COMISIA EUROPEANĂ

Bruxelles, 4.11.2010
COM(2010) 609 final

COMUNICAREA COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL ȘI COMITETUL REGIUNILOR

O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană

COMUNICAREA COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ŞI SOCIAL ŞI COMITETUL REGIUNILOR

O abordare globală a protecţiei datelor cu caracter personal în Uniunea Europeană

1. NOI PROVOCĂRI ÎN CEEA CE PRIVEŞTE PROTECŢIA DATELOR CU CARACTER PERSONAL

Directiva privind protecţia datelor cu caracter personal din 1995[1] a reprezentat un punct de reper în istoria protecţiei datelor cu caracter personal în Uniunea Europeană. Directiva consacră două dintre cele mai vechi şi la fel de importante ambiţii ale procesului de integrare europeană: protecţia drepturilor şi libertăţilor fundamentale ale persoanelor şi, în special, dreptul fundamental la protecţia datelor, pe de o parte, şi crearea pieţei interne – libera circulaţie a datelor cu caracter personal în acest caz – pe de altă parte.

Cincisprezece ani mai târziu, acest obiectiv dublu este în continuare de actualitate, iar principiile consacrate de directivă sunt în continuare pertinente. **Cu toate acestea, evoluţiile rapide în domeniul tehnologiei şi globalizarea au schimbat profund lumea din jurul nostru şi au creat noi provocări în ceea ce priveşte protecţia datelor cu caracter personal.**

În prezent, tehnologia le permite persoanelor să schimbe cu mai mare uşurinţă informaţii despre comportamentul sau preferinţele lor şi să le facă accesibile şi publice la nivel mondial, la o scară fără precedent. Site-urile de socializare, cu sute de milioane de membri de răspândiţi pe tot globul reprezintă, probabil, exemplul cel mai evident, dar nu unicul, al acestui fenomen. 'Cloud computing' - adică procesare bazată pe internet în care programele informatice, resursele comune şi informaţiile se află pe servere la distanţă ('in the cloud') care ar putea, de asemenea, să ridice probleme în ceea ce priveşte protecţia datelor, întrucât persoanele pot pierde controlul asupra informaţiilor potenţial sensibile care le privesc atunci când îşi stochează datele utilizând programe găzduite de echipamentele informatice ale altcuiva. Un studiu recent a confirmat că se pare că există o convergenţă de opinii – ale autorităţilor în domeniul protecţiei datelor, ale asociaţiilor profesionale şi ale organizaţiilor consumatorilor – potrivit cărora riscurile în ceea ce priveşte confidenţialitatea şi protecţia datelor cu caracter personal asociate activităţilor online[2] sunt din ce în ce mai mari.

În acelaşi timp, **modalităţile de colectare a datelor cu caracter personal au devenit din ce în ce mai elaborate şi mai greu de detectat**. De exemplu, utilizarea unor instrumente sofisticate le permite operatorilor economici să îşi orienteze activitatea astfel încât produsele lor să răspundă mai bine nevoilor persoanelor, graţie monitorizării comportamentului acestora. Iar utilizarea din ce în ce mai mare a procedurilor care permit colectarea automată de date, cum ar fi vânzarea de biletele de transport electronice şi colectarea taxelor de drum sau

---

1 Directiva 95/46/CE a Parlamentului European şi a Consiliului din 24.10.1995 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (JO L 281, 23.11.1995, p. 31).

2 A se vedea *Study on the economic benefits of privacy enhancing technologies* (Studiu privind beneficiile tehnologiilor de creştere a confidenţialităţii), *London Economics*, iulie 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), p. 14.

dispozitivele de geo-localizare, facilitează stabilirea locației persoanelor pur și simplu prin faptul că acestea folosesc un dispozitiv mobil. Autoritățile publice utilizează, de asemenea, din ce în ce mai multe date cu caracter personal în diverse scopuri, cum ar fi urmărirea persoanelor în eventualitatea apariției unei boli contagioase, prevenirea și lupta, mai eficace, împotriva terorismului și criminalității, administrarea sistemelor de securitate socială sau în scopuri fiscale, ca parte a aplicațiilor de e-guvernare ale acestora etc.

Toate acestea conduc inevitabil la întrebarea dacă legislația UE în domeniul protecției datelor existentă mai poate răspunde pe deplin și în mod eficace acestor provocări.

Pentru a aborda această problemă, Comisia a lansat o revizuire a cadrului juridic actual, prin organizarea unei conferințe la nivel înalt în mai 2009, urmată de o consultare publică deschisă până la sfârșitul anului 2009[3]. Au fost lansate, de asemenea, mai multe studii[4].

Concluziile au confirmat faptul că principiile de bază ale directivei sunt încă actuale și că ar trebui păstrat caracterul neutru din punct de vedere tehnologic al acesteia. Totuși, au fost identificate ca fiind problematice și ridicând provocări specifice, mai multe aspecte. Printre acestea se numără:

- *Abordarea impactului noilor tehnologii*

Răspunsurile la consultări, atât cele din partea persoanelor particulare, cât și din partea organizațiilor, au confirmat necesitatea clarificării și precizării modului de aplicare a principiilor privind protecția datelor la noile tehnologii, pentru a asigura o protecția reală și efectivă a datelor cu caracter personal ale persoanelor, indiferent de tehnologia utilizată pentru prelucrarea datelor acestora, precum și o cunoaștere integrală de către operatorii de date a implicațiilor noilor tehnologii asupra protecției datelor. Această problemă a fost parțial soluționată prin Directiva 2002/58/CE (așa-numita Directivă privind 'e-confidențialitatea')[5], care particularizează și completează Directiva generală privind protecția datelor în sectorul comunicațiilor electronice[6].

---

3 A se vedea răspunsurile la consultarea publică organizată de Comisie: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm. Pe parcursul anului 2010, au fost efectuate consultări pe teme mai specifice cu părțile interesate. Vicepreședintele Viviane Reding a condus, de asemenea, o reuniune la nivel înalt cu părțile interesate pe 5 octombrie 2010 în Bruxelles. Comisia s-a consultat, de asemenea, cu Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, care a furnizat o contribuție cuprinzătoare la consultarea din 2009 (WP 168) și a adoptat un aviz special în iulie 2010 cu privire la conceptul de *accountability* (WP 173).

4 În plus față de *Study on the economic benefits of privacy enhancing technologies* (citată la nota de subsol 2) a se vedea, de asemenea, *Comparative study on different approaches to new privacy challenges*, *in particular in the light of technological developments* (Studiu comparativ privind diversele abordări ale noilor provocări legate de confidențialitate, în special în lumina noilor dezvoltări tehnologice), ianuarie 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Este, de asemenea, în curs de elaborare, un studiu pentru o evaluare a impactului necesară cadrului juridic viitor al UE pentru protecția datelor cu caracter personal.

5 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37) .

6 Directiva 95/46/CE privind protecția datelor stabilește standardele de protecție a datelor pentru toate actele legislative ale UE, inclusiv pentru Directiva 2002/58/CE privind e-confidențialitatea (modificată prin Directiva 2009/136/CE - JO L 337, 18.12.2009, p.11). Directiva privind e-confidențialitatea se aplică prelucrării datelor cu caracter personal legate de furnizarea de servicii de comunicații electronice

- *Consolidarea dimensiunii privind piața internă a protecției datelor*

Una din principalele probleme recurente ridicate de părțile interesate, în special societăți multinaționale, o reprezintă inexistența unei suficiente armonizări a legislațiilor statelor membre referitoare la protecția datelor, în ciuda unui cadru juridic comun al UE. Acestea au subliniat necesitatea creșterii certitudinii juridice, reducerii sarcinii administrative și asigurării de condiții de concurență echitabile pentru operatorii economici și alți operatori de date.

- *Abordarea globalizării și îmbunătățirea transferurilor internaționale de date*

Mai multe părți interesate au subliniat faptul că externalizarea din ce în ce mai frecventă a prelucrării, deseori în afara UE, ridică numeroase probleme în ceea ce privește legislația aplicabilă prelucrării și alocarea responsabilității asociate. În ceea ce privește transferul internațional de date, mai multe organizații au considerat că sistemele actuale nu sunt pe deplin satisfăcătoare și este necesară revizuirea și raționalizarea acestora astfel încât transferurile să fie mai simple și să implice mai puține demersuri.

