CONSILIUL UNIUNII EUROPENE

Bruxelles, 14 februarie 2012 (15.02)

6468/12

Dosar interinstituțional: 2012/0009 (NLE)

EEE 8
TRANS 43
CH 6
MI 93
AELE 8
N 3
ISL 3
FL 6

PROPUNERE

Sursă:	Comisia Europeană
Data:	(date of receipt)
Nr. doc. Csie:	COM(2012) 43 final
Subiect:	COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL ȘI COMITETUL REGIUNILOR Protecția vieții private într-o lume interconectată Un cadru european privind protecția datelor pentru secolul 21

În anexă, se pune la dispoziția delegațiilor o propunere din partea Comisiei, transmisă printr-o notă de însoțire din partea dlui Jordi AYET PUIGARNAU, director, către dl Uwe CORSEPIUS, Secretar General al Consiliului Uniunii Europene.

Anexă: COM(2012) 43 final

COMISIA EUROPEANĂ

Bruxelles, 25.1.2012
COM(2012) 9 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL ȘI COMITETUL REGIUNILOR

Protecția vieții private într-o lume interconectată
Un cadru european privind protecția datelor pentru secolul 21

(Text cu relevanță pentru SEE)

[…]

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ŞI SOCIAL ŞI COMITETUL REGIUNILOR

Protecţia vieţii private într-o lume interconectată
Un cadru european privind protecţia datelor pentru secolul 21

(Text cu relevanţă pentru SEE)

1. PROVOCĂRILE ACTUALE PRIVIND PROTECŢIA DATELOR

Ritmul rapid al schimbărilor tehnologice şi globalizarea au transformat profund modul în care este colectat, accesat, utilizat şi transferat volumul tot mai mare de date cu caracter personal. Noile modalităţi de a face schimb de informaţii prin intermediul reţelelor sociale şi stocarea unor cantităţi mari de date la distanţă au devenit o parte a vieţii multor din cei 250 de milioane de utilizatori ai internetului din Europa. În acelaşi timp, pentru multe întreprinderi, datele cu caracter personal reprezintă un avantaj. Colectarea, agregarea şi analizarea datelor privind clienţii potenţiali constituie adesea o parte importantă a activităţilor lor economice[1].

În cadrul acestui nou mediu digital, **persoanele au dreptul să beneficieze de un control efectiv asupra informaţiilor cu caracter personal.** Protecţia datelor este un drept fundamental în Europa, prevăzut la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene şi la articolul 16 alineatul (1) din Tratatul privind funcţionarea Uniunii Europene (TFUE), care trebuie protejat în mod corespunzător.

Lipsa de încredere îi face pe consumatori să ezite în ceea ce priveşte achiziţionarea de produse online sau acceptarea de noi servicii. Prin urmare, un nivel ridicat de protecţie a datelor este, de asemenea, crucial pentru creşterea încrederii în serviciile online şi pentru valorificarea potenţialului economiei digitale, încurajând astfel **creşterea economică şi competitivitatea industriilor din UE**.

Sunt necesare norme moderne şi coerente pe întreg teritoriul UE pentru ca datele să circule liber de la un stat membru la altul. Întreprinderile au nevoie de norme clare şi uniforme care să le ofere securitate juridică şi să reducă sarcina administrativă la minimum. Acest lucru este esenţial pentru ca piaţa unică să funcţioneze şi să **stimuleze creşterea economică, să creeze noi locuri de muncă şi să încurajeze inovarea**[2]. O modernizare a normelor UE în materie de protecţie a datelor care să consolideze dimensiunea acestora privind piaţa internă, să asigure un nivel ridicat de protecţie a datelor persoanelor fizice şi să promoveze securitatea juridică, claritatea şi coerenţa; prin urmare, aceasta joacă un rol central în cadrul Planului de acţiune de la

---

1 Piaţa pentru analizarea seturilor de date foarte mari este în creştere cu 40% pe an la nivel mondial: http://www.mckinsey.com/mgi/publications/big_data/.

2 A se vedea, de asemenea, concluziile Consiliului European din 23 octombrie 2011 care subliniază „rolul esenţial" al pieţei unice „în asigurarea creşterii economice şi a ocupării forţei de muncă", precum şi necesitatea de a finaliza piaţa digitală unică până în 2015.

Stockholm al Comisiei Europene[3], al Agendei digitale pentru Europa[4] și, în sens mai larg, contribuie la strategia UE privind creșterea economică (Strategia Europa 2020[5]).

Directiva UE din 1995[6], principalul instrument legislativ privind protecția datelor cu caracter personal în Europa, a reprezentat un punct de reper în istoria protecției datelor. Obiectivele sale privind asigurarea unei piețe unice funcționale și protecția efectivă a drepturilor fundamentale și a libertăților persoanelor sunt în continuare valabile. Cu toate acestea, directiva a fost adoptată în urmă cu 17 ani când internetul era în fază incipientă. În noul mediu digital plin de provocări din zilele noastre, normele existente nu oferă nici gradul de armonizare corespunzător, nici eficiența necesară pentru a asigura dreptul la protecția datelor cu caracter personal. Acesta este motivul pentru care Comisia Europeană propune o reformă fundamentală a cadrului UE privind protecția datelor.

