie considerate drept date fără caracter personal (DNP) și că Regulamentul general privind protecția datelor (RGPD) își păstrează în întregime domeniul de aplicare,~~ chiar dacă, pentru aceasta, trebuie contopite cele două regulamente pe termen mediu,~~ în ~~sensul~~vederea creșterii protecției datelor, și nu a comercializării lor;*

…

Expunere de motive

RGPD și Regulamentul (UE) 2018/1807 au temeiuri juridice diferite, și anume articolul 16 din TFUE privind dreptul fundamental la protecția datelor cu caracter personal și, respectiv, articolul 114 din TFUE privind apropierea legislațiilor, cele două dispoziții permițând UE să intervină în mod diferit asupra întreprinderilor private (acesta fiind motivul pentru care în primul caz UE a intervenit printr-o reglementare foarte strictă și detaliată, iar în al doilea caz a ales autoreglementarea ca mijlocul de intervenție cel mai potrivit și proporțional). Așadar, cele două instrumente nu pot fi contopite sub aspect juridic.

Rezultatul votului asupra amendamentului:

Voturi pentru: 54

Voturi împotrivă: 84

Abțineri: 18