- *Asigurarea unor înțelegeri mai puternice la nivel instituțional în vederea unei aplicări efective a normelor de protecție a datelor*

Există un consens printre părțile interesate conform căruia rolul autorităților de protecție a datelor trebuie să fie întărit pentru a asigura o mai bună aplicare a normelor de protecție a datelor. Unele organizații au cerut, de asemenea, o creștere a transparenței în ceea ce privește activitatea Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal (*a se vedea punctul 2.5 de mai jos*) și o clarificare a atribuțiilor și competențelor acestuia.

- *Îmbunătățirea coerenței cadrului juridic privind protecția datelor*

În cadrul consultărilor, toate părțile interesate au subliniat necesitatea existenței unui instrument global care să se aplice operațiunilor de prelucrare a datelor în toate sectoarele și politicile Uniunii, asigurându-se o abordare integrată, precum și o protecție permanentă, coerentă și eficace[7].

Provocările prezentate mai sus **impun dezvoltarea unei abordări globale și coerente de către UE**, care să garanteze **respectarea deplină în UE și în afara acesteia a dreptului fundamental al persoanelor la protecția datelor**. Tratatul de la Lisabona a asigurat Uniunii Europene mijloace suplimentare de realizare a acestui obiectiv: Carta drepturilor fundamentale a Uniunii Europene – al cărei articol 8 recunoaște dreptul autonom la protecția datelor cu caracter personal – a devenit obligatorie din punct de vedere juridic și a fost introdus un nou temei juridic[8] care permite adoptarea unei legislații cuprinzătoare și coerente a Uniunii referitoare la protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ale acestora și libera circulație a unor astfel de date. În special, noul temei juridic îi

---

puse la dispoziția publicului prin intermediul rețelelor publice de comunicații electronice. Aceasta transpune principiile stabilite în directiva privind protecția datelor în norme specifice pentru sectorul comunicațiilor electronice. Directiva 95/46/CE se aplică, printre altele, și serviciilor de telecomunicații care nu sunt publice.

7 În contribuții separate făcute după terminarea consultării publice, Europol și Eurojust au susținut, cu toate acestea, să se țină cont de specificul activității acestora în ceea ce privește coordonarea aplicării legii și prevenirea infracțiunilor.

8 A se vedea articolul 16 din Tratatul privind funcționarea Uniunii Europene (TFUE).

permite UE să dispună de un instrument juridic unic pentru reglementarea protecției datelor, inclusiv domeniile cooperării polițienești și judiciare în materie penală. Domeniul politicii externe și de securitate comune este doar parțial acoperit de articolul 16 din TFUE întrucât normele specifice privind prelucrarea datelor de către statele membre trebuie să fie stabilite printr-o decizie a Consiliului, în baza unui temei juridic diferit[9].

Pornind de la aceste noi posibilități juridice, Comisia va acorda cea mai mare prioritate asigurării respectării dreptului fundamental la protecția datelor în întreaga Uniune și în toate politicile acesteia, consolidând în același timp dimensiunea privind piața internă și facilitând libera circulație a datelor cu caracter personal. În acest context, în asigurarea dreptului fundamental la protecția datelor cu caracter personal, trebuie să se țină seama, pe deplin, de alte drepturi fundamentale relevante consacrate în cartă și de alte obiective din tratate.

Prezenta comunicare își propune să definească abordarea care îi va permite Comisiei să modernizeze sistemul juridic pentru protecția datelor cu caracter personal al UE în toate domeniile de activitate ale Uniunii, ținându-se seama, în special, de provocările pe care le ridică globalizarea și noile tehnologii, pentru a se garanta în continuare un nivel înalt de protecție a persoanelor în ceea ce privește prelucrarea datelor cu caracter personal în toate domeniile de activitate ale Uniunii. Aceasta va permite UE să reprezinte în continuare o forță motrice în promovarea unor standarde înalte de protecție a datelor în întreaga lume.

2. OBIECTIVE CHEIE ALE ABORDĂRII GLOBALE A PROTECȚIEI DATELOR

2.1. Consolidarea drepturilor persoanelor

2.1.1. Asigurarea unei protecții corespunzătoare a persoanelor în toate circumstanțele

Obiectivul normelor din instrumentele actuale ale UE de protecție a datelor este de **a proteja drepturile fundamentale ale persoanelor fizice și în special dreptul acestora la protecția datelor cu caracter personal**, conform Cartei drepturilor fundamentale a Uniunii Europene[10].

Conceptul de 'date cu caracter personal' este unul din conceptele-cheie ale protecției persoanelor prin instrumentele actuale ale UE de protecție a datelor și implică aplicarea obligațiilor care incumbă operatorului de date și persoanei împuternicite de către operatorul de date[11]. Definiția 'datelor cu caracter personal' urmărește să acopere toate informațiile referitoare la o persoană identificată sau identificabilă în mod direct sau indirect. Pentru a determina dacă o persoană este identificabilă, trebuie să se ia în considerare 'toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată'[12]. Această abordare deliberată aleasă de legislator prezintă

---

9 A se vedea articolul 16 alineatul (2) ultimul paragraf din TFUE și articolul 39 din Tratatul privind Uniunea Europeană (TUE).

10 A se vedea Curtea Europeană de Justiție, cauzele C-101/01, Bodil Lindqvist, Rec., 2003, p. I-1297, punctele (96) și (97), și C-275/06, Productores de Música de Espańa (Promusicae) / Telefónica de Espańa SAU, Rep., 2008, p. I-271. A se vedea, de asemenea, jurisprudența Curții Europene a Drepturilor Omului, de ex. în cauzele: S. and Marper / Regatul Unit, 4.12. 2008 (numere de înregistrare 30562/04 și 30566/04) și Rotaru / România, 4.5. 2000; nr. 28341/95, § 55, CEDO 2000-V.

11 A se vedea definițiile pentru 'operatorul de date' și 'persoana împuternicită de către operatorul de date' de la articolul 2 literele (d) și (e) din Directiva 95/46/CE.

12 A se vedea considerentul 26 din Directiva 95/46/CE.

avantajul flexibilității prin faptul că permite aplicarea la situații și demersuri diverse care afectează drepturile fundamentale, inclusiv la acelea care nu puteau fi prevăzute la momentul adoptării directivei. Cu toate acestea, o consecință a unei astfel de abordări deschise și flexibile este faptul că există numeroase cazuri în care nu este întotdeauna clar, atunci când se aplică directiva, ce abordare trebuie aleasă și dacă persoanele beneficiază de drepturi de protecție a datelor și dacă operatorii de date ar trebui să respecte obligațiile impuse de directivă[13].

Există situații care presupun prelucrarea unor informații specifice care ar necesita măsuri suplimentare în temeiul dreptului Uniunii. Astfel de măsuri există deja în unele cazuri. De exemplu, stocarea de informații în dispozitive terminale (de exemplu telefoanele mobile) este permisă doar cu condiția ca persoana să își fi dat consimțământul. Poate că și acest aspect ar trebui să fie abordat la nivelul UE în ceea ce privește, de exemplu, datele codate cu cheie, datele de localizare, tehnologiile de 'extragere de date' care permit combinarea unor date provenind din diferite surse, sau cazurile în care trebuie să fie asigurată confidențialitatea și integritatea sistemelor de tehnologie a informațiilor[14].

Toate aspectele de mai sus necesită, prin urmare, o analiză atentă.

Comisia va avea în vedere **modul în care să asigure o aplicare coerentă a normelor de protecție a datelor, ținând seama de impactul noilor tehnologii asupra drepturilor și libertăților persoanelor și de obiectivul asigurării liberei circulații a datelor cu caracter personal în cadrul pieței interne.**

2.1.2. Creșterea transparenței pentru persoanele vizate

Transparența reprezintă o condiție fundamentală pentru a permite exercitarea de către persoane a controlului asupra datelor proprii și pentru a asigura o protecție efectivă a datelor cu caracter personal. Prin urmare, este esențial ca persoanele să fie **bine și clar informate și în mod transparent**, de către operatorii de date cu privire la modul în care și de către cine sunt colectate și prelucrate datele lor, din ce motive, pentru cât timp și care sunt drepturile acestora dacă doresc să acceseze, să rectifice sau să își șteargă datele. Dispozițiile relevante cu privire la informațiile care trebuie să fie furnizate persoanelor vizate[15] nu sunt suficiente.

