COMISIA EUROPEANĂ

Bruxelles 17.9.2013
C(2013) 5903 final

Domnul Valeriu Ştefan ZGONEA
Preşedinte al
Camerei Deputaţilor
Palatul Parlamentului
Str. Izvor nr. 2-4, sector 5
RO – 050563 BUCUREŞTI

Stimate Domnule Preşedinte,

Comisia ar dori să vă mulţumească pentru opinia Camerei Deputaţilor cu privire la propunerea de Regulament general privind protecţia datelor[1] *şi la propunerea de directivă privind protecţia datelor destinată autorităţilor poliţieneşti şi judiciare [COM (2012) 11 final], [COM (2012) 10 final], [COM (2012) 9 final]. Ne cerem scuze pentru întârzierea cu care vă transmitem acest răspuns.*

Comisia constată cu satisfacţie interesul şi atenţia specială pe care Camera Deputaţilor a acordat-o pachetului privind protecţia datelor şi salută observaţiile şi sugestiile punctuale pe care le-aţi prezentat.

Comisia ar dori să sublinieze faptul că pachetul de reforme privind protecţia datelor pe care l-a propus în luna ianuarie este destinat să creeze un cadru modern, puternic, coerent şi cuprinzător în materie de protecţie a datelor în Uniunea Europeană. Un astfel de cadru ar aduce beneficii persoanelor fizice, consolidându-le drepturile şi libertăţile fundamentale în ceea ce priveşte prelucrarea datelor cu caracter personal şi încrederea în mediul digital. De asemenea, ar simplifica semnificativ cadrul juridic pentru întreprinderi şi sectorul public. Se aşteaptă ca acest lucru să stimuleze dezvoltarea economiei digitale în ansamblul pieţei unice

[1] „Propunere de regulament al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (Regulament general privind protecţia datelor)", COM (2012) 11 final („Regulament").

a UE și dincolo de granițele acesteia, în conformitate cu obiectivele Strategiei „Europa 2020" și ale Agendei digitale pentru Europa.

În sfârșit, reforma va contribui la creșterea încrederii în rândul autorităților de aplicare a legii în scopul facilitării schimburilor de date dintre acestea și al cooperării în lupta împotriva formelor grave de criminalitate, asigurând, în același timp, un nivel ridicat de protecție a persoanelor fizice.

Pachetul constituie, de asemenea, un răspuns la apelurile insistente lansate de colegislatori, Consiliul[2] și Parlamentul European[3], precum și de diversele părți interesate, pentru crearea unui cadru juridic care să încorporeze standarde ridicate și care să se bazeze pe o abordare globală.

Fără a exclude evaluarea mai aprofundată a aspectelor conexe în cursul procedurilor legislative, Comisia ar dori să vă explice poziția sa cu privire la principalele probleme ridicate în opinia Camerei Deputaților:

I. Referitor la propunerea de directivă:

În ceea ce privește propunerea de directivă destinată autorităților polițienești și judiciare în materie penală, care ar urma să înlocuiască Decizia-cadru 2008/977/JAI[4], Comisia a propus ca domeniul de aplicare să includă nu numai prelucrarea datelor la nivel transfrontalier, ci și activitățile de prelucrare realizate în cadrul cooperării polițienești și judiciare la nivel național.

În primul rând, Comisia ar dori să sublinieze că nici articolul 8 din Carta drepturilor fundamentale a UE și nici articolul 16 din Tratatul privind funcționarea Uniunii Europene (TFUE), astfel cum au fost introduse în dreptul Uniunii prin Tratatul de la Lisabona, nu fac o distincție între operațiunile de prelucrare a datelor desfășurate la nivel național și cele desfășurate la nivel transfrontalier, ci se referă la posibilitatea adoptării unor norme referitoare la prelucrarea datelor cu caracter personal, precum și la libera circulație a acestora, în toate domeniile care intră în sfera de aplicare a dreptului UE. Comisia consideră că articolul 16 din TFUE permite organelor legislative ale Uniunii să adopte norme UE cu privire la prelucrarea datelor cu caracter personal de către autoritățile polițienești și judiciare în materie penală indiferent dacă prelucrarea are loc numai la nivel național sau are o dimensiune transfrontalieră.

