GRUPUL DE LUCRU PENTRU PROTECȚIA DATELOR INSTITUIT ÎN TEMEIUL ARTICOLULUI 29

0836 -02/10/RO
WP 179

Avizul nr. 8/2010 privind dreptul aplicabil

Adoptat la 16 decembrie 2010

Rezumat

Prezentul aviz clarifică domeniul de aplicare a Directivei 95/46/CE, în special articolul 4, care stabilește dreptul intern privind protecția datelor adoptat în temeiul directivei aplicabil prelucrării datelor cu caracter personal. De asemenea, avizul evidențiază anumite domenii care pot face obiectul unor îmbunătățiri ulterioare.

Stabilirea domeniului de aplicare a dreptului UE în ceea ce privește prelucrarea datelor cu caracter personal servește la clarificarea domeniului de aplicare a dreptului UE privind protecția datelor atât în cadrul UE/SEE, cât și într-un context internațional mai larg. Înțelegerea clară a dreptului aplicabil va contribui la asigurarea securității juridice pentru operatori și a unui cadru clar pentru persoanele fizice și alte părți interesate. De asemenea, înțelegerea corectă a dispozițiilor privind dreptul aplicabil ar trebui să asigure absența lacunelor în ceea ce privește nivelul ridicat de protecție a datelor cu caracter personal prevăzut de Directiva 95/46.

În ceea ce privește articolul 4 alineatul (1) litera (a), trimiterea la „un" sediu înseamnă că aplicabilitatea legislației unui stat membru este determinată de situarea unui sediu al operatorului în statul membru respectiv, în timp ce aplicabilitatea legislațiilor altor state membre este determinată de situarea altor sedii ale aceluiași operator pe teritoriul statelor membre în cauză. Noțiunea „în cadrul activităților" operatorului este decisivă pentru a determina aplicarea dreptului intern. Aceasta presupune că în cadrul *sediului* operatorului se desfășoară *activități* care implică prelucrarea datelor cu caracter personal, luând în considerare gradul său de implicare în activitățile de prelucrare, natura activităților respective și necesitatea de a garanta protecția eficientă a datelor.

În ceea ce privește formularea „recurge la mijloace" din articolul 4 alineatul (1) litera (c), care poate impune aplicarea directivei pentru operatorii care nu sunt stabiliți pe teritoriul UE/SEE, avizul clarifică faptul că aceasta trebuie aplicată în cazurile în care pe teritoriul UE/SEE nu există un sediu *care să determine aplicarea articolului 4 alineatul (1) litera (a)* sau în cazul în care prelucrarea *nu este efectuată în cadrul* unui astfel de sediu. Avizul menționează, de asemenea, că o interpretare largă a noțiunii de „echipamente" – justificată de utilizarea expresiei sale echivalente „mijloace" în alte limbi ale UE – poate în anumite cazuri să ocazioneze aplicarea dreptului european privind protecția datelor atunci când prelucrarea în cauză nu are o legătură reală cu spațiul UE/SEE.

De asemenea, avizul oferă orientări și exemple cu privire la: celelalte dispoziții ale articolului 4; cerințele de securitate care decurg din dreptul aplicabil în temeiul articolului 17 alineatul (3); posibilitatea ca autoritățile pentru protecția datelor să-și utilizeze competențele pentru a verifica și interveni într-o operațiune de prelucrare care are loc pe teritoriul lor chiar dacă dreptul aplicabil este dreptul unui alt stat membru [articolul 28 alineatul (6)].

Avizul sugerează, de asemenea, că formularea utilizată în directivă și compatibilitatea dintre diferitele secțiuni ale articolului 4 ar beneficia de pe urma clarificării ulterioare ca parte a revizuirii cadrului general de protecție a datelor.

Din această perspectivă, simplificarea normelor pentru stabilirea dreptului aplicabil ar consta într-o reorientare către principiul țării de origine: toate sediile unui operator din cadrul UE ar aplica, prin urmare, aceeași legislație – și anume, legislația sediului principal – indiferent de teritoriul pe care sunt situate acestea. Cu toate acestea, acest lucru poate fi acceptat doar dacă se realizează o armonizare cuprinzătoare a legislațiilor naționale, inclusiv armonizarea obligațiilor în materie de securitate.

Criterii suplimentare pot fi aplicate în cazul în care operatorul este stabilit în afara UE, pentru a se asigura că există o conexiune suficientă cu teritoriul UE, evitându-se în același timp utilizarea teritoriului UE pentru desfășurarea unor activități ilegale de prelucrare a datelor de către operatorii stabiliți pe teritoriul țărilor terțe. În acest scop, pot fi dezvoltate următoarele criterii: vizarea persoanelor fizice, având rezultat aplicarea dreptului UE privind protecția datelor în cazul în care activitățile care implică prelucrarea datelor cu caracter personal vizează persoane fizice de pe teritoriul UE; aplicarea criteriilor privind mijloacele într-o formă reziduală și limitată, care ar viza cazurile de referință (date privind persoane vizate care nu fac parte din UE, operatorii neavând vreo legătură cu UE) în care există o infrastructură relevantă de prelucrare a datelor pe teritoriul UE.

instituit în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 (JO L 281, 23.11.1995, p. 31),

având în vedere articolul 29, articolul 30 alineatul (1) litera (a) și articolul 30 alineatul (3) din directiva respectivă,

având în vedere regulamentul său de procedură,

adoptă următorul aviz:

I. Introducere

Definirea dreptului aplicabil în ceea ce privește prelucrarea datelor cu caracter personal în temeiul Directivei 95/46/CE (denumită în continuare „directiva" sau „Directiva 95/46") reprezintă un aspect esențial din mai multe motive. Dispozițiile privind dreptul aplicabil sunt cruciale pentru stabilirea domeniului extern de aplicare a dreptului UE privind protecția datelor, cu alte cuvinte, pentru stabilirea gradului de aplicabilitate a dreptului UE privind protecția datelor în ceea ce privește prelucrarea totală sau parțială a datelor cu caracter personal în afara UE/SEE, dar care are totuși o legătură relevantă cu teritoriul UE/SEE. De asemenea, normele privind dreptul aplicabil stabilesc, în egală măsură, domeniul de aplicare a dreptului privind protecția datelor în cadrul UE/SEE pentru a evita posibilele conflicte dintre statele membre ale UE/SEE și suprapunerea legislațiilor naționale ale acestora în ceea ce privește punerea în aplicare a directivei[1].

În plus, înțelegerea corectă a dispozițiilor dreptului aplicabil ar trebui să asigure absența lacunelor în ceea ce privește nivelul ridicat de protecție a datelor cu caracter personal prevăzut de Directiva 95/46.

Directiva include un număr de dispoziții care abordează aspectele privind dreptul aplicabil, în special articolul 4, articolul 17 și articolul 28. Aceste dispoziții definesc dreptul intern privind protecția datelor aplicabil în conformitate cu directiva, precum și autoritatea care răspunde de aplicarea dreptului respectiv. Este important de amintit faptul că există o interacțiune între dreptul material și competența judiciară. Aceasta este analizată în detaliu în cele ce urmează.