Elementele de bază ale transparenței sunt cerințele potrivit cărora **informațiile trebuie să fie ușor de accesat și ușor de înțeles, și să fie folosit un limbaj simplu și clar.** Acesta este relevant în mod special în mediul electronic, unde destul de multe ori, declarațiile de confidențialitate sunt neclare, dificil de accesat, netransparente[16] și nu respectă întotdeauna normele existente. Un caz în care este probabil să se întâmple acest lucru îl reprezintă publicitatea comportamentală online în care atât multitudinea de actori implicați în furnizarea de publicitate comportamentală, cât și complexitatea, din punct de vedere tehnologic, a

---

13 A se vedea, de exemplu, cazul adreselor IP, analizat în Avizul 4/2007 referitor la conceptul de date cu caracter personal al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal (WP 136).

14 A se vedea, de exemplu, hotărârea Curții Federale Constituționale a Germaniei *(Bundesverfassungsgericht)* din 27 februarie 2008, 1 BvR 370/07.

15 A se vedea articolele 10 și 11 din Directiva 95/46/CE.

16 Un sondaj Eurobarometru efectuat în 2009 a indicat că aproximativ jumătate din respondenți au apreciat declarațiile de confidențialitate de pe pagini internet ca fiind 'foarte neclare' sau 'destul de neclare' (a se vedea Eurobarometru Flash nr. 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

practicii fac să fie dificil pentru o persoană să știe și să înțeleagă dacă sunt colectate date cu caracter personal, de către cine și în ce scop.

În acest context **copiii** au nevoie de o protecție specifică întrucât aceștia ar putea să cunoască mai puțin riscurile, consecințele, măsurile de protecție și drepturile legate de prelucrarea datelor cu caracter personal[17].

Comisia va avea în vedere:

- introducerea în cadrul juridic a unui **principiu general de prelucrare transparentă** a datelor cu caracter personal;

- introducerea unor **obligații specifice** pentru operatorii de date cu privire la tipul informațiilor care să fie furnizate și cu privire la **modalitățile** de furnizare a acestora, inclusiv în ceea ce privește **copiii;**

- stabilirea unuia sau a mai multor **formulare standard ale UE** ('**declarații de confidențialitate**') care să fie utilizate de către operatorii de date.

Este, de asemenea, important ca persoanele să fie informate atunci când datele lor sunt, în mod accidental sau ilegal, distruse, pierdute, modificate, accesate de către persoane neautorizate sau divulgate acestora. Revizuirea recentă a Directivei privind e-confidențialitatea electronice a introdus o **notificare obligatorie privind violarea datelor cu caracter personal** care acoperă, cu toate acestea, doar sectorul telecomunicațiilor. Dat fiind că riscul violării datelor există și în alte sectoare (de exemplu sectorul financiar), Comisia va analiza modalitățile de extindere a obligației notificării violării datelor cu caracter personal la alte sectoare, în conformitate cu declarația Comisiei privind notificarea violării datelor făcută în fața Parlamentului European în 2009, în contextul reformei cadrului de reglementare pentru comunicațiile electronice[18]. Această analiză nu va afecta dispozițiile Directivei e-confidențialității, care trebuie să fie transpusă în dreptul național până la 25 mai 2011[19]. Va trebui să se asigure o abordare consistentă și coerentă a acestei chestiuni.

Comisia intenționează:

- să analizeze modalitățile de introducere în cadrul juridic general a unei **notificări generale în cazul violării datelor cu caracter personal**, care să includă destinatarii unor astfel de notificări și criteriile în baza cărora se stabilește obligația de notificare.

---

17 A se vedea studiul calitativ *Safer Internet for Children* (Internet mai sigur pentru copii) referitor la copiii cu vârste cuprinse între 9-10 ani și 12-14 ani, care a indicat tendința acestora de a subaprecia riscurile legate de utilizarea internetului și de a minimaliza consecințele comportamentului lor riscant (disponibil la: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 'Comisia ia act de dorința Parlamentului European ca obligația de notificare a încălcării securității datelor cu caracter personal să nu se limiteze la sectorul comunicațiilor electronice, ci să se aplice și unor entități precum furnizorii de servicii ale societății informaționale […]. Prin urmare, Comisia va iniția în mod neîntârziat lucrările pregătitoare adecvate, inclusiv consultarea cu părțile interesate, în vederea prezentării de propuneri în acest domeniu, după caz, până la sfârșitul anului 2011[…]', se poate obține la http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//RO. A se vedea, de asemenea, considerentul 59 din Directiva 2009/136 CE de modificare a Directivei 2002/58/CE privind e-confidențialitatea: 'Este clar că interesul cetățenilor de a fi informați nu se limitează la sectorul comunicațiilor electronice și prin urmare ar trebui introduse cu prioritate la nivel comunitar cerințe obligatorii explicite de notificare aplicabile în toate sectoarele'.

19 Articolul 4 din Directiva 2009/136/CE.

2.1.3. Întărirea controlului asupra propriilor date

Două precondiții importante pentru a se asigura că persoanele beneficiază de un nivel înalt de protecție a datelor sunt **limitarea prelucrării de către operatorii de date la scopurile acesteia (principiul reducerii la minimum a datelor** și păstrarea de către persoanele vizate a unui **control efectiv asupra propriilor lor date**. Articolul 8 alineatul (2) din cartă prevede că 'orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora'. Persoanele ar trebui întotdeauna să poată accesa, rectifica, șterge sau bloca datele proprii, doar dacă nu există motive legitime, în baza legii, de împiedicare a acestui lucru. Aceste drepturi există deja în cadrul juridic actual. Cu toate acestea, modul în care aceste drepturi pot fi exercitate nu este armonizat și, prin urmare, exercitarea acestora este de fapt mai ușoară în unele state membre față de altele. În plus, această chestiune ridică probleme deosebit de mari în mediul electronic unde datele sunt deseori reținute fără ca persoana în cauză să fie informată și/sau să își fi dat consimțământul.

Exemplul rețelelor de socializare online este deosebit de relevant în acest caz întrucât ridică probleme semnificative în ceea ce privește controlul efectiv al persoanei asupra datelor sale cu caracter personal. Comisia a primit diverse întrebări de la persoane care nu au putut întotdeauna să retragă date cu caracter personal de la furnizorii de servicii online, cum ar fi fotografiile lor, și care au fost, prin urmare, împiedicați să își exercite drepturile de acces, rectificare și ștergere.

Astfel de drepturi ar trebui, prin urmare, să fie mai explicite, clarificate și, dacă este posibil, consolidate.

Comisia va analiza, prin urmare, căile prin care:

- să consolideze **principiul reducerii la minimum a datelor**:

- **să îmbunătățească modalitățile de exercitare** efectivă **a drepturilor de acces, rectificare, ștergere sau blocare a datelor** (de ex. prin introducerea de termene de răspuns la solicitările persoanelor, prin posibilitatea exercitării drepturilor prin mijloace electronice sau prin asigurarea gratuității dreptului de acces, ca principiu);

- să clarifice așa-numitul '**drept de a fi uitat**', și anume dreptul persoanelor de a nu mai avea datele prelucrate ci șterse atunci când nu mai sunt necesare în scopuri legitime. Acesta este cazul, de exemplu, când prelucrarea se bazează pe consimțământul persoanei și atunci când aceasta își retrage consimțământul sau când perioada de stocare a expirat;

- să completeze drepturile persoanelor vizate prin asigurarea '**portabilității datelor**', și anume, prin acordarea dreptului explicit unei persoane de a-și retrage datele proprii (de ex. fotografiile acesteia, sau o listă cu prieteni) de pe o aplicație sau un serviciu, astfel încât datele retrase să poată fi transferate într-o altă aplicație sau serviciu, în măsura în care acest lucru este fezabil din punct de vedere tehnic, fără piedici din partea operatorilor de date.