În plus, Tratatul de la Lisabona a creat, prin articolul 16 din TFUE, un nou temei juridic pentru o abordare globală și modernizată a protecției datelor și a liberei circulații a datelor cu caracter personal, care acoperă, de asemenea, cooperarea polițienească și judiciară în materie penală[7]. Această abordare se reflectă în comunicările Comisiei Europene privind Programul de la Stockholm și în Planul de acțiune de la Stockholm[8], care subliniază necesitatea ca Uniunea „să instituie un regim cuprinzător de protecție a datelor cu caracter personal care să acopere toate domeniile de competență ale UE” și „să se asigure că dreptul fundamental privind protecția datelor este aplicat în mod coerent”.

Pentru a pregăti în mod transparent reforma cadrului UE privind protecția datelor, Comisia a lansat, încă din 2009, consultări publice în acest domeniu[9] și s-a angajat într-un dialog intens cu părțile interesate[10]. La 4 noiembrie 2010, Comisia a publicat o comunicare privind o abordare globală a protecției datelor cu caracter personal în Uniunea Europeană[11], care precizează principalele teme ale reformei. În perioada septembrie - decembrie 2011, Comisia a fost implicată într-un dialog intens cu autoritățile naționale pentru protecția datelor din Europa și cu Autoritatea Europeană

---

3 COM(2010)171 final.
4 COM(2010) 245 final.
5 COM(2010) 2020 final.
6 Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO L 281, 23.11.1995, p. 31.
7 Normele specifice pentru prelucrarea de către statele membre a datelor în materie de politică externă și de securitate comună se stabilesc printr-o decizie a Consiliului în temeiul articolului 39 din TUE.
8 COM (2009) 262 și, respectiv, COM (2010) 171.
9 Au fost lansate două consultări publice privind reforma protecției datelor: prima a avut loc din iulie până în decembrie 2009 ((http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) și a doua din noiembrie 2010 până în ianuarie 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).
10 În 2010, au fost organizate consultări specifice cu autoritățile statelor membre și părțile interesate din sectorul privat. În noiembrie 2010, comisarul UE pentru justiție, Viviane Reding, a organizat o masă rotundă având ca temă reforma în materie de protecție a datelor. De asemenea, pe parcursul anului 2011, s-au mai organizat alte ateliere și seminarii cu privire la aspecte specifice (de exemplu,. notificările în caz de încălcare a securității datelor).
11 COM(2010) 609.

pentru Protecția Datelor în vederea explorării opțiunilor pentru o aplicare mai coerentă a normelor UE privind protecția datelor în toate statele membre ale Uniunii[12].

În urma acestor discuții, a rezultat în mod clar că atât cetățenii, cât și întreprinderile doreau realizarea de către Comisia Europeană a unei reforme cuprinzătoare a normelor UE în materie de protecție a datelor. După evaluarea efectelor diferitelor opțiuni de politică[13], Comisia Europeană propune în prezent **un cadru legislativ solid și coerent aplicabil tuturor politicilor Uniunii, care să consolideze drepturile persoanelor, dimensiunea protecției datelor privind piața unică și să contribuie la reducerea birocrației cu care se confruntă întreprinderile**[14]. În conformitate cu propunerea Comisiei, noul cadru ar trebui să fie constituit din:

– un **regulament** (de înlocuire a Directivei 95/46/CE), care stabilește un cadru general al UE privind protecția datelor[15]; și

– o **directivă** (de înlocuire a Deciziei-cadru 2008/977/JAI[16]), care definește normele privind protecția datelor cu caracter personal prelucrate în scopul **prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor, precum și în scopul activităților judiciare conexe**.

Prezenta comunicare descrie principalele elemente ale reformei cadrului UE privind protecția datelor.

2. EXERCITAREA CONTROLULUI DE CĂTRE PERSOANE ASUPRA DATELOR ACESTORA CU CARACTER PERSONAL

Modalitățile prin care persoanele își pot exercita dreptul la protecția datelor, prevăzute în Directiva 95/46/CE – principalul act legislativ al UE în domeniul protecției datelor în vigoare – nu sunt suficient de armonizate în statele membre. De asemenea, nici competențele autorităților naționale responsabile cu protecția datelor nu sunt suficient de armonizate pentru a se asigura o aplicare coerentă și efectivă a normelor în acest domeniu. Aceasta înseamnă, de fapt, că exercitarea unor astfel de drepturi este mai dificilă în unele state membre decât în altele, în special on line.

---

12 A se vedea scrisoarea comisarului UE pentru justiție, Viviane Reding, din 19 septembrie 2011 adresată membrilor Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, publicată la adresa http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 A se vedea Evaluarea impactului [SEC (2012)72].