S-a sugerat că punerea în aplicare și interpretarea dispozițiilor directivei privind dreptul aplicabil nu sunt deloc uniforme pe teritoriul Uniunii Europene. Primul raport al Comisiei referitor la punerea în aplicare a Directivei privind protecția datelor a subliniat că punerea în aplicare a articolului 4 din directivă era „deficitară în mai multe cazuri, rezultatul fiind posibila apariție a tipului de conflicte de legi pe care acest articol încearcă să îl evite"[2]. Conform anexei tehnice a raportului, care prezintă o analiză detaliată a diferitelor dispoziții naționale, o astfel de transpunere deficitară se explică, în parte, prin complexitatea dispoziției în sine.

În mod similar, un studiu sponsorizat de Comisia Europeană[3] subliniază ambiguitatea și punerea în aplicare divergentă a normelor privind dreptul aplicabil din directivă și recomandă „*adoptarea imediată de norme mai bune, mai clare și neechivoce privind dreptul aplicabil*".

Comunicarea recentă a Comisiei intitulată „O abordare cuprinzătoare privind protecția datelor cu caracter personal în Uniunea Europeană"[4] menționează că „*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*

---

1 Directiva 95/46/CE se aplică, de asemenea, țărilor AELS Norvegia, Islanda și Liechtenstein în temeiul Acordului SEE (cf. Decizia nr. 83/1999 a Comitetului mixt al SEE din 25 iunie 1999 de modificare a protocolului 37 și a anexei XI (Servicii de telecomunicații) la Acordul SEE; JO L 296/41, 23.11.2000).

2 Primul raport referitor la punerea în aplicare a Directivei privind protecția datelor (95/46/CE), mai 2003, p. 17. Raportul este disponibil la http://ec.europa.eu/justice/policies/privacy/lawreport/report_en.htm

3 „Studiu comparativ privind diversele abordări ale noilor provocări privind viața privată, în special în lumina progreselor tehnologice", ianuarie 2010, disponibil la http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

4 COM (2010) 609 final, 4.11.2010.

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".

De asemenea, complexitatea aspectelor privind dreptul aplicabil crește din cauza globalizării accentuate și a dezvoltării noilor tehnologii: întreprinderile operează din ce în ce mai mult în jurisdicții diverse, furnizând servicii și asistență 24 de ore din 24; internetul facilitează furnizarea de servicii la distanță, precum și colectarea și împărtășirea datelor cu caracter personal într-un mediu virtual; informatica dematerializată („cloud computing") îngreunează stabilirea locației datelor cu caracter personal și a mijloacelor utilizate în orice moment.

Prin urmare, este esențial ca sensul precis al dispozițiilor directivei privind dreptul aplicabil să fie suficient de clar pentru toți cei implicați în punerea în aplicare a directivei, precum și în aplicarea de zi cu zi a dreptului intern privind protecția datelor atât în sectorul public, cât și în cel privat.

În consecință, grupul de lucru a hotărât să contribuie la clarificarea anumitor dispoziții esențiale ale directivei și să analizeze conceptul de drept aplicabil, la fel cum a procedat în cazul conceptului de date cu caracter personal și al conceptelor de „operator" și „persoană împuternicită de către operator"[5]. În prezentul aviz, grupul de lucru face, de asemenea, trimiteri la alte avize în care a abordat problema dreptului aplicabil rezultată în legătură cu subiectele specifice abordate în avizele respective[6].

Obiectivul final al grupului de lucru este de a oferi o anumită securitate juridică în ceea ce privește aplicarea dreptului UE privind protecția datelor. Aceasta înseamnă, pe de o parte, că persoanele vizate sunt conștiente de normele care se aplică în materie de protecție a datelor cu caracter personal și, pe de altă parte, că operatorii economici, precum și alte organisme publice și private, cunosc normele de protecție a datelor care reglementează prelucrarea datelor de către aceștia.

Clarificarea conceptului de drept aplicabil este foarte importantă, independent de posibilele modificări viitoare ale dispozițiilor actuale ale directivei. Dispozițiile actuale vor rămâne valabile până când vor fi modificate și în măsura în care nu sunt modificate. Prin urmare, clarificarea dispozițiilor privind dreptul aplicabil va contribui la asigurarea unei mai bune respectări a directivei până la modificarea legislației. În plus, pentru redactarea prezentului aviz, grupul de lucru a avut posibilitatea de a valorifica experiența rezultată în urma aplicării dispozițiilor actuale pentru a furniza orientări legiuitorilor în ceea ce privește viitoarele revizuiri ale directivei.

---

5 Avizul nr. 4/2007 privind conceptul de date cu caracter personal (WP 136); Avizul nr. 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator" (WP 169). Toate avizele sunt disponibile la: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

6 În special, documentul de lucru privind stabilirea aplicării la nivel internațional a dreptului UE privind protecția datelor în ceea ce privește prelucrarea online a datelor cu caracter personal de către site-uri internet stabilite în afara UE (WP 56), Avizul nr. 10/2006 privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT) (WP 128) și Avizul nr. 1/2008 privind aspectele referitoare la protecția datelor în legătură cu motoarele de căutare (WP 148).

În cele din urmă, dispozițiile privind stabilirea dreptului aplicabil cu privire la protecția datelor sunt menite să reglementeze implementarea directivei în cadrul propriului domeniu de aplicare, astfel cum a fost definit la articolul 3. Ca atare, acestea vor interacționa adesea cu alte domenii legislative fără a le influența dincolo de domeniul lor de aplicare[7].

II. Observații generale și aspecte politice

II.1. Scurt istoric: de la Convenția 108 la Directiva 95/46/CE

În 1981, autorii Convenției 108, redactată sub auspiciile Consiliului Europei, au identificat riscurile prezentate de cazurile de conflict de legi sau lacună juridică care ar putea rezulta în urma aplicării diferitelor legislații naționale. Cu toate acestea, convenția în cauză nu includea norme specifice privind abordarea acestor probleme: furnizarea unei „baze comune de drept material" de către convenție era considerată ca fiind principala garanție conform căreia, în pofida existenței unor reglementări diverse, principiile care urmau să fie aplicate în cele din urmă ar fi aceleași, evitându-se astfel diferențele în ceea ce privește nivelul de protecție.

Necesitatea unor criterii de stabilire a dreptului aplicabil a fost abordată de Comisia Europeană în momentul redactării Directivei privind protecția datelor. În propunerea sa inițială[8], Comisia a identificat locația fișierelor de date drept factorul determinant principal, iar sediul operatorilor drept factorul determinant secundar în cazul în care fișierul este localizat pe teritoriul unei țări terțe.

În cursul discuțiilor din cadrul Parlamentului European și Consiliului UE, a existat o reorientare dinspre criteriul privind locația fișierului către criteriul privind sediul operatorului. Localizarea mijloacelor a fost identificată drept criteriu secundar în cazul în care operatorul nu este stabilit pe teritoriul UE.

Consiliul a completat aceste criterii și a furnizat indicații suplimentare referitoare la noțiunea de sediu. Propunerea modificată a Comisiei[9] specifica faptul că prelucrarea ar trebui să aibă loc „în cadrul activităților operatorului cu sediul..." și lua în considerare posibilitatea ca operatorul să aibă mai multe sedii în diferite state membre. O modificare majoră viza faptul că principalul criteriu de stabilire a dreptului aplicabil nu consta în locul în care operatorul își are sediul principal, ci în locul în care există *un* sediu al operatorului. Consecințele acestor modificări, în termeni de aplicare distributivă și nu uniformă a dreptului intern în cazul sediilor multiple, vor fi dezvoltate mai jos.