2.1.4. Creșterea nivelului de sensibilizare

Pe lângă transparența care este esențială, este necesar, de asemenea, ca publicul general, și cu precădere tinerii, să fie mai sensibilizați cu privire la riscurile legate de prelucrarea datelor cu caracter personal și cu privire la drepturile lor. Un sondaj Eurobarometru din 2008 a indicat că o mare parte a persoanelor din statele membre UE consideră că nivelul de sensibilizare cu

privire la protecția datelor personale din țara lor este scăzut[20]. Activitățile de sensibilizare ar trebui deci să fie încurajate și promovate de o serie largă de actori, și anume autoritățile statelor membre, în special autoritățile în domeniul protecției datelor și organismele educaționale, precum și operatorii de date și asociațiile societății civile. Acestea ar trebui să includă măsuri care nu au caracter legislativ precum campanii de sensibilizare în mijloacele de comunicare tipărite și electronice și furnizarea de informații clare pe site-urile internet, care prezintă în mod clar drepturile persoanelor vizate și responsabilitățile operatorilor de date.

Comisia va analiza:

- posibilitatea **cofinanțării unor activități de creștere a nivelului de sensibilizare cu privire la protecția datelor** din bugetul Uniunii;

- necesitatea și oportunitatea includerii în cadrul juridic a **unei obligații privind efectuarea de activități de creștere a nivelului de sensibilizare** în acest domeniu.

2.1.5. Asigurarea unui consimțământ în cunoștință de cauză și liber

Atunci când este necesar consimțământul în cunoștință de cauză, normele curente prevăd că, pentru prelucrarea datelor cu caracter personal, consimțământul persoanei respective ar trebui să fie o 'manifestare de voință, liberă, specifică și informată', prin care persoana își face cunoscut acordul privind prelucrarea datelor sale[21]. Dar aceste condiții sunt în prezent interpretate în mod diferit în statele membre, variind de la obligația generală a existenței consimțământului în scris, până la acceptarea consimțământului implicit.

Mai mult, în mediul electronic – din cauza opacității politicilor de confidențialitate – adeseori este mai dificil pentru persoane să își cunoască drepturile și să dea un consimțământ în cunoștință de cauză. Acest lucru este chiar și mai complicat de faptul că, în unele cazuri, nu este nici măcar clar ce ar însemna un consimțământ liber, specific și în cunoștință de cauză acordat pentru prelucrarea datelor, cum ar fi în cazul publicității comportamentale, în care setările browser-ului internet, se consideră de către unii, dar nu și de către alții, exprimă consimțământul utilizatorului.

Prin urmare ar trebui furnizate clarificări cu privire la condițiile consimțământului persoanei vizate, pentru a se garanta întotdeauna un consimțământ în cunoștință de cauză și a se asigura că persoana cunoaște foarte bine faptul că își dă consimțământul, și pentru ce fel de prelucrare a datelor, conform articolului 8 din Carta drepturilor fundamentale a Uniunii Europene. Claritatea conceptelor-cheie poate favoriza, de asemenea, dezvoltarea unor inițiative de autoreglementare în vederea găsirii unor soluții practice conforme cu dreptul UE.

Comisia va avea în vedere modalități de **clarificare și întărire a normelor privind consimțământul**.

2.1.6. Protejarea datelor sensibile

Prelucrarea datelor sensibile, și anume datele care dezvăluie originea rasială sau etnică, opiniile politice, credințele religioase sau filosofice, apartenența sindicală, precum și

[20] A se vedea Eurobarometru Flash nr. 225 – protecția datelor în Uniunea Europeană: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Cf. articolul 2, litera (h) din Directiva 95/46/CE.

prelucrarea datelor privind sănătatea sau viața sexuală, sunt la ora actuală deja interzise, ca regulă generală, cu excepții în număr limitat, în anumite condiții și cu garanții suplimentare[22]. Cu toate acestea, având în vedere evoluțiile tehnologice și de alt tip la nivelul societății, este necesar să se revizuiască prevederile existente cu privire la datele sensibile, să se analizeze dacă ar trebui adăugate alte categorii de date și să se clarifice în continuare condițiile prelucrării acestora. Acest lucru este valabil, de exemplu, pentru datele genetice care, în prezent, nu sunt menționate explicit ca fiind o categorie sensibilă de date.

Comisia va avea în vedere:

- dacă alte categorii de date ar trebui să fie considerate ca fiind **'date sensibile'**, de exemplu datele **genetice;**

- clarificarea și **armonizarea în continuare a condițiilor** care permit prelucrarea categoriilor de date sensibile.

2.1.7. Sporirea eficacității căilor de atac și a sancțiunilor

Pentru a asigura aplicarea normelor de protecție a datelor, existența unor **dispoziții eficace privind remedierile și sancțiunile** este esențială. Sunt numeroase cazurile în care încălcarea normelor de protecție a datelor în detrimentul unei persoane afectează, de asemenea, un număr considerabil de alte persoane aflate într-o situație similară.

În consecință, Comisia:

- va avea în vedere posibilitatea **extinderii competenței de a aduce o acțiune înaintea instanțelor naționale** la autoritățile de protecție a datelor și la asociațiile societății civile, precum și la **alte asociații care reprezintă interesele persoanelor vizate**;

- va evalua necesitatea consolidării dispozițiilor existente în materie de sancțiuni, de exemplu prin includerea explicită a sancțiunilor penale în cazul violării grave a protecției datelor, pentru a le face mai eficace.

2.2. Consolidarea dimensiunii privind piața internă

2.2.1. Creșterea certitudinii juridice și asigurarea unor condiții de concurență echitabile pentru operatorii de date

Protecția datelor în UE are o **puternică dimensiune privind piața internă**, și anume necesitatea asigurării circulației libere a datelor cu caracter personal între statele membre în cadrul pieței interne. În consecință, armonizarea legislațiilor naționale privind protecția datelor prevăzută în directivă nu se limitează la o armonizare minimă, ci se îndreaptă către o armonizare care este, în general, completă[23].

În același timp, directiva oferă statelor membre o marjă de acțiune în anumite domenii și le autorizează să mențină sau să introducă norme speciale pentru situații specifice[24]. Acest lucru, la care se adaugă faptul că directiva a fost uneori incorect pusă în aplicare de către statele membre, a condus la **divergențe între legile naționale de punere în aplicare a directivei, care contravin unuia dintre obiectivele principale ale acesteia, și anume asigurarea**

22 Cf. articolul 8 din Directiva 95/46/CE.

23 Curtea Europeană de Justiție, C-101/01, Bodil Lindqvist, Rec., 2003, p. I-1297, punctele (96), și (97).

24 *Ibidem*, 97. A se vedea, de asemenea, considerentul 9 din Directiva 95/46/CE:

liberei circulații a datelor cu caracter personal în cadrul pieței interne. Acest lucru este valabil pentru un număr mare de sectoare și contexte, de ex. prelucrarea datelor în contextul ocupării unui loc de muncă sau din motive legate de sănătatea publică. Lipsa armonizării, reprezintă, într-adevăr, una din principalele probleme recurente ridicate de părțile interesate din sectorul privat, în special operatorii economici, întrucât, pentru ei, aceasta înseamnă costuri și sarcini administrative suplimentare. Acesta este cazul, în special, al operatorilor de date stabiliți în mai multe state membre și care sunt obligați să respecte cerințele și practicile din fiecare din aceste țări. Mai mult, divergențele în punerea în aplicare a directivei de către statele membre creează incertitudine juridică nu doar pentru operatorii de date, dar și pentru persoanele vizate, conducând la denaturarea nivelului echivalent de protecție pe care se presupune că directiva trebuie să îl obțină și să îl asigure.