---

[2] Concluziile Consiliului privind Comunicarea Comisiei către Parlamentul European și Consiliu — O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană, a 3071-a reuniune a Consiliului Justiție și Afaceri Interne, Bruxelles, 24 și 25 februarie 2011.

[3] Rezoluția Parlamentului European din 6 iulie 2011 referitoare la o abordare globală a protecției datelor cu caracter personal în Uniunea Europeană P7_TA_(2011)0323.

[4] Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO L 350/2008, p. 60 (denumită în continuare „Decizia-cadru").

În plus, evaluarea efectuată de Comisie în ceea ce privește decizia-cadru[5] *a arătat că diferențierea care se face între „prelucrarea transfrontalieră a datelor și prelucrarea la nivel național" este o distincție artificială care — astfel cum s-a confirmat de către unele state membre în timpul consultărilor Comisiei — ar putea crea, de asemenea, probleme de ordin practic pentru autoritățile de aplicare a legii: unui ofițer de poliție îi este greu să facă distincția, în cursul unei anchete, între date cu „origini" diferite și să aplice norme distincte unor astfel de date cu caracter personal. În plus, nu se poate prevedea întotdeauna în prealabil dacă datele cu caracter personal colectate de un stat membru vor face apoi obiectul schimburilor transfrontaliere. Prin urmare, existența unor norme comune care să acopere atât prelucrarea datelor la nivel „național", cât și transmiterile transfrontaliere între statele membre reprezintă o condiție preliminară pentru schimbul eficient de date cu caracter personal și va consolida cooperarea în domeniul aplicării legii în UE.*

În ceea ce privește definirea clară a noțiunii de „securitate națională", nici tratatele și niciun alt instrument din legislația UE nu propun o definiție pentru „securitatea națională", deși în tratate se fac mai multe trimiteri la aceasta. Articolul 4 din Tratatul privind Uniunea Europeană (TUE) prevede că Uniunea Europeană acționează în limitele competențelor care îi sunt atribuite prin tratate de către statele membre. Articolul 4 alineatul (2) din TUE prevede că „securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru". În mod similar, articolele 72 și 73 din TFUE se referă la securitatea internă și națională ca la o responsabilitate care le revine statelor membre.

În ceea ce privește autoritățile de supraveghere a protecției datelor (DPA), atât articolul 8 din Cartă, cât și articolul 16 alineatul (2) din TFUE impun existența unor autorități independente care să verifice respectarea normelor privind prelucrarea datelor cu caracter personal. Rolul acestor autorități de supraveghere a protecției datelor total independente este esențial pentru asigurarea respectării normelor privind protecția datelor cu caracter personal. Aceste autorități veghează la respectarea drepturilor și libertăților fundamentale în materie de protecție a datelor cu caracter personal, persoanele bazându-se pe acestea pentru asigurarea protecției datelor lor cu caracter personal și a legalității operațiunilor de prelucrare a acestora.

Cu toate acestea, Comisia a constatat că statutul de independență, resursele și competențele acestor autorități naționale de supraveghere variază în mod considerabil între statele membre. Prin urmare, atât propunerea de regulament, cât și cea de directivă ar urma să sporească și mai mult independența autorităților naționale de supraveghere a protecției datelor care aplică cerințele impuse de Curtea de Justiție a Uniunii Europene (CJUE) prin clarificarea în detaliu a condițiilor necesare pentru instituirea și pentru asigurarea deplinei independențe a autorităților de supraveghere din statele membre. Propunerile respective se

[5] A se vedea evaluarea impactului care însoțește pachetul de reforme privind protecția datelor [SEC (2012) 72 final], precum și raportul privind punerea în aplicare a Deciziei-cadru [COM (2012) 12].