14 Reforma va include, într-o etapă ulterioară, modificări în vederea alinierii instrumentelor specifice și sectoriale, ca de exemplu Regulamentul (CE) nr. 45/2011 (JO L 8, 12.1.2001, p. 1).

15 Regulamentul aduce, de asemenea, un număr limitat de modificări tehnice Directivei asupra confidențialității și comunicațiilor electronice (Directiva 2002/58/CE, astfel cum a fost modificată prin Directiva 2009/136/CE - JO L 337, 18.12.2009, p. 11), pentru a lua în considerare transformarea Directivei 95/46/CE în regulament. Consecințele juridice de fond pe care noul regulament și noua directivă le vor presupune pentru Directiva asupra confidențialității și comunicațiilor electronice vor face, în timp util, obiectul unei revizuiri de către Comisie, ținând seama de rezultatul negocierilor privind propunerile actuale cu Parlamentul European și cu Consiliul.

16 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, 30.12.2008, p. 60. Un raport privind punerea în aplicare de către statele membre a deciziei-cadru [COM(2012)12] este adoptat ca parte a pachetului de reforme privind protecția datelor.

Aceste dificultăți sunt cauzate, de asemenea, de volumul datelor colectate zilnic și de faptul că utilizatorii nu sunt întotdeauna pe deplin conștienți că datele lor cu caracter personal sunt colectate. Deși numeroși europeni consideră că divulgarea datelor cu caracter personal constituie, într-o măsură din ce în ce mai mare, o parte a vieții moderne[17], 72% dintre utilizatorii de internet din Europa sunt preocupați în continuare de faptul că li se cere divulgarea unui număr prea mare de date cu caracter personal online[18]. Aceștia au sentimentul că nu dețin controlul asupra datelor cu caracter personal. De asemenea, consideră că nu sunt corect informați cu privire la ceea ce se întâmplă cu informațiile lor cu caracter personal, la destinatarii acestor informații și la scopul transmiterii acestora. Adesea, utilizatorii nu știu cum să își exercite drepturile online.

„Dreptul de a fi uitat"

Un student european care este membru al unui serviciu de socializare online decide să solicite accesul la toate datele sale cu caracter personal pe care le deține rețeaua. Cu această ocazie, realizează că rețeaua colectează mult mai multe date decât credea și că anumite date cu caracter personal despre care acesta credea că au fost șterse, erau stocate în continuare de către rețea.

Reforma normelor UE în materie de protecție a datelor va garanta că o astfel de situație nu mai poate avea loc, prin introducerea:

- unei cerințe explicite care obligă serviciile de socializare online (și toți ceilalți operatori de date) să limiteze la minimum volumul de date cu caracter personal ale utilizatorilor pe care le culeg și prelucrează;

- unei cerințe privind asigurarea faptului că setările standard ale sistemului garantează că datele nu sunt făcute publice;

- unei obligații explicite a operatorilor de date de a șterge datele cu caracter personal ale unei persoane în cazul în care persoana solicită în mod explicit acest lucru și în cazul în care nu există alte motive întemeiate pentru păstrarea lor.

În acest caz specific, furnizorul rețelei sociale ar avea obligația de a șterge imediat totalitatea datelor referitoare la student.

Astfel cum se subliniază în „O Agendă digitală pentru Europa", preocupările legate de viața privată sunt printre cele mai frecvente motive pentru care oamenii nu cumpără bunuri și servicii online. Având în vedere contribuția sectorului tehnologiilor informației și comunicațiilor (TIC) la creșterea globală a productivității în Europa – 20% provenind direct de la sectorul TIC și 30% de la investițiile în cadrul TIC[19] – încrederea în aceste servicii este foarte importantă pentru a stimula creșterea economiei UE și competitivitatea industriei europene.

---

17 A se vedea Eurobarometrul special 359 – Atitudini privind protecția datelor și identitatea electronică în Uniunea Europeană, iunie 2011, p. 23.

18 Ibidem, p. 54.

19 A se vedea „O agenda digitală pentru Europa", cit., p. 4.

Notificările privind încălcarea securității datelor

Hackerii au atacat un serviciu de jocuri de noroc care se adresează utilizatorilor din UE. Încălcarea a afectat baze de date care conțineau date cu caracter personal (inclusiv nume, adrese și, posibil, date referitoare la cărțile de credit) ale zeci de milioane de utilizatori din întreaga lume. Societatea respectivă a așteptat o săptămână înainte de a notifica utilizatorii în cauză.

Reforma normelor UE în materie de protecție a datelor va asigura faptul că o astfel de situație nu mai poate avea loc, noile norme obligând societățile să:

- consolideze măsurile de securitate pentru a preveni și evita încălcarea securității datelor;

- notifice încălcarea securității datelor atât autorității naționale de protecție a datelor - dacă este posibil, în termen de 24 de ore de la constatare – cât și persoanelor în cauză, fără întârzieri nejustificate.

Noile acte legislative propuse de Comisie au ca obiectiv consolidarea drepturilor, punerea la dispoziția cetățenilor a unor mijloace eficiente și operaționale pentru a se asigura că aceștia sunt informați pe deplin cu privire la ceea ce se întâmplă cu datele lor cu caracter personal și pentru a le permite să își exercite drepturile într-un mod mai eficace.