---

7 Deși directiva conține dispoziții privind răspunderea (articolul 23) și sancțiunile (articolul 24), în principiu nu se aduce atingere normelor generale de drept civil sau penal, astfel cum se prevede la considerentul 21 din directivă. Acestea ar fi vizate doar în măsura în care sunt necesare anumite sancțiuni în cazul nerespectării principiilor referitoare la protecția datelor. În practică, punerea în aplicare la nivel național a directivei a condus la diverse scenarii, care includ sau nu sancțiuni penale. Pentru a menționa un alt exemplu, deși directiva conține dispoziții privind necesitatea acordului – a se vedea articolul 2 litera (h), articolul 7 litera (a) și articolul 8 alineatul (2) litera (a) – sau relevanța obligațiilor contractuale – a se vedea articolul 7 litera (b) – aceasta nu abordează dreptul contractual (de exemplu, condițiile de încheiere a unui contract, dreptul aplicabil) sau alte aspecte de drept civil în afara dispozițiilor sale.

8 COM (1990) 314 – 2, 18.07.1990, Propunere de directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește protecția datelor cu caracter personal.

9 COM (1992) 422 final, 15.10.1992.

II.2. Rolul conceptelor

II.2.a) Context și importanța strategică

Stabilirea aplicării dreptului UE în ceea ce privește prelucrarea datelor cu caracter personal, astfel cum s-a menționat anterior, servește la clarificarea domeniului de aplicare a dreptului UE privind protecția datelor atât în cadrul UE/SEE, cât și într-un context internațional mai larg. Înțelegerea clară a dreptului aplicabil va contribui la asigurarea securității juridice pentru operatori și a unui cadru clar pentru persoanele vizate și alte părți interesate.

Identificarea dreptului aplicabil este strâns legată de identificarea operatorului[10] și a sediului (sediilor) său (sale): principala consecință a acestei legături constă în reafirmarea responsabilităților operatorului și ale reprezentantului acestuia în cazul în care operatorul este stabilit într-o țară terță.

Astfel cum se va arăta în cele ce urmează, aceasta nu înseamnă că va exista întotdeauna un singur drept aplicabil, în special dacă operatorul are mai multe sedii: situarea acestor sedii și natura activităților desfășurate în cadrul acestora vor fi, de asemenea, decisive. Legătura clară dintre dreptul aplicabil și operator poate fi, în schimb, o garanție a eficacității și a punerii în aplicare, în special în contextul în care localizarea unui fișier (cum poate fi cazul informaticii dematerializate) poate fi dificilă sau uneori imposibil de realizat.

Orientările clare privind normele de drept aplicabil ar trebui să contribuie la abordarea noilor progrese: tehnologice (internet; fișiere bazate pe rețea/informatică dematerializată) și comerciale (întreprinderi multinaționale).

II.2.b) Domeniul de aplicare a dreptului UE și a dreptului intern în cadrul UE/SEE

Principalele criterii de stabilire a dreptului aplicabil sunt situarea sediului operatorului și situarea mijloacelor sau echipamentelor[11] care sunt utilizate în cazul în care operatorul este stabilit în afara SEE. Aceasta înseamnă că naționalitatea sau locul de reședință obișnuită a persoanelor vizate, precum și locația fizică a datelor cu caracter personal nu sunt decisive în acest sens[12].

Acest fapt induce un domeniu mai larg de aplicare cu implicații juridice extinse dincolo de teritoriul SEE: directiva – și normele naționale de punere în aplicare – se aplică prelucrării datelor cu caracter personal în afara SEE (în cazul în care prelucrarea este efectuată în cadrul activităților operatorului cu sediul pe teritoriul SEE), precum și operatorilor stabiliți în afara SEE (în cazul în care aceștia recurg la mijloace situate pe teritoriul SEE). În consecință, dispozițiile directivei pot fi aplicabile serviciilor cu dimensiune internațională, cum ar fi motoarele de

---

10 A se vedea Avizul nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator” (WP 169).

11 Astfel cum se explică mai jos la punctul III.2.b, noțiunea de „echipamente” a fost redată în alte limbi ale UE drept „mijloace”. Aceasta susține interpretarea largă a noțiunii de echipamente și explică de ce în prezentul document sunt utilizate ambele noțiuni.

12 A se vedea în același sens Directiva 2000/31/CE privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă. Un factor relevant suplimentar este locația persoanei împuternicite de către operator cu privire la dreptul aplicabil măsurilor de securitate (articolul 17). Cu toate acestea, criteriul menționat anterior nu este decisiv în sine și trebuie aplicat în legătură cu principalul criteriu privind sediul operatorului.

căutare, rețelele sociale și informatica dematerializată. Aceste exemple sunt dezvoltate mai jos în prezentul document.

În cazul în care datele cu caracter personal sunt prelucrate de către un operator de date (X) al cărui sediu unic este situat pe teritoriul unui stat membru A, dreptul aplicabil prelucrării va fi dreptul intern al statului membru A, indiferent de locul în care este efectuată aceasta.

În cazul în care X dispune, de asemenea, de un sediu (Y) pe teritoriul unui stat membru B, dreptul intern aplicabil prelucrării la sediul Y va fi dreptul intern al statului membru B, cu condiția ca prelucrarea să fie efectuată în cadrul activităților Y. Dacă la sediul Y se efectuează prelucrarea în cadrul activităților X cu sediul pe teritoriul statului membru A, dreptul aplicabil prelucrării va fi dreptul statului membru A.

În cazul în care datele cu caracter personal sunt prelucrate de către un operator de date care nu este stabilit pe teritoriul niciunui stat membru, prelucrarea va intra sub incidența domeniului de aplicare a dreptului intern al statului membru în care sunt localizate echipamentele (sau mijloacele) folosite de către operatorul de date pentru prelucrarea datelor. Exemple de astfel de scenarii diferite vor fi analizate pe parcursul prezentului aviz.

Obiectivul acestui amplu domeniu de aplicare este în primul rând de a asigura protecția persoanelor fizice prevăzută de directivă și, în același timp, de a preveni eludarea dreptului.

Directiva prevede criterii pentru a stabili:
(i) atât dacă dreptul european – coroborat sau nu cu dreptul unei țări terțe – se aplică unei activități specifice de prelucrare a datelor cu caracter personal; cât și
(ii) dacă dreptul european se aplică prelucrării, care dintre drepturile interne ale statelor membre se aplică prelucrării.

De asemenea, trebuie remarcat faptul că anumite activități de prelucrare în cadrul UE se află în afara domeniului de aplicare a directivei, însă pot determina aplicarea altor instrumente juridice ale UE, cum ar fi Decizia-cadru 2008/977/JAI privind protecția datelor în cadrul cooperării polițienești și judiciare în materie penală[13] sau Regulamentul 45/2001 privind prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare[14] sau alte instrumente privind organisme sau sisteme specifice de informare (de exemplu, Europol, Eurojust, SIS, CIS etc.)[15] ale UE.

II.2.c) Evitarea lacunelor și a suprapunerilor nejustificate

Obiectivul criteriilor clare de stabilire a dreptului aplicabil este de a evita atât eludarea reglementărilor de drept intern ale statelor membre, cât și suprapunerea reglementărilor respective. Numărul drepturilor aplicabile prelucrării va depinde de numărul și de natura activităților efectuate în cadrul sediului (sediilor) operatorului:

[13] 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).