Comisia va analiza mijloacele de **armonizare, în continuare, a normelor de protecție a datelor la nivelul UE.**

2.2.2. Reducerea sarcinii administrative

Asigurarea unor condiții de concurență echitabile va reduce nevoia de a răspunde cerințelor naționale divergente și astfel va reduce considerabil sarcina administrativă care revine operatorilor. Un alt element concret pentru ușurarea sarcinii administrative și reducerea costurilor pentru operatorii de date ar fi **revizuirea și simplificarea sistemului actual de notificare**[25]**.** Există un consens general la nivelul operatorilor de date potrivit căruia obligația generală actuală de notificare a tuturor operațiunilor de prelucrare a datelor către autoritățile de protecția datelor este mai degrabă o obligație greoaie care nu aduce, prin sine, nicio valoare adăugată reală în ceea ce privește protecția datelor cu caracter personal ale persoanelor. Mai mult, acesta este unul din cazurile în care directiva lasă o anumită posibilitate de acțiune statelor membre, care sunt libere să decidă asupra unor posibile excepții și simplificări, precum și asupra procedurii care trebuie urmată.

Un sistem armonizat și simplificat ar reduce costurile precum și sarcina administrativă, în special pentru societățile multinaționale stabilite în mai multe state membre.

Comisia va analiza diferite posibilități în vederea **simplificării și armonizării sistemului actual de notificare**, inclusiv posibilitatea întocmirii unui **formular de înregistrare uniform în întreaga UE.**

2.2.3. Clarificarea normelor privind dreptul aplicabil și responsabilitatea statelor membre

Încă din 2003, primul raport al Comisiei referitor la punerea în aplicare a Directivei privind protecția datelor[26] sublinia că dispozițiile privind dreptul aplicabil[27] au fost „deficitare în mai multe cazuri, rezultatul fiind posibila apariție a tipului de conflicte de legi pe care acest articol încearcă să îl evite". Situația nu s-a îmbunătățit de atunci și, ca urmare, nu este întotdeauna clar pentru operatorii de date și pentru autoritățile de supraveghere a protecției datelor care este statul membru responsabil și care este dreptul aplicabil atunci când sunt implicate mai multe state membre. Acesta este cazul, în special, atunci când un operator de date primește cereri diferite din partea unor state membre diferite, atunci când o întreprindere multinațională

---

25 A se vedea articolul 18 din Directiva 95/46/CE.

26 Raport al Comisiei - Primul raport referitor la punerea în aplicare a Directivei privind protecția datelor (95/46/CE) - COM (2003) 265.

27 A se vedea articolul 4 din Directiva 95/46/CE.

își are sediul în mai multe state membre sau când operatorul de date nu este stabilit în UE, dar furnizează servicii rezidenților UE.

Complexitatea crește și datorită globalizării și evoluțiilor tehnologice: din ce în ce mai frecvent, operatorii de date își desfășoară activitatea în mai multe state membre și sub mai multe jurisdicții, furnizând servicii și asistență 24 de ore din 24. Internetul permite operatorilor de date stabiliți în afara Spațiului Economic European (SEE)[28] să furnizeze mai ușor servicii de la distanță și să prelucreze date cu caracter personal într-un mediu electronic și, adesea, este dificil să se localizeze datele cu caracter personal și să se stabilească ce echipament s-a utilizat la un moment dat (de exemplu, în aplicațiile și serviciile „*cloud computing*").

Cu toate acestea, Comisia consideră că, chiar dacă prelucrarea datelor cu caracter personal este efectuată de un operator de date stabilit într-o țară terță, acest fapt nu ar trebui să priveze persoanele de protecția la care au dreptul în temeiul Cartei drepturilor fundamentale a UE și a legislației UE în materie de protecție a datelor.

Comisia va analiza modul în care **dispozițiile existente privind dreptul aplicabil ar putea fi revizuite și clarificate**, inclusiv actualele criterii de stabilire a dreptului aplicabil, pentru a îmbunătăți securitatea juridică, a clarifica responsabilitatea statelor membre cu privire la aplicarea normelor de protecție a datelor și, în cele din urmă, pentru a furniza același grad de protecție tuturor persoanelor vizate din UE, indiferent de locul în care este stabilit operatorul de date.

2.2.4. Creșterea responsabilității operatorilor de date

Simplificarea administrativă **nu ar trebui să conducă la o reducere globală a responsabilității operatorului de date în ceea ce privește asigurarea unei protecții eficace a datelor**. Dimpotrivă, Comisia este de părere că obligațiile acestora ar trebui să fie stabilite mai clar în cadrul juridic, inclusiv în ceea ce privește mecanismele de control intern și cooperarea cu autoritățile de supraveghere a protecției datelor. În plus, ar trebui să se asigure că o astfel de responsabilitate se aplică și operatorilor care au obligația de a respecta secretul profesional (de exemplu, avocații), precum și în cazurile, din ce în ce mai frecvente, în care operatorii de date deleagă prelucrarea acestora altor entități (de exemplu, persoane împuternicite de către operatori).

Prin urmare, Comisia va analiza modalitățile de **a garanta că operatorii de date introduc politici și mecanisme eficace pentru a asigura conformitatea cu normele de protecție a datelor**. Acționând astfel, Comisia va lua în considerare actuala dezbatere privind eventuala introducere a conceptului de *accountability*[29]. Acesta nu ar duce la creșterea sarcinii administrative suportate de operatorii de date, întrucât astfel de măsuri ar viza, mai degrabă, instituirea de garanții și de mecanisme mai eficace de protecție a datelor, reducând și simplificând, totodată, anumite formalități administrative, cum ar fi notificările (*a se vedea secțiunea 2.2.2. de mai sus*).

Promovarea utilizării tehnologiilor de protecție a vieții private (*Privacy Enhancing Technologies* - PET), astfel cum s-a subliniat deja în comunicarea din 2007 a Comisiei pe

---

[28] Spațiul Economic European include Norvegia, Liechtenstein și Islanda.

[29] A se vedea, în special, avizul nr. 3/2010 adoptat de Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal la 13 iulie 2010.

această temă, precum și principiul „luării în considerare a vieții private începând cu momentul conceperii”, ar putea juca un rol important în această privință, inclusiv în asigurarea securității datelor[30].

Comisia va analiza următoarele elemente pentru creșterea responsabilității operatorilor de date:

- introducerea obligației de a desemna un **responsabil cu protecția datelor** independent și armonizarea normelor referitoare la sarcinile și competențele operatorilor de date[31], reflectând, totodată, asupra stabilirii unui prag corespunzător pentru evitarea sarcinilor administrative nejustificate, în special asupra întreprinderilor mici și mijlocii;
- includerea în cadrul juridic a obligației pentru operatorii de date de a efectua o **evaluare a impactului asupra protecției datelor** în anumite cazuri, de exemplu, atunci când sunt prelucrate date sensibile sau atunci când tipul de prelucrare implică alte riscuri specifice, în special atunci când se utilizează tehnologii, mecanisme sau proceduri specifice, inclusiv stabilirea unui profil și supravegherea video;
- promovarea în continuare a utilizării PET și posibilitățile de punere concretă în aplicare a conceptului de „**luare în considerare a vieții private începând cu momentul conceperii**”.

2.2.5. Încurajarea inițiativelor de autoreglementare și analizarea posibilității de a introduce scheme de certificare la nivelul UE

Comisia continuă să considere că **inițiativele de autoreglementare** luate de operatorii de date pot **contribui la o mai bună aplicare a normelor de protecție a datelor.** Actualele dispoziții în materie de autoreglementare din Directiva privind protecția datelor, și anume posibilitatea de a elabora coduri de conduită[32], au fost rar aplicate până în prezent și nu sunt considerate satisfăcătoare de către părțile interesate din sectorul privat.

În plus, Comisia va analiza posibilitatea de a crea **scheme de certificare** la nivelul UE (**de exemplu, „mărci de protecție a vieții private”**) pentru procese, tehnologii, produse și servicii „care respectă viața privată”[33]. Acestea nu numai că ar orienta persoanele care utilizează astfel de tehnologii, produse și servicii, ci și ar avea un rol în ceea ce privește responsabilitatea operatorilor de date: alegerea unor tehnologii, produse sau servicii certificate ar putea contribui la dovedirea faptului că operatorul și-a îndeplinit obligațiile care îi revin (*a se vedea secțiunea 2.2.4. de mai sus*). Bineînțeles, un element esențial ar fi **asigurarea**

---

30 Cu privire la PET, a se vedea: Comunicare a Comisiei către Parlamentul European și către Consiliu privind promovarea protecției datelor prin intermediul tehnologiilor de protecție a vieții private (*Privacy Enhancing Technologies* - PET) - COM(2007) 228. Principiul „luării în considerare a vieții private începând cu momentul conceperii” înseamnă că protecția vieții private și a datelor cu caracter personal fac parte integrantă din întregul ciclu de viață al acestor tehnologii, din momentul proiectării, până în momentul implementării, utilizării și eliminării lor definitive. Acest principiu se regăsește*, inter alia*, în Comunicarea Comisiei privind „O Agendă digitală pentru Europa” - COM(2010) 245.