În vederea consolidării dreptului persoanelor fizice la protecția datelor, Comisia propune noi norme care vor contribui la:

Îmbunătățirea capacității persoanelor de a-și exercita controlul asupra datelor care îi privesc, prin:

- garantarea faptului că, în cazul în care este necesar **consimțământul** persoanei în cauză, acesta este **acordat în mod explicit, adică se bazează fie pe o declarație, sau pe un act neechivoc al acesteia**, și în mod liber;

- oferirea posibilității utilizatorilor de internet de a-și exercita efectiv „**dreptul de a fi uitat"** în mediul online: dreptul ca datele lor să fie șterse în cazul în care aceștia își retrag consimțământul și în cazul în care nu există alte motive întemeiate pentru păstrarea datelor;

- garantarea **facilității accesului la propriile date** și **dreptul la portabilitatea datelor**: dreptul de a obține o copie a datelor stocate din partea operatorului și libertatea de a transfera datele de la un furnizor de servicii la altul, fără restricții;

- consolidarea **dreptului la informare**, astfel încât persoanele să înțeleagă pe deplin modul în care sunt utilizate datele lor cu caracter personal, în special în cazul în care operațiunile de prelucrare a datelor privesc **minorii**.

Îmbunătățirea mijloacelor de care dispun persoanele fizice pentru a fi în măsură să își exercite drepturile, prin:

- consolidarea **independenței și a competențelor autorităților naționale de protecție a datelor**, astfel încât acestea să dețină mijloacele necesare pentru soluționarea eficientă a plângerilor, să desfășoare investigații eficiente, să ia decizii cu caracter obligatoriu și să impună sancțiuni eficiente și disuasive;

- consolidarea **acțiunilor judiciare și a celor administrative** în cazul încălcării drepturilor privind protecția datelor. În special, asociațiile specializate în acest domeniu vor putea să introducă o acțiune în instanță în numele unei persoane fizice.

Consolidarea securității datelor, prin:

- încurajarea utilizării **tehnologiilor de consolidare a protecției vieții private** (tehnologii care protejează confidențialitatea informațiilor prin reducerea la minimum a datelor cu caracter personal stocare), a **setărilor standard care respectă confidențialitatea** și a **regimurilor de certificare a respectării confidențialității**;

- introducerea unei **obligații generale**[20] a operatorilor de date de a **notifica încălcarea securității datelor fără întârzieri nejustificate** atât autorităților pentru protecția datelor (în termen de 24 de ore, dacă acest lucru este posibil), cât și persoanelor în cauză.

O mai mare responsabilitate a celor care prelucrează date, în special prin:

- solicitarea desemnării de către operatori a unui **responsabil cu protecția datelor** în cadrul societăților cu mai mult de 250 de angajați și în întreprinderile implicate în operațiuni de prelucrare a datelor care, prin natura, domeniul de aplicare sau obiectivele lor, prezintă riscuri specifice pentru drepturile și libertățile persoanelor fizice („prelucrare riscantă”);

- introducerea **principiului privind luarea în considerare a vieții private începând cu momentul conceperii** (*privacy by design*) pentru a se asigura că garanțiile în materie de protecție a datelor sunt luate în considerare în faza de planificare a procedurilor și a sistemelor de prelucrare;

- introducerea obligației de a efectua **studii de impact privind protecția datelor** pentru organizațiile implicate în operațiuni de prelucrare riscante.

3. NORME ÎN MATERIE DE PROTECȚIE A DATELOR ADECVATE PENTRU PIAȚA DIGITALĂ UNICĂ

În pofida obiectivului directivei în vigoare de a asigura un nivel echivalent de protecție a datelor în ansamblul UE, există încă diferențe considerabile privind normele aplicate în statele membre. În consecință, operatorii de date trebuie să lucreze cu 27 de legislații și cerințe diferite la nivel național. Rezultatul acestei situații este un **mediu juridic fragmentat** care a generat **incertitudine juridică** și o protecție inegală a persoanelor. Acest lucru a cauzat **costuri și sarcini administrative inutile** pentru întreprinderi, fiind un factor de descurajare pentru întreprinderile care își desfășoară activitatea pe piața unică și care ar dori să își extindă activitatea pe plan internațional.

[20] Acest lucru este în prezent obligatoriu numai în sectorul telecomunicațiilor, în conformitate cu Directiva asupra confidențialității și comunicațiilor electronice.

Resursele și competențele autorităților naționale responsabile pentru protecția datelor variază în mod considerabil între statele membre[21]. În anumite cazuri, acestea nu sunt în măsură să își îndeplinească sarcinile de asigurare a aplicării legislației în mod satisfăcător. Cooperarea dintre aceste autorități la nivel european – prin intermediul grupului consultativ existent (așa-numitul Grup de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal)[22] – nu conduce întotdeauna la o aplicare coerentă a normelor în vigoare și trebuie, de asemenea, să fie îmbunătățită.