inspiră din dispozițiile relevante din Regulamentul (CE) nr. 45/2001[6]*, luând în același timp în considerare tradițiile constituționale din statele membre în ceea ce privește numirea autorităților de protecție a datelor (și anume, de către parlament sau guvern)*[7]*. În ceea ce privește mențiunea de la articolul 39 din directiva propusă în conformitate cu care „fiecare stat membru prevede dispoziții potrivit cărora una sau mai multe autorități publice sunt responsabile de monitorizarea aplicării dispozițiilor adoptate în temeiul directivei", aceasta se înscrie în logica articolului 25 alineatul (1) din Decizia-cadru 2008/977/JAI și a Directivei 95/46/CE.*

II. Referitor la propunerea de Regulament general privind protecția datelor:

În ceea ce privește opiniile dumneavoastră privind DPA și numirea acestora, observațiile de mai sus privind directiva propusă sunt în întregime valabile pentru regulamentul propus. În ceea ce privește controlul financiar, propunerea prevede la articolul 47 că „statele membre se asigură că autoritatea de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale. Statele membre se asigură că autoritatea de supraveghere dispune de bugete anuale distincte. Bugetele se fac publice." Această dispoziție trebuie înțeleasă în contextul general în care autoritățile de supraveghere a protecției datelor trebuie să nu fie influențate politic în exercitarea atribuțiilor și competențelor lor și să fie – și din punctul de vedere al resurselor și infrastructurii - în măsură să asigure efectiv protecția datelor cu caracter personal — în propria țară, precum și în cooperarea cu autoritățile de supraveghere din alte state membre și în cadrul mecanismului pentru asigurarea coerenței.

În ceea ce privește rolul Comisiei în cadrul mecanismului pentru asigurarea coerenței, trebuie subliniate mai multe aspecte. Noul mecanism pentru asigurarea coerenței este destinat să contribuie la raționalizarea activității între autoritățile de protecție a datelor. Mecanismul pentru asigurarea coerenței ar asigura o abordare armonizată cu privire la orice problemă de importanță europeană, fie că este vorba de cazuri individuale sau de aspecte generale legate de protecția datelor. Ajutându-se reciproc, autoritățile însărcinate cu protecția datelor și-ar întări puterea de intervenție. Mecanismul pentru asigurarea coerenței ar consolida, de asemenea, independența autorităților responsabile cu protecția datelor față de guvernele naționale. Presiunile la care ar fi supuse statele membre din partea celorlalte ar fi mult mai puternice decât în prezent, și problemele legate de insuficiența personalului sau lipsa resurselor ar fi mai vizibile.

Rolul Comisiei în cadrul mecanismului pentru asigurarea coerenței este clar: o eventuală intervenție este o măsură care poate fi luată doar în ultimă instanță. Comisia acționează ca un mecanism de susținere. Competența sa de a suspenda o decizie a unei autorități de protecție a datelor se va limita la cazurile în care legislația UE este îndoielnică, sau în care există un risc de aplicare incoerentă a normelor noastre privind protecția datelor. Comisia nu își propune să devină o „autoritate supranațională de protecție a datelor". Deliberarea și

---

[6] Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date, JO L 8/2000, p.1.

[7] A se vedea, de asemenea, în acest sens, cazul *Comisia împotriva Germaniei*, C -518/07, punctul 44.

determinarea cazurilor individuale este de competența autorităților însărcinate cu protecția datelor, nu a Comisiei.