[14] Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

[15] Europol: Decizia Consiliului 2009/371/JAI, JO L 121, 15.5.2009, p. 37); Eurojust: Decizia Consiliului 2002/187/JAI, JO L 63, 6.3.2002, p. 1, modificată prin Decizia Consiliului 2009/426/JAI, JO L 138, 4.6.2009, p. 14.

- Dacă operatorul are un singur sediu, se va aplica o singură legislație pentru întreg teritoriul UE/SEE, în funcție de situarea sediului respectiv[16].
- Dacă operatorul are mai multe sedii: aplicarea legislației naționale va fi distribuită în funcție de activitățile din cadrul fiecărui sediu în parte.

Aplicarea criteriilor ar trebui să prevină aplicarea simultană a mai multor legislații naționale pentru aceeași activitate de prelucrare.

II.2.d) Dreptul aplicabil și competența judiciară în contextul directivei

În materie de protecție a datelor, este deosebit de important să se facă distincția între conceptul de *drept aplicabil* (care stabilește regimul juridic aplicabil într-un anumit caz) și conceptul de *competență judiciară* (care stabilește de obicei competența unei instanțe naționale de a soluționa anumite cauze sau de a pune în aplicare o hotărâre sau un ordin). Dreptul aplicabil și competența judiciară în ceea ce privește o anumită activitate de prelucrare pot să nu fie întotdeauna unul și același lucru.

Domeniul extern de aplicare a dreptului UE este o expresie a capacității Uniunii de a prevedea norme pentru a proteja interesele fundamentale în cadrul jurisdicției sale. Dispozițiile directivei stabilesc, de asemenea, domeniul de aplicare a legislațiilor naționale ale statelor membre, fără a afecta însă competența judiciară a instanțelor naționale în soluționarea cauzelor relevante înaintate acestora. Cu toate acestea, dispozițiile directivei fac referire la domeniul teritorial de aplicare a competenței autorităților de supraveghere care pot să pună în aplicare și să execute dreptul aplicabil.

Deși în majoritatea cazurilor aceste două concepte – drept aplicabil și competența autorităților de supraveghere – tind să se confunde, rezultatul fiind de obicei aplicarea dreptului unui stat membru A de către autoritățile statului membru A, directiva prevede în mod explicit posibilitatea unor aranjamente diverse. Articolul 28 alineatul (6) presupune că autoritățile naționale pentru protecția datelor ar trebui să își poată exercita puterile în momentul în care se aplică dreptul unui alt stat membru privind protecția datelor în ceea ce privește prelucrarea datelor cu caracter personal efectuată în cadrul jurisdicției lor. Consecințele practice ale acestei situații vor fi examinate ulterior într-un viitor aviz al grupului de lucru.

Astfel de situații au ca rezultat gestionarea cazurilor transfrontaliere și evidențiază necesitatea cooperării între autoritățile pentru protecția datelor, având în vedere competențele de executare ale fiecărei autorități pentru protecția datelor implicate. Aceasta ilustrează, de asemenea, necesitatea unui drept intern care să pună în aplicare în mod corespunzător dispozițiile relevante ale directivei, întrucât acest lucru poate fi decisiv pentru cooperarea și aplicarea transfrontalieră eficientă.

III. Analiza dispozițiilor

Dispoziția esențială privind dreptul aplicabil o constituie articolul 4, care stabilește dreptul (drepturile) intern(e) privind protecția datelor adoptat(e) în temeiul directivei aplicabil(e) în ceea ce privește prelucrarea datelor cu caracter personal.

[16] Cu excepția măsurilor de securitate, care vor depinde de locația operatorului posibil, astfel cum prevede articolul 17 alineatul (3) din directivă.

III.1. Operatorul este stabilit pe teritoriul unuia sau mai multor state membre [articolul 4 alineatul (1) litera (a)]

Prima situație prevăzută de articolul 4 alineatul (1) este cea a operatorilor care au unul sau mai multe sedii pe teritoriul UE. În acest caz, articolul 4 alineatul (1) litera (a) prevede că un stat membru aplică dreptul intern privind protecția datelor atunci când *„[...] prelucrarea este efectuată în cadrul activităților operatorului cu sediul pe teritoriul statului membru; dacă același operator este stabilit pe teritoriul mai multor state membre, acesta trebuie să ia măsurile necesare pentru a se asigura că fiecare din sedii respectă obligațiile prevăzute în dreptul intern aplicabil”*.

Trebuie reamintit faptul că conceptul de „operator” este definit la articolul 2 litera (d) din directivă. Definiția nu va fi analizată în prezentul aviz deoarece aceasta a fost clarificată deja de grupul de lucru instituit în temeiul articolului 29 în avizul său privind conceptele de „operator” și „persoană împuternicită de către operator”[17].

În plus, este important de subliniat faptul că un sediu nu necesită personalitate juridică și că noțiunea de sediu are conexiuni flexibile cu noțiunea de control. Un operator poate avea mai multe sedii, operatorii în comun pot concentra activitățile în cadrul unui singur sediu sau în cadrul unor sedii diferite. Elementul decisiv de determinare a unui sediu în temeiul directivei constă în exercitarea efectivă și reală a activităților în cadrul cărora sunt prelucrate datele cu caracter personal.

a) „…operatorului cu sediul pe teritoriul statului membru…”

Noțiunea de sediu nu este definită în directivă. Preambulul directivei indică totuși că „*stabilirea pe teritoriul unui stat membru presupune exercitarea efectivă și reală a unei activități într-o formă de instalare stabilă (și că) forma juridică a stabilirii, fie că este doar sucursală, fie că este filială cu personalitate juridică, nu este factorul determinant în această privință” (considerentul 19).*

În ceea ce privește libertatea de stabilire în temeiul articolului 50 TFUE (fostul articol 43 TCE), Curtea Europeană de Justiție (CEJ) a hotărât că un sediu stabil necesită ca „atât resursele umane, cât și resursele tehnice necesare pentru furnizarea de servicii specifice să fie disponibile în permanență”[18].

Accentul puternic pus în preambulul directivei pe „exercitarea efectivă și reală a unei activități într-o formă de instalare stabilă” reflectă în mod clar noțiunea de „sediu stabil” la care face referire Curtea de Justiție la momentul adoptării directivei. Deși nu este clar dacă această interpretare, precum și interpretările ulterioare ale CEJ privind libertatea de stabilire în temeiul articolului 50 TFUE pot fi aplicate în totalitate situațiilor reglementate de articolul 4 din Directiva privind protecția datelor, interpretarea Curții în cauzele respective poate furniza orientări utile pentru analiza formulării directivei.

---

17 Avizul nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator” (WP 169).

18 Hotărârea CEJ din 4 iulie 1985, *Bergholz*, (cauza 168/84, Rec., p. 2251, punctul 14) și hotărârea din 7 mai 1998, *Lease Plan Luxembourg* contra *Belgische Staat* (C-390/96, Rec., p. I-2553). În cel de-al doilea caz, problema consta în a stabili dacă un server de întreprindere, situat într-o țară alta decât țara furnizorului de servicii, poate fi considerat drept sediu stabil. Obiectivul consta în identificarea țării pentru care trebuia plătit TVA. Judecătorul a refuzat să considere mijloacele informatice drept sediu virtual (interpretare care ne face să ne întoarcem la noțiunea „clasică” de „sediu”, diferită de cea adoptată în hotărârile anterioare din 17 iulie 1997, *ARO Lease* contra *Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (C-190/95, Rec., p. I-4383).