Aplicarea coerentă a normelor în materie de protecție a datelor în întreaga Europă

O societate multinațională cu mai multe sedii în UE a dezvoltat un sistem de cartografiere online în întreaga Europă, care colectează imagini ale tuturor clădirilor publice și private și, de asemenea, poate fotografia persoanele aflate pe stradă. Într-un stat membru, a fost considerată ilegală includerea în cadrul sistemului a fotografiilor clare ale persoanelor care nu erau conștiente de faptul că au fost fotografiate, în timp ce în alte state membre, acest lucru nu a fost considerat ca reprezentând o încălcare a legislației privind protecția datelor. Prin urmare, nu a existat o reacție coerentă în rândul autorităților naționale pentru protecția datelor în vederea remedierii acestei situații.

Prin reforma normelor UE în materie de protecție a datelor, se va asigura că situația menționată mai sus nu va mai putea avea loc în viitor, deoarece:

- cerințele și garanțiile privind protecția datelor vor fi prevăzute în cadrul unui regulament al UE cu aplicare directă în întreaga Uniune;

- autoritatea pentru protecția datelor din statul membru în care societatea în cauză își are sediul principal va fi singura responsabilă pentru a decide dacă societatea acționează în mod legal;

- o coordonare promptă și eficientă între autoritățile naționale pentru protecția datelor - având în vedere că serviciul se adresează persoanelor din mai multe state membre - va contribui la asigurarea faptului că noile norme ale UE în materie de protecție a datelor vor fi aplicate și respectate în mod coerent la nivelul tuturor statelor membre.

Este necesară consolidarea autorităților naționale și a cooperării între acestea pentru a garanta respectarea în mod coerent și, în ultimă instanță, aplicarea uniformă a normelor în întreaga UE.

Un cadru legislativ solid, clar și unitar la nivelul UE va contribui la valorificarea potențialului pieței digitale unice și la stimularea creșterii economice, a inovării și a creării de locuri de muncă. Adoptarea unui regulament va duce la eliminarea fragmentării regimurilor juridice din cele 27 de state membre și a barierelor la intrarea pe piață, un factor deosebit de important atât pentru microîntreprinderi, cât și pentru întreprinderile mici și mijlocii.

---

21 Pentru mai multe detalii cu privire la acest aspect, a se vedea studiul de impact care însoțește propunerile legislative, SEC (2012) 72.

22 Grupul de lucru a fost înființat în 1996 (prin articolul 29 din Directiva 95/46/CE), având un caracter consultativ și fiind format din reprezentanți ai autorităților naționale de supraveghere a protecției datelor (DPA), ai Autorității Europene pentru Protecția Datelor (AEPD) și ai Comisiei. Pentru mai multe informații cu privire la activitățile grupului de lucru, a se vedea http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

De asemenea, noile norme vor oferi un avantaj societăților din UE în contextul concurenței globale. Cadrul de reglementare revizuit le va permite acestora să ofere asigurări clienților cu privire la faptul că informațiile importante cu caracter personal vor fi tratate cu maximă atenție și seriozitate. Încrederea într-un regim de reglementare coerent la nivelul UE va reprezenta un avantaj major pentru prestatorii de servicii și un stimulent pentru investitorii aflați în căutare de condiții optime în vederea localizării serviciilor.

În vederea consolidării **dimensiunii protecției datelor privind piața unică**, Comisia propune:

- stabilirea normelor în materie de protecție a datelor la nivelul UE prin intermediul unui **regulament direct aplicabil în toate statele membre**[23] care va pune capăt aplicării cumulative și simultane a diferitelor legislații naționale în materie de protecție a datelor. Aceasta va conduce la realizarea de către societăți a unor **economii nete de aproximativ 2,3 miliarde EUR pe an numai în ceea ce privește sarcinile administrative**;

- **simplificarea cadrului de reglementare prin reducerea drastică a birocrației** și eliminarea **formalităților**, cum ar fi cerințele de notificare generală (generând economii nete în valoare de 130 de milioane EUR pe an numai în ceea ce privește sarcinile administrative). Dată fiind importanța acestora pentru competitivitatea economiei europene, se acordă o atenție specială nevoilor specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii;

- **consolidarea în continuare a independenței și a competențelor autorităților naționale pentru protecția datelor (APD)** pentru a le permite să efectueze anchete, să ia decizii cu caracter obligatoriu, să impună sancțiuni eficiente și disuasive și să oblige statele membre să le furnizeze **suficiente resurse** în acest sens;

- **instituirea unui sistem bazat pe un „ghișeu unic" privind protecția datelor în UE:** operatorii de date din UE vor lucra doar cu **o singură APD**, și anume autoritatea din statul membru în care se află sediul principal al societății;

- crearea condițiilor pentru o cooperare rapidă și eficientă între APD-uri, inclusiv obligația unei APD de a efectua anchete și inspecții la cererea unei alte APD, precum și recunoașterea reciprocă a deciziilor;

- **instituirea unui mecanism pentru asigurarea coerenței** la nivelul UE pentru ca deciziile APD-urilor care au un impact mai larg la nivel european să ia pe deplin în considerare opiniile celorlalte APD-uri în cauză și să fie în conformitate cu legislația UE;

- creșterea rolului Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal prin transformarea acestuia într-un comitet european independent pentru protecția datelor, ceea ce va conduce la o

[23] De asemenea, Comisia a prezentat o propunere de directivă în care să se definească normele aplicabile în domeniul cooperării polițienești și al cooperării judiciare în materie penală (a se vedea punctul 4 de mai jos), ceea ce va oferi statelor membre o mai mare flexibilitate în acest domeniu specific.