În ceea ce privește actele delegate, articolul 290 din TFUE permite organului legislativ al Uniunii să delege Comisiei competența de a adopta acte fără caracter legislativ și cu domeniu de aplicare general, care completează sau modifică anumite elemente neesențiale ale unui act legislativ (acte „cvasilegislative"). Regulamentul propus a fost elaborat în mod deliberat ca un instrument juridic neutru din punct de vedere tehnologic. Deși nu își propune să anticipeze toate evoluțiile tehnologice din următorii 20 de ani, a fost conceput astfel încât să poată fi adaptat la evoluțiile viitoare și ar trebui să aibă o anvergură suficient de mare încât să cuprindă inovațiile tehnologice și practicile de consum în schimbare. Actele delegate sunt instrumentele prevăzute în Tratatul de la Lisabona care permit ca normele și principiile enunțate în regulament să fie adaptate la evoluțiile viitoare fără ca acest lucru să conducă întotdeauna la revizuirea totală a textului legislativ.

În plus, actele juridice adoptate de Comisia Europeană în acest mod fac obiectul controlului ex-post exercitat de organul legislativ. Actele delegate pot intra în vigoare numai în cazul în care nu a fost exprimată nicio obiecție de către Parlamentul European sau Consiliu — de fapt, cele două organe legislative au drept de veto. În plus, organul legislativ își poate rezerva dreptul de a revoca ulterior competențele delegate Comisiei Europene. În același timp, Comisia este dispusă să reexamineze, de la caz la caz, competențele prevăzute în propunerea de regulament.

În legătură cu stabilirea sarcinilor responsabilului cu protecția datelor prin intermediul unui regulament, aceasta este situația în prezent, având în vedere că regulamentul propus prevede sarcinile responsabilului cu protecția datelor la articolul 37.

În ceea ce privește dreptul de a fi uitat, este vorba despre prelungirea dreptului la ștergerea datelor și, după cum se arată în propunere, se încadrează în limite stricte. Aceasta nu prevede o „clauză generală privind ștergerea datelor", dar permite ștergerea acestora în cazul în care nu mai sunt necesare în alte scopuri legitime. Așadar, este o obligație cu privire la mijloace și nu cu privire la rezultat. În plus, definirea „măsurilor rezonabile" ar depinde de situația specifică. Nu există „măsuri universale", iar dreptul de a fi uitat nu se limitează la soluții tehnice. Uneori, poate fi suficient un simplu e-mail către un site terț. În plus, regulamentul prevede excepțări importante pentru a garanta că libertatea de exprimare este luată pe deplin în considerare. Acest lucru le-ar permite, de exemplu, site-urilor de știri să continue să funcționeze pe baza acelorași principii. Noile dispoziții sunt clare: libertatea de exprimare, cercetarea istorică și cea științifică sunt protejate. Totuși, organele legislative pot solicita clarificări suplimentare în scopul de a asigura un maximum de securitate juridică. Același lucru este valabil și pentru dreptul la portabilitatea datelor, care dezvoltă dreptul de acces. Comisia va sprijini colegislatorii în aceste eforturi de clarificare și de ajustare a textului.

În ceea ce privește articolul 42 (Transferul în baza unor garanții corespunzătoare), pentru transferurile către țările terțe trebuie prezentate garanții corespunzătoare, în special clauze

standard de protecție a datelor, reguli corporatiste obligatorii și clauze contractuale. Posibilitatea de a face uz de clauzele standard ale Comisiei de protecție a datelor se bazează pe articolul 26 alineatul (4) din Directiva 95/46/CE. Ca element de noutate, în prezent, astfel de clauze standard de protecție a datelor ar putea fi, de asemenea, adoptate de o autoritate de supraveghere și declarate ca fiind general valabile de către Comisie. În prezent, regulile corporatiste obligatorii sunt menționate în mod specific în textul legislativ propus. Opțiunea privind clauzele contractuale oferă o anumită flexibilitate operatorului sau persoanei împuternicite de operator, sub rezerva autorizării prealabile de către autoritățile de supraveghere.

Comisia speră că aceste clarificări răspund problemelor ridicate de Camera Deputaților și așteaptă cu interes continuarea dialogului nostru politic în viitor.

Cu deosebită considerație,

Maroš Šefčovič
Vicepreședinte