Această interpretare este utilizată în următoarele exemple:

- În cazul în care are loc „exercitarea efectivă și reală a unei activități”, de exemplu, într-un oficiu al procuraturii, prin „instalare stabilă”, oficiul respectiv este considerat drept sediu.

- Un server sau un calculator nu pot fi considerate drept sediu, întrucât acestea reprezintă simple echipamente sau instrumente tehnice pentru prelucrarea informațiilor[19].

- Un oficiu cu o singură persoană poate fi considerat drept sediu atât timp cât acesta nu se limitează la simpla reprezentare a unui operator stabilit în altă parte, ci este implicat activ în activitățile în cadrul cărora este efectuată prelucrarea datelor cu caracter personal.

- În orice caz, forma oficiului nu este decisivă: chiar și un simplu agent poate fi considerat drept sediu relevant dacă prezența acestuia în statul membru prezintă suficientă stabilitate.

Exemplul nr. 1: Broșuri pentru călători

O întreprindere stabilită pe teritoriul statului membru A colectează date privind serviciile furnizate de stațiile de benzină din statul membru B cu scopul de a crea o broșură pentru călători. Datele sunt colectate de către un angajat care, călătorind pe teritoriul B, adună și trimite fotografii și comentarii angajatorului de pe teritoriul A. În acest caz, datele sunt colectate pe teritoriul B (în lipsa unui „sediu” pe teritoriul respectiv) și sunt prelucrate în cadrul activităților operatorului cu sediul pe teritoriul A: dreptul aplicabil este dreptul A.

Articolul 4 alineatul (1) litera (a), făcând referire la *un* sediu al *operatorului* pe teritoriul *statului membru*, generează preocupări – altele decât conceptul de sediu – care necesită clarificare.

În primul rând, trimiterea la „un” sediu înseamnă că aplicabilitatea legislației unui stat membru va fi determinată de situarea sediului operatorului pe teritoriul statului membru în cauză, în timp ce aplicabilitatea legislațiilor altor state membre este determinată de situarea altor sedii aparținând aceluiași operator pe teritoriul statelor membre respective.

Chiar dacă sediul principal al operatorului se află pe teritoriul unei țări terțe, faptul că unul dintre sediile acestuia se află pe teritoriul unui stat membru poate determina aplicabilitatea dreptului intern al țării respective, cu condiția ca celelalte dispoziții ale articolului 4 alineatul (1) litera (a) să fie îndeplinite [a se vedea litera (b) de mai jos]. Acest lucru este confirmat, de asemenea, de cea de-a doua parte a dispoziției, care prevede în mod explicit că, în cazul în care același operator este stabilit pe teritoriul mai multor state membre, acesta trebuie să se asigure că fiecare sediu respectă dreptul aplicabil relevant.

b) „… prelucrarea este efectuată în cadrul activităților ...”

Directiva leagă aplicabilitatea dreptului unui stat membru privind protecția datelor de prelucrarea datelor cu caracter personal. Conceptul de „prelucrare” a fost abordat deja în mod incidental de grupul de lucru în alte avize, care au evidențiat faptul că diversele operațiuni sau seturi de operațiuni asupra datelor cu caracter personal pot fi efectuate

[19] Problema dacă acestea pot fi considerate altfel, de exemplu, drept „mijloace”, va fi dezbătută ulterior în text.

simultan sau în etape[20]. În contextul stabilirii dreptului aplicabil, aceasta poate la fel de bine să însemne că diversele drepturi aplicabile pot fi determinate de diferitele etape de prelucrare a datelor cu caracter personal.

În timp ce multiplicarea drepturilor aplicabile reprezintă, prin urmare, un risc serios, ar trebui să se țină seama de posibilitatea ca legăturile la nivel macro dintre diversele activități de prelucrare să conducă alternativ la aplicarea unui singur drept intern. Pentru a stabili dacă se aplică unul sau mai multe drepturi pentru diversele etape de prelucrare, este important să se țină cont de perspectiva globală a activităților de prelucrare: un set de operațiuni efectuate într-un număr de state membre diferite, însă toate menite să deservească un singur scop, pot avea ca rezultat aplicarea unui singur drept intern.

În astfel de circumstanțe, noțiunea „în cadrul activităților" – și nu locația datelor – constituie factorul decisiv în identificarea dreptului aplicabil.

Noțiunea „în cadrul activităților" nu presupune că dreptul aplicabil este dreptul statului membru pe teritoriul căruia se află sediul *operatorului*, ci pe teritoriul căruia un *sediu* al operatorului este implicat în *activități* de prelucrare a datelor.

Analiza diverselor scenarii poate contribui la clarificarea noțiunii „în cadrul activităților" și a influenței acesteia în ceea ce privește stabilirea dreptului aplicabil pentru diversele activități de prelucrare din țări diferite.

a. Dacă un operator este stabilit în Austria și prelucrează date cu caracter personal pe teritoriul Austriei, în cadrul activităților sediului respectiv, dreptul aplicabil va fi în mod evident dreptul austriac – și anume, dreptul țării pe teritoriul căreia se află situat sediul în cauză.

b. În cel de-al doilea scenariu, prelucrarea datelor cu caracter personal colectate prin intermediul unui site internet este efectuată în cadrul activităților operatorului cu sediul în Austria. Site-ul internet este accesibil utilizatorilor din diverse țări. Dreptul aplicabil privind protecția datelor va fi în continuare dreptul austriac – și anume, dreptul țării pe teritoriul căreia se află situat sediul în cauză – independent de locația utilizatorilor și a datelor.

c. În cel de-al treilea scenariu, operatorul este stabilit în Austria și externalizează prelucrarea către o persoană împuternicită din Germania. Prelucrarea în Germania este efectuată în cadrul activităților operatorului din Austria. Cu alte cuvinte, prelucrarea este efectuată în scopurile comerciale și la instrucțiunile sediului austriac. Dreptul aplicabil prelucrării efectuate de către persoana împuternicită din Germania va fi dreptul austriac. În plus, persoana împuternicită va face obiectul cerințelor dreptului german cu privire la măsurile de securitate pe care aceasta este obligată să le pună în aplicare în legătură cu prelucrarea[21]. Astfel de aranjamente necesită supravegherea coordonată a autorităților germane și austriece pentru protecția datelor.

---

20 A se vedea, de exemplu, Avizul nr. 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator" (WP 169).

21 În conformitate cu articolul 17 alineatul (3) din Directiva 95/46/CE, persoana împuternicită de către operator face obiectul obligațiilor definite de dreptul statului membru pe teritoriul căruia se află sediul acesteia în ceea ce privește măsurile de securitate. În cazul unui conflict între obligațiile de fond privind securitatea prevăzute de dreptul persoanei împuternicite de către operator și de dreptul operatorului, *lex loci* (dreptul persoanei împuternicite de către operator) primează. În timp ce obligația finală revine operatorului, persoana împuternicită de către operator trebuie să demonstreze că a întreprins toate măsurile necesare în conformitate cu contractul încheiat cu operatorul, precum și obligațiile de securitate definite de dreptul statului membru pe teritoriul căruia se află sediul persoanei împuternicite de către operator (a se vedea mai multe detalii la punctul III.5).

d. În cel de-al patrulea scenariu, operatorul stabilit în Austria înființează o sucursală în Italia, care organizează toate conținuturile italiene ale site-ului internet și gestionează cererile utilizatorilor italieni. Activitățile de prelucrare a datelor efectuate de sucursala italiană sunt desfășurate în cadrul sediului din Italia, dreptul aplicabil acestora fiind, prin urmare, dreptul italian.