îmbunătățire a contribuției acestuia la aplicarea coerentă a legislației privind protecția datelor și la asigurarea unei baze solide pentru cooperarea între autoritățile de protecție a datelor, inclusiv cu Autoritatea Europeană pentru Protecția Datelor; precum și consolidarea sinergiilor și a eficacității prin asigurarea activităților de secretariat ale Comitetului european pentru protecția datelor de către Autoritatea Europeană pentru Protecția Datelor.

Noul regulament al UE va asigura o protecție solidă a dreptului fundamental la protecția datelor în toată Uniunea Europeană și va consolida funcționarea pieței unice. În același timp – având în vedere faptul că, astfel cum a subliniat Curtea de Justiție a UE[24], dreptul la protecția datelor cu caracter personal nu este unul absolut, ci trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate[25] și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității[26] – regulamentul va conține dispoziții explicite care să asigure respectarea celorlalte drepturi fundamentale, precum libertatea de exprimare și de informare, dreptul la apărare, precum și dreptul de a păstra secretul profesional (cum este cazul profesiilor juridice), fără a duce prejudicii statutului bisericilor în temeiul legislațiilor statelor membre.

4. UTILIZAREA DATELOR ÎN CADRUL COOPERĂRII POLIȚIENEȘTI ȘI JUDICIARE ÎN MATERIE PENALĂ

Intrarea în vigoare a Tratatului de la Lisabona și, în special, introducerea unui nou temei juridic (articolul 16 din TFUE) permit stabilirea unui cadru cuprinzător privind protecția datelor care asigură un înalt nivel de protecție pentru datele persoanelor fizice, respectând în același timp caracterul specific al domeniului cooperării polițienești și judiciare în materie penală. În special, cadrul revizuit al UE privind protecția datelor poate fi aplicat prelucrării datelor cu caracter personal atât la nivel transfrontalier, cât și la nivel național. Aceasta ar reduce diferențele dintre legislațiile statelor membre, aducând beneficii în domeniul protecției datelor cu caracter personal în ansamblul său. De asemenea, ar putea conduce la o simplificare a schimbului de informații între autoritățile polițienești și judiciare ale statelor membre și, prin urmare, la îmbunătățirea cooperării în lupta împotriva formelor grave de criminalitate în Europa. În prezent, prelucrarea datelor de către autoritățile polițienești și judiciare în materie penală este reglementată, în principal, prin Decizia-cadru 2008/977/JAI a Consiliului, care este anterioară intrării în vigoare a Tratatului de la Lisabona. Comisia nu are competența de a asigura respectarea normelor sale deoarece este vorba de o decizie-cadru, aceasta contribuind la o punere în aplicare inegală. În plus, domeniul de aplicare al deciziei-cadru este limitat la

---

24 Curtea de Justiție a UE, hotărârea din 9.11.2010 în cauzele conexate C-92/09 și C-93/09 Volker und Markus Schecke și Eifert Rep [2010], nepublicată încă.

25 În conformitate cu articolul 52 alineatul (1) din cartă, pot fi impuse limitări privind exercitarea dreptului la protecția datelor, atât timp cât acestea sunt prevăzute prin lege, respectă substanța acestor drepturi și libertăți și, sub rezerva principiului proporționalității, sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

26 Curtea de Justiție a UE, hotărârea din 6.11.2003, cauza C-101/01, Lindqvist [2003] ECR I-12971, para 82-90; hotărârea din 16.12.2008, C-73/07, Satamedia [2008], ECR I-9831, para 50-62.

activitățile de prelucrare transfrontaliere[27]. Aceasta înseamnă că prelucrarea datelor cu caracter personal care nu au făcut obiectul unor schimburi nu este acoperită, în prezent, de normele UE care reglementează o astfel de prelucrare și care protejează dreptul fundamental la protecția datelor. De asemenea, acest lucru generează, în anumite cazuri, dificultăți practice pentru poliție și alte autorități pentru care este posibil să nu fie evident dacă prelucrarea datelor trebuie să se desfășoare exclusiv la nivel național sau transfrontalier sau este dificil pentru autorități să prevadă dacă datele „naționale" ar putea face obiectul unui schimb transfrontalier ulterior[28].