31 Actuala posibilitate ca un operator de date să desemneze un responsabil cu protecția datelor pentru a asigura, în mod independent, conformitatea cu normele UE și cu normele naționale de protecție a datelor și pentru a ajuta persoanele în cauză, a fost deja utilizată în mai multe state membre [a se vedea, de exemplu, *Beauftragter für den Datenschutz* în Germania și *correspondant informatique et libertés* (CIL) în Franța].

32 A se vedea articolul 27 din Directiva 95/46/CE.

33 Cu privire la acest aspect, a se vedea și Comunicarea privind PET, citată la nota de subsol nr. 30.

fiabilității unor astfel de mărci de protecție a vieții private, precum și compatibilitatea acestora cu obligațiile legale și standardele tehnice internaționale.

Comisia intenționează:

- să examineze modalitățile de **a încuraja în continuare inițiativele de autoreglementare**, inclusiv promovarea activă a codurilor de conduită;

- să analizeze posibilitatea introducerii unor **scheme de certificare la nivelul UE** în domeniul protecției vieții private și al protecției datelor.

2.3. Revizuirea normelor de protecție a datelor în domeniul cooperării polițienești și judiciare în materie penală

Directiva privind protecția datelor se aplică tuturor activităților de prelucrare a datelor cu caracter personal în statele membre, atât în sectorul public, cât și în cel privat. Cu toate acestea, directiva nu se aplică prelucrării datelor cu caracter personal „puse în practică pentru exercitarea activităților din afara domeniului de aplicare a dreptului comunitar", cum ar fi activitățile în domeniile cooperării polițienești și judiciare în materie penală[34]. Cu toate acestea, Tratatul de la Lisabona a eliminat vechea „structură bazată pe piloni" a UE și a introdus un temei juridic nou și cuprinzător pentru protecția datelor cu caracter personal în cadrul tuturor politicilor Uniunii[35]. În acest context, și având în vedere Carta drepturilor fundamentale a UE, comunicările Comisiei privind Programul de la Stockholm și Planul de acțiune de la Stockholm[36] au evidențiat necesitatea de a institui un „regim complet de protecție" și „de a întări poziția UE cu privire la protecția datelor cu caracter personal ale persoanelor în contextul tuturor politicilor UE, inclusiv în contextul aplicării legii și al prevenirii criminalității".

Instrumentul UE pentru asigurarea protecției datelor cu caracter personal în domeniile cooperării polițienești și judiciare în materie penală este **Decizia-cadru 2008/977/JAI**[37]. Aceasta reprezintă un progres important într-un domeniu în care standardele comune pentru protecția datele erau foarte necesare. Cu toate acestea, mai sunt multe de făcut.

Decizia-cadru se aplică numai schimbului transfrontalier de date cu caracter personal în interiorul UE și nu vizează operațiunile interne de prelucrare a datelor efectuate în statele membre. Această distincție este greu de făcut în practică și poate complica actuala punere în aplicare a deciziei-cadru[38].

De asemenea, **decizia-cadru prevede o derogare prea largă de la principiul limitării scopului**. O altă carență este absența dispozițiilor conform cărora ar trebui să se facă distincție

---

34 A se vedea articolul 3 alineatul (2) prima liniuță din Directiva 95/46/CE.

35 A se vedea articolul 16 din TFUE.

36 A se vedea COM(2009) 262, 10.6.2009 și COM(2010) 171, 20.4.2010.

37 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). Decizia-cadru are în vedere doar o armonizare minimă a standardelor de protecție a datelor.

38 Această distincție nu există în cadrul instrumentelor relevante ale Consiliului Europei, cum ar fi: Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (seria tratatelor Consiliului Europei nr. 108) și protocolul adițional la aceasta cu privire la autoritățile de supraveghere și fluxul transfrontalier al datelor (seria tratatelor Consiliului Europei nr. 181) și Recomandarea nr. R (87) 15 a Comitetului de Miniștri către statele membre de reglementare a utilizării datelor cu caracter personal în sectorul polițienesc, adoptată la 17 septembrie 1987.

între diferitele categorii de date, în funcție de gradul lor de acuratețe și de fiabilitate; de asemenea, ar trebui să se facă distincție între datele bazate pe fapte și datele bazate pe opinii sau evaluări personale[39], precum și între diferitele categorii de persoane vizate (infractori, suspecți, victime, martori etc.), prevăzându-se garanții specifice pentru datele care se referă la persoane care nu sunt suspectate[40].

În plus, **Decizia-cadru nu înlocuiește diferitele instrumente legislative de natură sectorială care au fost adoptate la nivelul UE în domeniile cooperării polițienești și judiciare în materie penală**[41], în special cele care reglementează funcționarea Europol, Eurojust, Sistemului de Informații Schengen (SIS) și Sistemului de informații al vămilor (CIS)[42], care fie prevăd regimuri speciale de protecție a datelor, fie se referă în general la instrumente de protecție a datelor ale Consiliului Europei. În ceea ce privește activitățile din domeniul cooperării polițienești și judiciare, toate statele membre au aderat la Recomandarea nr. R (87) 15 a Consiliului Europei, care stabilește principiile Convenției 108 în sectorul polițienesc. Cu toate acestea, recomandarea respectivă nu este un instrument obligatoriu din punct de vedere juridic.

Această situație poate aduce atingere în mod direct posibilităților persoanelor de a-și exercita drepturile în materie de protecție a datelor în acest domeniu (de exemplu, de a fi informați ce date cu caracter personal care îi privesc sunt prelucrate și fac obiectul unui schimb, precum și de către cine și în ce scop sunt acestea prelucrate; de a fi informați cu privire la modul de exercitare a acestor drepturi, cum ar fi dreptul de a avea acces la datele lor).

Obiectivul instituirii unui sistem global și coerent în UE și față de țări terțe **necesită luarea în considerare a revizuirii actualelor norme privind protecția datelor în domeniul cooperării polițienești și judiciare în materie penală**. Comisia subliniază că noțiunea de regim complet de protecție a datelor nu exclude adoptarea unor norme specifice pentru sectorul polițienesc și pentru cel judiciar în interiorul cadrului general, luând în considerare în mod corespunzător natura specifică a acestor domenii, astfel cum s-a arătat în Declarația 21, atașată la Tratatul de la Lisabona. Aceasta implică, de exemplu, necesitatea de a analiza în ce măsură exercitarea de către o persoană a anumitor drepturi în materie de protecție a datelor ar pune în pericol, într-un anumit caz, prevenirea, anchetarea, depistarea sau urmărirea penală și judecarea infracțiunilor, ori executarea pedepselor.

În special, Comisia:

- va lua în considerare oportunitatea **de a extinde aplicarea normelor generale de protecție a datelor în domeniile cooperării polițienești și judiciare în materie penală**, inclusiv în cazul prelucrării la nivel național, asigurând, totodată, după caz, **limitări** armonizate ale anumitor drepturi ale persoanelor în materie de protecție a datelor, de exemplu în ceea ce privește dreptul de acces sau principiul transparenței;

- va analiza necesitatea de a introduce **dispoziții specifice și armonizate** în noul cadru

---

39 Conform cerințelor principiului 3.2 din Recomandarea nr. R (87) 15.

40 Contrar principiului 2 din Recomandarea nr. R (87) 15 și rapoartelor sale de evaluare.

41 A se vedea prezentarea generală a acestor instrumente în Comunicarea Comisiei „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție" - COM(2010) 385.