Concluziile privind dreptul aplicabil pot fi trase doar pe baza înțelegerii precise a noțiunii „în cadrul activităților". În realizarea acestei analize trebuie avute în vedere următoarele considerații:

Gradul de implicare a sediului (sediilor) în activitățile în cadrul cărora este efectuată prelucrarea datelor cu caracter personal este esențial. În acest context, trebuie să se verifice „cine și ce face", și anume, care activități sunt efectuate în cadrul unui anumit sediu pentru a se putea stabili dacă sediul respectiv este relevant pentru a determina aplicarea dreptului intern privind protecția datelor. În cazul în care la un sediu se prelucrează date cu caracter personal în cadrul activităților proprii, dreptul aplicabil va fi dreptul statului membru pe teritoriul căruia este situat sediul respectiv. În cazul în care la sediul respectiv se prelucrează date cu caracter personal în cadrul activităților unui alt sediu, dreptul aplicabil va fi dreptul statului membru pe teritoriul căruia este situat celălalt sediu.

Natura activităților sediilor constituie un element secundar, însă va contribui la identificarea dreptului aplicabil pentru fiecare sediu în parte: întrebarea dacă o activitate implică sau nu prelucrarea datelor și ce tip de prelucrare are loc în cadrul unei anumite activități depinde în mare parte de natura activităților respective. Ca alternativă, faptul că diferite sedii pot fi implicate în activități complet diferite în cadrul cărora sunt prelucrate date cu caracter personal va avea impact asupra dreptului aplicabil. Exemplul 4 dezvoltă o ilustrare a acestor considerații.

De asemenea, ar trebui luat în considerare obiectivul general al directivei, întrucât acesta vizează să garanteze o protecție eficientă pentru persoanele fizice într-un mod simplu, operațional și previzibil.

Exemplul nr. 2: Transferul datelor cu caracter personal în legătură cu factorizarea

O întreprindere italiană de utilități transferă informații referitoare la creditorii săi unei bănci franceze de investiții în vederea factorizării datoriilor. Datoriile au rezultat în legătură cu facturile neplătite la energie. Transferul de informații privind datoriile implică transferul datelor cu caracter personal ale clienților către banca franceză de investiții, în special către sucursala din Italia (și anume, sediul băncii franceze de pe teritoriul Italiei).

Banca franceză de investiții este un operator de date în ceea ce privește operațiunile de prelucrare care constituie transferul, iar sucursala sa din Italia gestionează și percepe datoriile în numele său. Datele sunt prelucrate de către operatorul de date atât în Franța, cât și cadrul sucursalei italiene. Operatorul de date din Franța furnizează tuturor clienților italieni un aviz de informare privind operațiunea de mai sus prin intermediul sucursalei din Italia.

Sucursala italiană este un sediu în temeiul directivei, iar activitățile sale care constau în prelucrarea datelor cu caracter personal în vederea informării clienților în legătură cu aranjamentele vor trebui să respecte legislația italiană privind protecția datelor. Măsurile de securitate din cadrul sucursalei italiene vor trebui să respecte, de asemenea, condițiile legislației italiene privind protecția datelor, în timp ce operatorul

francez va trebui să respecte în paralel obligațiile franceze privind securitatea datelor prelucrate în cadrul sediului său din Franța. Persoanele vizate, și anume creditorii, pot înainta plângeri sucursalei italiene cu scopul de a-și exercita drepturile privind protecția datelor, cum ar fi accesul, rectificarea și ștergerea datelor în temeiul dreptului italian.

Pentru analizarea acestor criterii trebuie avută în vedere o abordare funcțională: mai mult decât evaluarea teoretică efectuată de către părți în legătură cu dreptul aplicabil, comportamentul practic și interacțiunea acestora ar trebui să fie factorii decisivi: care este rolul real al fiecărui sediu și care sunt activitățile care au loc în cadrul unui anumit sediu?

Trebuie să se acorde o atenție specială gradului de implicare a fiecărui sediu în legătură cu activitățile în cadrul cărora sunt prelucrate datele cu caracter personal. Înțelegerea noțiunii „în cadrul" este, prin urmare, utilă în cazurile complexe care diferențiază activitățile efectuate în cadrul diferitelor sedii aparținând aceleiași întreprinderi pe teritoriul UE.

Exemplul nr. 3: Colectarea datelor clienților de către magazine

Un lanț de magazine „prêt à porter" cu sediul principal în Spania dispune de magazine pe întreg teritoriul UE. Datele referitoare la clienți sunt colectate în fiecare dintre magazinele respective, acestea fiind însă transferate către sediul principal din Spania, unde au loc o serie de activități legate de prelucrarea datelor (analiza profilurilor clienților, servicii destinate clienților, publicitate țintă).

Activități cum ar fi promovarea directă pentru clienții europeni sunt gestionate exclusiv de către sediul principal din Spania. Aceste activități sunt catalogate ca având loc în cadrul activităților sediului spaniol. Prin urmare, dreptul aplicabil activităților de prelucrare este dreptul spaniol.

Cu toate acestea, magazinele individuale sunt în continuare responsabile de aspectele privind prelucrarea datelor cu caracter personal ale clienților lor care au loc în cadrul activităților magazinului respectiv (de exemplu, colectarea informațiilor cu caracter personal ale clienților). În măsura în care prelucrarea are loc în cadrul activităților fiecărui magazin, aceasta face obiectul dreptului țării pe teritoriul căruia se află magazinul în cauză.

O consecință practică directă a acestei analize este că fiecare magazin trebuie să adopte măsurile necesare pentru a informa persoanele fizice în legătură cu condițiile de colectare și prelucrare ulterioară a datelor lor în temeiul dreptului intern.

Clienții pot depune plângeri direct la autoritatea pentru protecția datelor din țara de origine. Dacă plângerile fac referire la acțiunile de promovare directă din cadrul activităților sediului principal din Spania, autoritatea locală pentru protecția datelor va trebuie să înainteze cazul către autoritatea pentru protecția datelor din Spania.

Prin urmare, este posibil ca un singur sediu să fie implicat în diferite tipuri de activități și ca diferite drepturi interne să fie aplicabile prelucrării datelor în cadrul acestor activități diferite. Pentru a oferi o abordare previzibilă și operațională în care există posibilitatea aplicării mai multor drepturi pentru diferitele activități ale aceluiași sediu, ar trebui utilizată o abordare funcțională, inclusiv un context juridic mai larg.

Exemplul nr. 4: Bază de date centralizată privind resursele umane

Situațiile în care aceeași bază de date poate face obiectul unor drepturi aplicabile diferite au loc frecvent în practică. Acesta este adesea cazul în domeniul resurselor umane, în care filialele/sediile din țări diferite centralizează datele angajaților într-o singură bază de date. În timp ce aceasta se întâmplă în mod tradițional din cauza economiilor de scară, acest lucru nu ar trebui să aibă impact asupra responsabilităților fiecărui sediu în parte în temeiul dreptului intern. Acesta este cazul nu doar din perspectiva protecției datelor, ci și în contextul dispozițiilor privind dreptul muncii și ordinea publică.