Prin urmare, noul cadru revizuit al UE privind protecția datelor are ca scop asigurarea unui nivel coerent și ridicat de protecție a datelor în vederea **consolidării încrederii reciproce dintre autoritățile polițienești și judiciare din diferitele state membre, contribuind astfel la libera circulație a datelor și la o cooperare eficientă între aceste autorități.**

În vederea asigurării unui nivel ridicat de protecție a datelor cu caracter personal în domeniul cooperării polițienești și judiciare în materie penală și al facilitării schimburilor de date cu caracter personal între autoritățile polițienești și judiciare ale statelor membre, Comisia propune, ca parte a pachetului de reforme privind protecția datelor, o directivă care va urmări:

- **aplicarea principiilor generale în materie de protecție a datelor** în cazul cooperării polițienești și al cooperării judiciare în materie penală, respectând, în același timp, natura specifică a acestor domenii[29];

- prevederea unor **criterii și condiții minime armonizate privind posibilele limitări** referitoare la regulile generale. Aceasta vizează, în special, drepturile persoanelor de a fi informate atunci când autoritățile polițienești și judiciare prelucrează sau accesează datele persoanelor respective. Astfel de limitări sunt necesare pentru eficiența prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor;

- instituirea unor **norme specifice care să ia în considerare particularitățile activităților în materie de aplicare a legii, inclusiv o distincție între diferitele categorii de persoane vizate** (cum ar fi martorii și suspecții) ale căror drepturi pot varia.

5. PROTECȚIA DATELOR ÎNTR-O LUME GLOBALIZATĂ

Respectarea drepturilor persoanelor trebuie garantată în continuare atunci când datele cu caracter personal sunt transferate din UE către țări terțe și ori de câte ori sunt

---

27 Mai precis, decizia-cadru se aplică datelor cu caracter personal care sunt sau au fost transmise sau puse la dispoziție de către statele membre, sau schimbate între statele membre și instituțiile sau organismele UE [a se vedea articolul 1 alineatul (2)].

28 Acest lucru a fost confirmat de unele state membre în răspunsurile la chestionarul Comisiei referitor la raportul de punere în aplicare a deciziei-cadru [COM (2012) 12].

29 În conformitate cu Declarația nr. 21 privind protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, astfel cum este anexată la Actul final al Conferinței interguvernamentale care a adoptat Tratatul de la Lisabona.

vizate persoane din statele membre, iar datele acestora sunt utilizate sau analizate de către furnizori de servicii din țări terțe. Aceasta înseamnă că standardele UE în materie de protecție a datelor trebuie să fie aplicate indiferent de localizarea geografică a unei societăți sau al serviciului acesteia de prelucrare a datelor.

În lumea globalizată de astăzi, datele cu caracter personal sunt transferate peste un număr din ce în ce mai mare de frontiere virtuale și geografice, fiind stocate pe servere situate în numeroase țări. Din ce în ce mai multe companii oferă servicii de „cloud computing" (informatică dematerializată), care permit consumatorilor să aibă acces și să stocheze date pe servere aflate la distanță. Factorii menționați conduc la necesitatea îmbunătățirii mecanismelor actuale pentru transferul de date către țări terțe. Aceasta include decizii privind caracterul adecvat – și anume decizii de certificare a existenței unor standarde „adecvate" de protecție a datelor în țări terțe – și garanții corespunzătoare, cum ar fi clauzele contractuale standard sau regulile corporative cu forță juridică obligatorie[30], astfel încât să se asigure un nivel ridicat de protecție a datelor în cadrul operațiunilor de prelucrare a datelor la nivel internațional și să se faciliteze fluxurile transfrontaliere de date.

Reguli corporatiste obligatorii

Un grup de întreprinderi trebuie să transfere în mod curent date cu caracter personal de la filialele sale cu sediul în UE către filialele sale situate în țări terțe. Grupul ar dori să introducă un set de reguli corporatiste obligatorii (Binding Corporate Rules - BCR) pentru a se conforma legislației UE, limitând, în același timp, cerințele administrative pentru fiecare transfer individual. În practică, BCR garantează aplicarea unui set unic de norme în ansamblul grupului, în detrimentul existenței unor diverse contracte interne.

În conformitate cu practicile actuale stabilite la nivelul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, recunoașterea caracterului adecvat al garanțiilor prevăzute de regulile corporatiste obligatorii ale unei societăți implică o revizuire amănunțită efectuată de către trei APD-uri (o „autoritate principală" și două „autorități secundare"), precum și prezentarea de observații de către alte autorități în domeniu. În plus, multe dintre legislațiile statelor membre impun obținerea de autorizații naționale suplimentare în cazul transferurilor reglementate prin BCR, ceea ce conduce la un proces de adoptare foarte greoi, costisitor, lung și complex.

În urma reformei în materie de protecție a datelor:

- acest proces va fi mai simplu și mai raționalizat;

- BCR vor fi validate doar de o singură APD, iar mecanismele în vigoare vor asigura implicarea rapidă a altor APD relevante;

- odată ce o autoritate a aprobat o BCR, aceasta va fi valabilă pe întreg teritoriul UE, fără a avea nevoie de o autorizație suplimentară la nivel național.