42 Autoritățile comune de supraveghere au fost înființate în temeiul instrumentelor relevante pentru a asigura supravegherea protecției datelor, suplimentar competențelor de supraveghere generale pe care Autoritatea Europeană pentru Protecția Datelor (AEPD) le exercită asupra instituțiilor, organismelor și agențiilor Uniunii, în baza Regulamentului (CE) nr. 45/2001.

general de protecție a datelor, de exemplu în ceea ce privește prelucrarea **datelor genetice** în scopuri penale sau identificarea diferitelor categorii de persoane vizate (martori, suspecți etc.) în domeniul cooperării polițienești și judiciare în materie penală;

- va lansa, în 2011, o **consultare** a tuturor părților interesate vizate cu privire la cea mai bună modalitate de **revizuire a actualelor sisteme de supraveghere în domeniul cooperării polițienești și judiciare în materie penală**, în vederea asigurării unei supravegheri eficace și coerente a protecției datelor în toate instituțiile, organismele, birourile și agențiile Uniunii;

- va evalua necesitatea de a **alinia**, pe termen lung, **actualele norme diferite de natură sectorială, adoptate la nivelul UE în domeniul cooperării polițienești și judiciare în materie penală și conținute de instrumente specifice**, cu noul cadru juridic general de protecție a datelor.

2.4. Dimensiunea mondială a protecției datelor

2.4.1. Clarificarea și simplificarea normelor pentru transferurile internaționale de date

Înainte de a transfera date cu caracter personal în afara UE și a SEE, trebuie să se efectueze așa-numita **„evaluare a caracterului adecvat"**. În prezent, caracterul adecvat al unei țări terțe – și anume, dacă o țară terță asigură un nivelul de protecție pe care UE îl consideră drept adecvat – poate fi stabilit de Comisie și de statele membre.

Atunci când Comisia apreciază drept adecvat nivelul de protecție asigurat de o țară terță, datele cu caracter personal pot circula liber din cele 27 de state membre ale UE și din cele trei țări membre ale SEE către țara terță în cauză, fără a mai fi necesare alte garanții suplimentare. Cu toate acestea, în prezent, cerințele exacte care trebuie îndeplinite pentru recunoașterea de către Comisie a caracterului adecvat nu sunt precizate suficient de detaliat în Directiva privind protecția datelor. În plus, decizia-cadru nu prevede adoptarea unei astfel de decizii de către Comisie.

În unele state membre, caracterul adecvat este evaluat, într-o primă etapă, de operatorul de date care transferă datele cu caracter personal către o țară terță, uneori în cadrul unui control ex-post efectuat de autoritatea de supraveghere a protecției datelor. Această situație poate duce la abordări diferite în evaluarea caracterului adecvat al protecției asigurate de țările terțe, sau de organizațiile internaționale, și **implică riscul ca nivelul de protecție al persoanelor vizate prevăzut într-o țară terță să fie apreciat diferit de la un stat membru la altul**. De asemenea, actualele instrumente juridice nu conțin cerințe detaliate, armonizate în funcție de care transferurile să poată fi considerate legale. Astfel, practicile diferă de la un stat membru la altul.

În plus, în ceea ce privește transferurile de date către țări terțe care nu asigură un nivel adecvat de protecție, actualele clauze standard ale Comisiei pentru transferurile de date cu caracter personal către operatori[43] și persoane împuternicite de către operatori[44] nu sunt concepute

[43] Decizia 2001/497/CE a Comisiei din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE (JO L 181, 4.7.2001, p. 19); Decizia 2002/16/CE a Comisiei din 27 decembrie 2001 privind clauzele contractuale tip pentru transferul de date cu caracter personal către procesatorii de date stabiliți în țări terțe, în temeiul Directivei 95/46/CE (JO L 6, 10.1.2002, p. 52); Decizia 2004/915/CE a Comisiei din 27 decembrie 2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către țări terțe (JO L 385, 29.12.2004, p. 74).

pentru situații necontractuale și, de exemplu, nu pot fi utilizate în cazul transferurilor între administrațiile publice.

În plus, acordurile internaționale încheiate de UE sau de statele membre ale acesteia necesită, adesea, includerea principiilor de protecție a datelor și a unor dispoziții specifice. Aceasta poate avea drept rezultat texte diferite, care prevăd dispoziții și drepturi lipsite de coerență și care, prin urmare, pot fi interpretate în mod diferit, în detrimentul persoanelor vizate. În consecință, Comisia a anunțat că își va concentra activitatea asupra elementelor-cheie pentru protecția datelor cu caracter personal, pe care trebuie să le conțină acordurile încheiate între Uniune și țări terțe în scopul aplicării legii[45].

Alte modalități care au fost dezvoltate ca o formă de autoreglementare, cum ar fi coduri interne de conduită ale unor societăți, cunoscute sub numele de „reguli corporatiste obligatorii" (*Binding Corporate Rules* - BCR)[46], pot fi, de asemenea, un instrument util pentru a transfera în mod legal date cu caracter personal între societăți care fac parte din același grup. Cu toate acestea, părțile interesate au sugerat că acest mecanism ar putea fi îmbunătățit în continuare și punerea sa în aplicare ar putea fi facilitată.

Pentru soluționarea problemelor identificate, există **o necesitate generală de a îmbunătăți actualele mecanisme care permit efectuarea transferurilor internaționale de date cu caracter personal**, asigurând, totodată, un nivel corespunzător de protecție al acestor date în cazul în care sunt transferate și prelucrate în afara UE și a SEE.

Comisia intenționează să analizeze modalitățile de:

- îmbunătățire și raționalizare a actualelor proceduri pentru transferurile internaționale de date, inclusiv a instrumentelor obligatorii din punct de vedere juridic și a „regulilor corporatiste obligatorii", în vederea asigurării unei **abordări mai uniforme și mai coerente a UE** față de țări terțe și organizații internaționale;

- **clarificare a procedurii de evaluare de către Comisie a caracterului adecvat** și de precizare mai clară a **criteriilor și a cerințelor** în materie de evaluare a nivelului de protecție a datelor într-o țară terță sau în cadrul unei organizații internaționale;

- definire a **elementelor-cheie de protecție a datelor la nivelul UE**, care ar putea fi utilizate în cadrul tuturor tipurilor de acorduri internaționale.

2.4.2. Promovarea principiilor universale

Prelucrarea datelor are un caracter global și necesită elaborarea unor principii universale de protecție a persoanelor în ceea e privește prelucrarea datelor cu caracter personal.

---

44 Decizia Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către procesatorii de date stabiliți în țări terțe, în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului (JO L 39, 12.2.2010, p. 5).

45 Planul de acțiune de la Stockholm, citat la notat de subsol nr. 36.

46 „Regulile corporatiste obligatorii" sunt coduri de bune practici bazate pe standardele europene de protecție a datelor, pe care organizațiile multinaționale le stabilesc și le respectă în mod voluntar în scopul asigurării unor garanții corespunzătoare pentru transferurile sau categoriile de transferuri de date cu caracter personal între societăți care fac parte din același grup și care au obligații în temeiul acestor reguli corporatiste. A se vedea: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

Adesea, cadrul juridic al UE în materie a servit drept **reper pentru țările terțe în reglementarea protecției datelor**. Efectul și impactul acestuia, în interiorul și în afara Uniunii, au fost deosebit de importante. Prin urmare**, Uniunea Europeană trebuie să joace în continuare un rol activ în dezvoltarea și promovarea standardelor juridice și tehnice internaționale în materie de protecție a datelor cu caracter personal**, pe baza instrumentelor relevante ale UE și a altor instrumente europene privind protecția datelor. Acest aspect este deosebit de important în cadrul politicii de extindere a UE.

În ceea ce privește standardele tehnice internaționale dezvoltate de organizațiile de standardizare, Comisia consideră că asigurarea unei coerențe între viitorul cadru juridic și astfel de standarde este foarte importantă pentru garantarea unei puneri în aplicare coerente și efective a normelor de protecție a datelor de către operatorii de date.