Dacă, de exemplu, datele angajaților unei filiale irlandeze (care se califică drept sediu) au fost transferate către o bază de date centralizată din Regatul Unit în care sunt stocate, de asemenea, datele angajaților filialei/sediului britanic, se aplică două drepturi diferite (irlandez și britanic) privind protecția datelor.

Aplicarea a două drepturi interne diferite nu este consecința faptului că datele își au originea în două state membre diferite, ci rezultă în urma prelucrării datelor angajaților din Irlanda de către sediul din Regatul Unit în cadrul activităților sediului irlandez în calitate de angajator.

Acest exemplu ilustrează faptul că nu locul în care sunt trimise sau localizate datele este cel care determină dreptul intern aplicabil, ci natura și locul activităților curente sunt factorii cheie care determină „cadrul" în care este efectuată prelucrarea: prin urmare, datele privind resursele umane sau clienții fac în mod normal obiectul dreptului privind protecția datelor din țara în care are loc activitatea – în cadrul căreia sunt prelucrate datele. Aceasta confirmă, de asemenea, că nu există o corelație directă între dreptul intern aplicabil și competența judiciară, întrucât dreptul intern se poate aplica în afara jurisdicției naționale.

Pentru a sintetiza, criteriile utilizate pentru a stabili dreptul aplicabil au efect la diferite niveluri:

- În primul rând, acestea sunt utile pentru a stabili dacă dreptul UE privind protecția datelor este sau nu aplicabil în ceea ce privește prelucrarea;
- În al doilea rând, în cazul în care se aplică dreptul UE privind protecția datelor, criteriile vor stabili
  (a) dreptul cărui stat membru este aplicabil în ceea ce privește protecția datelor, și
  (b) în cazul în care există mai multe sedii în state membre diferite, care dintre drepturile statelor membre privind protecția datelor se aplică unei anumite activități de prelucrare;
- În al treilea rând, criteriile vor fi utile în cazul în care există o dimensiune extra-europeană pentru activitățile de prelucrare – precum în următoarea ilustrare, în care operatorul este stabilit în afara SEE.

Exemplul nr. 5: Furnizorul de servicii internet

Un furnizor de servicii internet (operatorul de date) este stabilit în afara UE, de exemplu în Japonia. Acesta are sedii comerciale în majoritatea statelor membre ale UE și un sediu în Irlanda, care se ocupă cu probleme legate de prelucrarea datelor cu caracter personal, inclusiv, în special, suport TIC. Operatorul dezvoltă un centru de date în Ungaria, cu angajați și servere dedicate prelucrării și stocării datelor referitoare la utilizatorii serviciilor sale.

De asemenea, operatorul din Japonia dispune de anumite sedii în diverse state membre ale UE, care desfășoară diferite activități:

- centrul de date din Ungaria se ocupă doar de întreținerea tehnică;
- sediile comerciale ale FSI organizează campanii generale de publicitate;
- sediul din Irlanda este singurul sediu de pe teritoriul UE care desfășoară activități în cadrul cărora sunt prelucrate efectiv datele cu caracter personal (fără a aduce atingere datelor de intrare ale sediilor centrale din Japonia).

Activitățile sediului irlandez determină aplicarea dreptului UE privind protecția datelor: datele cu caracter personal sunt prelucrate în cadrul activităților sediului irlandez, prin urmare, prelucrarea face obiectul legislației UE privind protecția datelor.

Dreptul aplicabil prelucrării efectuate în cadrul activităților sediului irlandez este legislația irlandeză privind protecția datelor, indiferent dacă prelucrarea are loc în Portugalia, Italia sau alt stat membru.

Aceasta înseamnă că, potrivit acestei ipoteze, centrul de date din Ungaria ar trebui să respecte dreptul irlandez privind protecția datelor în ceea ce privește prelucrarea datelor cu caracter personal ale utilizatorilor furnizorului de servicii. Cu toate acestea, acest lucru nu aduce atingere aplicării dreptului maghiar în ceea ce privește prelucrarea diferită a datelor cu caracter personal de către centrul de date din Ungaria în legătură cu propriile activități – de exemplu, prelucrarea datelor cu caracter personal referitoare la angajații centrului de date.

În ceea ce privește sediile comerciale înființate pe teritoriul altor state membre, dacă activitatea acestora se limitează la campanii generale de publicitate care nu vizează utilizatorii și care nu implică prelucrarea datelor cu caracter personal ale utilizatorilor, acestea nu fac obiectul dreptului UE privind protecția datelor. Cu toate acestea, dacă sediile respective decid să prelucreze în cadrul activităților lor datele cu caracter personal ale persoanelor fizice din țara pe teritoriul căreia sunt stabilite (cum ar fi trimiterea de reclame țintă către anumiți utilizatori și posibili viitori utilizatori în scopuri comerciale proprii), acestea vor trebui să respecte dreptul intern privind protecția datelor.

În cazul în care nu poate fi stabilită o conexiune clară între prelucrarea datelor și sediul irlandez (suportul TIC este foarte limitat și nu există o implicare în prelucrarea datelor cu caracter personal), alte dispoziții ale directivei pot în continuare să determine aplicarea principiilor privind protecția datelor, de exemplu, dacă operatorul recurge la mijloace pe teritoriul UE. Acest lucru este analizat în capitolul III.3 de mai jos.

III.2. Operatorul este stabilit într-un loc în care se aplică dreptul intern al statului membru în temeiul dreptului internațional public [articolul 4 alineatul (1) litera (b)]

Articolul 4 alineatul (1) litera (b) abordează cazul mai rar întâlnit în care dreptul intern al unui stat membru privind protecția datelor se aplică atunci când „operatorul nu este stabilit pe teritoriul statului membru, ci într-un loc în care se aplică dreptul intern al acestuia, în temeiul dreptului internațional public”.

III.2.a) „…operatorul nu este stabilit pe teritoriul statului membru …”

Prima condiție trebuie interpretată ca însemnând, din motive de compatibilitate cu articolul 4 alineatul (1), că operatorul nu deține pe teritoriul statului membru un sediu care ar determina aplicabilitatea articolului 4 alineatul (1) litera (a) (a se vedea mai jos punctul III.3.a). Cu alte cuvinte, în absența unui sediu relevant pe teritoriul UE, nu poate

fi identificată nicio legislație națională privind protecția datelor în temeiul articolului 4 alineatul (1) litera (a).

III.2.b) „…, ci într-un loc în care se aplică dreptul intern al acestuia, în temeiul dreptului internațional public …”

Cu toate acestea, criteriile externe care rezultă din dreptul internațional public pot stabili, în situații specifice, gradul de aplicabilitate a dreptul intern privind protecția datelor în afara granițelor naționale. Acesta poate fi cazul în care dreptul internațional public sau acordurile internaționale stabilesc dreptul aplicabil în cadrul unei ambasade sau al unui consulat, sau dreptul aplicabil unei nave sau unui avion. În acele cazuri în care operatorul este stabilit în unul dintre aceste locuri specifice, dreptul intern aplicabil în ceea ce privește protecția datelor va fi determinat de dreptul internațional.