[30] Regulile corporatiste obligatorii sunt coduri de bune practici bazate pe standarde europene de protecție a datelor, aprobate de cel puțin o APD, pe care organizațiile le stabilesc în mod voluntar și le respectă în scopul asigurării unor garanții corespunzătoare pentru diverse categorii de transferuri de date cu caracter personal între societăți care fac parte din același grup și care au obligații în temeiul acestor reguli. Acestea nu sunt incluse în mod explicit în Directiva 95/46/CE, fiind dezvoltate în cadrul practicii între APD-uri, cu sprijinul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal.

În vederea **abordării provocărilor generate de globalizare**, sunt necesare instrumente și mecanisme flexibile – în special pentru întreprinderile care își desfășoară activitatea pe plan mondial – garantând totodată o protecție a datelor persoanelor fizice fără niciun fel de neajunsuri. Comisia propune următoarele măsuri:

- elaborarea unor **norme clare** care să definească cazurile în care **legislația UE este aplicabilă operatorilor de date stabiliți în țări terțe**, în special, care să specifice că, de fiecare dată când sunt oferite bunuri și servicii persoanelor fizice din UE, sau când comportamentul lor este monitorizat, **se aplică normele europene**;

- orice **decizie privind caracterul adecvat al nivelului de protecție** va fi luată de către Comisia Europeană pe baza unor criterii explicite și clare, inclusiv în domeniul cooperării polițienești și al justiției penale;

- simplificarea fluxurilor legitime de date către țările terțe prin consolidarea și simplificarea **normelor privind transferurile internaționale** către țările care nu fac obiectul unei decizii privind caracterul adecvat al nivelului de protecție, în special prin raționalizarea și extinderea utilizării unor instrumente, cum ar fi **regulile corporatiste obligatorii**, astfel încât acestea să poată fi aplicate atât **operatorilor de date**, cât și în cadrul **grupurilor de societăți**, astfel, reflectând mai bine numărul din ce în ce mai mare de societăți implicate în activități de prelucrare a datelor, în special în domeniul „cloud computing”;

- inițierea unui **dialog** și, acolo unde este cazul, a unor **negocieri** cu țările terțe – în special cu partenerii strategici ai UE și cu țările care fac obiectul politicii europene de vecinătate – și cu organizațiile internaționale relevante (cum ar fi Consiliul Europei, Organizația pentru Cooperare și Dezvoltare Economică, Organizația Națiunilor Unite) pentru promovarea unor standarde **ridicate și interoperabile de protecție a datelor** în întreaga lume.

6. CONCLUZII

Reforma în materie de protecție a datelor își propune să dezvolte un **cadru modern, solid, coerent și cuprinzător privind protecția datelor în Uniunea Europeană**. Dreptul fundamental al persoanelor fizice la protecția datelor va fi consolidat. Alte drepturi, precum libertatea de exprimare și de informare, drepturile copilului, dreptul de a desfășura o activitate comercială, dreptul la un proces echitabil, dreptul de a păstra secretul profesional (cum este cazul profesiilor juridice), precum și statutul bisericilor în legislațiile statelor membre vor fi, de asemenea, respectate.

De această reformă vor beneficia, în primul rând, persoanele fizice, prin consolidarea drepturilor acestora privind protecția datelor și a încrederii lor în mediul digital. Reforma va simplifica în continuare cadrul legislativ pentru întreprinderi și sectorul public în mod substanțial. Se așteaptă ca acest lucru să stimuleze dezvoltarea economiei digitale în ansamblul pieței unice 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 schimburile 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.

Comisia Europeană va colabora strâns cu Parlamentul European și cu Consiliul în vederea finalizării, până la sfârșitul anului 2012, a unui acord referitor la noul cadru al UE privind protecția datelor. Pe toată durata procesului de adoptare și ulterior acestuia, în special în contextul punerii în aplicare a noilor instrumente juridice, Comisia va menține **un dialog strâns și transparent cu toate părțile interesate**, în care vor fi implicați reprezentanți ai sectorului public și privat, cum ar fi reprezentanți ai autorităților polițienești și judiciare, ai autorităților de reglementare în domeniul comunicațiilor electronice, ai organizațiilor societății civile, ai autorităților de protecție a datelor și ai mediului universitar, precum și ai agențiilor specializate ale UE, ca de exemplu Eurojust, Europol, Agenția pentru Drepturi Fundamentale, precum și Rețeaua Europeană și Agenția pentru o societate informațională (*European Network and Information Society Agency*).

În contextul dezvoltării constante a tehnologiilor informației și a comportamentelor sociale în continuă schimbare, este deosebit de importantă desfășurarea unui astfel de dialog pentru a putea beneficia de contribuțiile necesare în scopul asigurării unui nivel ridicat de protecție a datelor privind persoanele fizice, creșterii și competitivității industriilor UE, eficienței operaționale a sectorului public (inclusiv poliția și sistemul judiciar) și a unui nivel scăzut al sarcinii administrative.