Comisia intenționează:

- să promoveze în continuare **dezvoltarea unor standarde juridice și tehnice ridicate în materie de protecție a datelor** în țări terțe și la nivel internațional;

- să susțină **principiul reciprocității protecției** în acțiunile internaționale ale Uniunii și, în special, în ceea ce privește persoanele vizate ale căror date sunt transferate din UE către țări terțe;

- **să consolideze cooperarea sa, în acest scop, cu țări terțe și cu organizații internaționale**, cum ar fi OCDE, Consiliul Europei, Organizația Națiunilor Unite și alte organizații regionale;

- **să monitorizeze îndeaproape dezvoltarea standardelor tehnice internaționale de către organizațiile de standardizare**, cum ar fi Comitetul European de Standardizare (CEN) și Organizația Internațională de Standardizare (ISO), pentru a se asigura că acestea completează în mod util normele juridice și că cerințele-cheie de protecție a datelor sunt puse în aplicare în mod eficace la nivel operațional.

2.5. Consolidarea cadrului instituțional în vederea unei mai bune aplicări a normelor de protecție a datelor

Punerea în aplicare și asigurarea respectării principiilor și a normelor de protecție a datelor sunt elemente-cheie pentru a garanta respectarea drepturilor persoanelor.

În acest context, **rolul autorităților de protecție a datelor (APD) este esențial** pentru asigurarea respectării normelor privind protecția datelor. Aceste autorități sunt gardieni independenți ai drepturilor și libertăților fundamentale în materie de protecție a datelor cu caracter personal, pe care persoanele se bazează pentru asigurarea protecției datelor lor cu caracter personal și legalitatea operațiunilor de prelucrare a acestora. Din acest motiv, Comisia consideră că rolul autorităților de protecție a datelor ar trebui consolidat, în special luând în considerare jurisprudența recentă a CEJ privind independența lor[47] și că acestea ar trebui să dispună de competențele și de resursele necesare pentru a-și îndeplini în mod corespunzător sarcinile, atât la nivel național, cât și atunci când cooperează reciproc.

În același timp, Comisia consideră că **autoritățile de protecție a datelor ar trebui să își intensifice cooperarea și să își coordoneze mai bine activitățile**, în special atunci când se confruntă cu aspecte care, prin natura lor, au o dimensiune transfrontalieră. Acesta este cazul,

[47] Hotărârea CEJ din 9.3.2010, Comisia / Germania, cauza C-518/07.

în special, atunci când întreprinderi multinaționale au sediul în mai multe state membre și își desfășoară activitatea în fiecare dintre aceste țări sau atunci când este necesar să se efectueze o supraveghere coordonată împreună cu Autoritatea Europeană pentru Protecția Datelor (AEPD)[48].

În această privință, **un rol important poate reveni Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal**[49], care, suplimentar funcției sale consultative[50], are deja sarcina de a contribui la aplicarea uniformă la nivel național a normelor UE de protecție a datelor. Cu toate acestea, aplicarea și interpretarea divergente în mod continuu ale normelor UE de către autoritățile de protecție a datelor, chiar și atunci când provocările în acest domeniu sunt aceleași în întreaga UE, impune consolidarea rolului Grupului de lucru în coordonarea pozițiilor APD, asigurând o aplicare mai uniformă la nivel național și, astfel, un nivel echivalent al protecției datelor.

Comisia va analiza modalitățile:

- de **consolidare, clarificare și armonizare a statutului și competențelor autorităților naționale de protecție a datelor** în noul cadru juridic, incluzând punerea integrală în aplicare a conceptului de „independență deplină”[51];

- de **îmbunătățire a cooperării și coordonării între autoritățile de protecție a datelor**;

- de asigurare a unei aplicări mai coerente a normelor UE de protecție a datelor în cadrul pieței interne. Aceasta poate include **consolidarea rolului autorităților naționale de supraveghere a protecției datelor, o mai bună coordonare a activității acestora prin intermediul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal (care ar trebui să devină un organism mai transparent) și/sau crearea unui mecanism în vederea asigurării coerenței în cadrul pieței interne, sub autoritatea Comisiei Europene**.

3. CONCLUZII: CALEA DE URMAT

Ca și tehnologia, utilizarea și partajarea datelor cu caracter personal în societatea noastră evoluează în permanență. Provocarea cu care se confruntă legiuitorii este aceea de a stabili un cadru juridic care să se dovedească viabil pe termen lung. La încheierea procesului de reformă, normele europene privind protecția datelor ar trebui să garanteze în continuare un nivel ridicat de protecție și să asigure securitate juridică persoanelor, administrațiilor publice și întreprinderilor de pe piața internă, la același nivel și timp de mai multe generații. Indiferent de complexitatea situației sau de caracterul sofisticat al tehnologiei, este esențial ca normele și

---

48 În prezent, acesta este cazul sistemelor informatice de mari dimensiuni, de exemplu SIS II [cf. articolului 46 din Regulamentul (CE) nr. 1987/2006 - JO L 318, 28.12.2006, p. 4) și VIS [cf. articolului 43 din Regulamentul (CE) nr. 767/2008 - JO L 218, 13.8.2008, p. 60).

49 Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal este un organism consultativ format din câte un reprezentat din partea statelor membre, autorităților de protecție a datelor, Autorității Europene pentru Protecția Datelor (AEPD) și Comisiei (fără drept de vot). Secretariatul acestuia este asigurat de Comisie. A se vedea: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal are rolul de a oferi consultanță Comisiei cu privire la nivelul de protecție în UE și în țări terțe, precum și cu privire la orice alte măsuri care se referă la prelucrarea datelor cu caracter personal.

51 Hotărârea CEJ din 9.3.2010, Comisia / Germania, cauza C-518/07.

standardele în materie, pe care autoritățile naționale trebuie să le aplice, iar întreprinderile și dezvoltatorii de tehnologie trebuie să le respecte, să fie definite în mod clar. De asemenea, și persoanele ar trebui să cunoască drepturile pe care le au.

Abordarea globală a Comisiei în vederea remedierii problemelor și îndeplinirii obiectivelor-cheie evidențiate în prezenta comunicare va servi, de asemenea, drept bază pentru discuții ulterioare cu alte instituții europene și cu alte părți interesate, iar apoi va lua forma unor propuneri și măsuri concrete, deopotrivă de natură legislativă și nelegislativă. În acest scop, Comisia dorește să primească reacții cu privire la problemele ridicate în prezenta comunicare.

Pe această bază, în urma unei evaluări a impactului și luând în considerare Carta drepturilor fundamentale a UE, **în 2011**, Comisia **va prezenta propuneri legislative** menite să revizuiască cadrul juridic în materie de protecție a datelor, având obiectivul de a întări poziția UE cu privire la protecția datelor cu caracter personal ale persoanelor în contextul tuturor politicilor UE, inclusiv în contextul aplicării legii și al prevenirii criminalității, luând în considerare elementele specifice acestor domenii. În paralel, se vor lua măsuri nelegislative, cum ar fi încurajarea autoreglementării și analizarea posibilității de a introduce mărci de protecție a vieții private la nivelul UE.

Într-o a doua etapă, Comisia **va evalua necesitatea de a adapta alte instrumente juridice** la noul cadru general în materie de protecție a datelor. Este vorba, în primul rând, de Regulamentul (CE) nr. 45/2001, ale cărui dispoziții vor trebui să fie adaptate la noul cadru juridic general. De asemenea, va trebui analizat cu atenție impactul asupra altor instrumente sectoriale, într-un stadiu ulterior.

De asemenea, Comisia va continua să asigure monitorizarea corespunzătoare a punerii în aplicare corecte a dreptului UE în acest domeniu, ducând o **politică activă de sancționare a încălcărilor**, în cazul în care normele UE de protecție a datelor nu sunt puse în practică și aplicate în mod corect. Într-adevăr, actuala revizuire a instrumentelor de protecție a datelor nu aduce atingere obligației statelor membre de a pune în practică și de a asigura aplicarea corespunzătoare a instrumentelor juridice existente în materie de protecție a datelor cu caracter personal[52].

Un nivel ridicat și uniform de protecție a datelor în interiorul UE va fi cea mai bună modalitate de a susține și a promova, în întreaga lume, standardele UE în materie.

[52] Printre acestea se numără și Decizia-cadru a Consiliului 2008/977/JAI: statele membre trebuie să ia măsurile necesare pentru a se conforma dispozițiilor acesteia până la data de 27 noiembrie 2010.