Cu toate acestea, este important să se sublinieze, de asemenea, că dreptul intern privind protecția datelor poate să nu se aplice misiunilor străine sau organizațiilor internaționale de pe teritoriul UE în măsura în care acestea beneficiază de un statut special în temeiul dreptului internațional în general sau prin intermediul unui acord referitor la sediu: o astfel de exonerare ar împiedica aplicarea articolului 4 alineatul (1) litera (a) pentru misiunea sau organizația internațională în cauză.

Exemplul nr. 6: Ambasade străine

Ambasada unui stat membru al UE în Canada face obiectul dreptului intern al statului membru respectiv privind protecția datelor și nu al dreptului canadian privind protecția datelor.

Ambasada oricărei țări a UE pe teritoriul Țărilor de Jos nu face obiectul dreptului olandez privind protecția datelor, întrucât orice ambasadă dispune de un statut special în temeiul dreptului internațional. Violarea securității datelor în cadrul activităților ambasadei în cauză nu ar determina, prin urmare, aplicarea dreptului olandez privind protecția datelor și nici măsurile executorii ulterioare.

O organizație neguvernamentală care are sedii pe teritoriul statelor membre ale UE nu ar beneficia, în principiu, de o exonerare similară decât în cazul în care acest lucru este prevăzut în mod explicit în cadrul unui acord internațional cu țara gazdă.

III.3. Operatorul nu este stabilit pe teritoriul Comunității, însă prelucrează datele prin intermediul mijloacelor situate pe teritoriul unui stat membru [articolul 4 alineatul (1) litera (c)]

Articolul 4 alineatul (1) litera (c) urmărește să asigure dreptul la protecția datelor cu caracter personal prevăzut de directiva UE, inclusiv în cazul în care operatorul nu este stabilit pe teritoriul UE/SEE, însă prelucrarea datelor cu caracter personal are o legătură clară cu teritoriul respectiv, astfel cum se arată la considerentul 20[22].

Articolul 4 alineatul (1) litera (c) prevede aplicarea dreptului intern al unui stat membru în cazul în care „*operatorul nu este stabilit pe teritoriul Comunității, dar în scopul prelucrării datelor cu caracter personal recurge la mijloace automate sau neautomate,*

[22] Considerentul 20: „*Întrucât faptul că prelucrarea datelor este efectuată de o persoană stabilită într-o țară terță nu trebuie să împiedice protecția persoanelor prevăzută în prezenta directivă; întrucât, în aceste cazuri, prelucrarea este reglementată de legislația statelor membre în care sunt amplasate mijloacele de prelucrare și trebuie să existe garanții că drepturile și obligațiile prevăzute în prezenta directivă sunt respectate în practică*”

situate pe teritoriul statului membru respectiv, cu excepția cazului în care aceste mijloace sunt folosite numai în vederea tranzitului pe teritoriul Comunității".

Această dispoziție este în special relevantă în lumina progresului noilor tehnologii, în special în ceea ce privește internetul, care facilitează colectarea și prelucrarea la distanță a datelor cu caracter personal, indiferent de prezența fizică a operatorului pe teritoriul UE/SEE[23].

a) „… operatorul nu este stabilit pe teritoriul Comunității …"

Această dispoziție devine relevantă în cazul în care prezența operatorului pe teritoriul UE/SEE nu poate fi considerată drept sediu în temeiul articolului 4 alineatul (1) litera (a) din directivă, astfel cum se analizează mai sus.

Este important să se clarifice interpretarea formulării „nu este stabilit". Trebuie să fie clar faptul că articolul 4 alineatul (1) litera (c) se aplică doar în cazul în care articolul 4 alineatul (1) litera (a) nu este aplicabil: și anume, în cazul în care operatorul nu are un sediu *relevant pentru activitățile în cauză* pe teritoriul UE/SEE. În consecință, faptul că un operator stabilit în afara UE/SEE recurge la mijloace într-un stat membru A pe teritoriul căruia nu este stabilit nu determină aplicabilitatea dreptului intern al statului membru respectiv dacă operatorul are deja un sediu în statul membru B și prelucrează datele cu caracter personal în cadrul activităților sediului respectiv. Atât prelucrarea din statul membru A (în care sunt folosite mijloacele), cât și cea din statul membru B (în care se află sediul) vor face obiectul dreptului intern al statului membru B. Acest aspect a fost clarificat de către grupul de lucru în avizul său privind aspectele referitoare la protecția datelor legate de motoarele de căutare[24].

Pe de altă parte, articolul 4 alineatul (1) litera (c) se va aplica în cazul în care operatorul are un sediu „irelevant" pe teritoriul UE. Cu alte cuvinte, operatorul are mai multe sedii pe teritoriul UE, însă activitățile acestora *nu sunt legate de prelucrarea datelor cu caracter personal*. Sediile respective nu determină aplicarea articolului 4 alineatul (1) litera (a).

Aceasta înseamnă că, de vreme ce nu ar trebui să existe lacune sau incoerențe în ceea ce privește aplicarea dispozițiilor directivei, aplicarea criteriului privind „mijloacele" nu trebuie să fie împiedicată de sediile irelevante: aceasta poate fi împiedicată de existența unui sediu doar în măsura în care sediul respectiv prelucrează date cu caracter personal în cadrul aceleași activități.

O consecință a acestei interpretări este aceea că o întreprindere care desfășoară activități diverse poate declanșa aplicarea articolului 4 alineatul (1) litera (a) și a articolului 4 alineatul (1) litera (c) dacă a recurs la mijloace și a deținut sedii în diferite contexte. Cu alte cuvinte, un operator stabilit în afara UE/SEE care recurge la mijloace situate pe teritoriul UE ar trebui să respecte articolul 4 alineatul (1) litera (c) chiar dacă a avut un sediu pe teritoriul UE atât timp cât la sediul în cauză s-au prelucrat date cu caracter personal *în cadrul altor activități*. Sediul respectiv ar determina aplicarea articolului 4 alineatul (1) litera (a) pentru aceste activități specifice.

---

23 A se vedea documentul grupului de lucru privind stabilirea aplicării la nivel internațional a dreptului UE privind protecția datelor în ceea ce privește prelucrarea online a datelor cu caracter personal de către site-urile internet situate în afara UE (WP 56).

24 Avizul 1/2008 al Grupului de lucru instituit în temeiul articolului 29, privind aspectele de protecție a datelor legate de motoarele de căutare (WP 148).

O oportunitate de clarificare a domeniului de aplicare a articolului 4 alineatul (1) litera (c) și a ceea ce trebuie să se înțeleagă prin „operatorul nu este stabilit pe teritoriul Comunității" poate surveni pe parcursul revizuirii cadrului privind protecția datelor, în conformitate cu spiritul directivei și formularea considerentului 20. Preambulul directivei prevede în mod clar că obiectivul constă în protejarea persoanelor fizice și evitarea lacunelor în ceea ce privește aplicarea principiilor. Din acest motiv, grupul de lucru consideră că articolul 4 alineatul (1) litera (c) ar trebui să se aplice în cazurile în care nu există un sediu pe teritoriul UE/SEE *care să determine aplicarea articolului 4 alineatul (1) litera (a)* sau în care prelucrarea *nu este efectuată în cadrul* activităților unui astfel de sediu.

b) „…, dar în scopul prelucrării datelor cu caracter personal recurge la mijloace automate sau neautomate, situate pe teritoriul statului membru…"

Elementul esențial care determină aplicabilitatea acestui articol și, prin urmare, a dreptului intern al unui stat membru privind protecția datelor este recurgerea la mijloace situate pe teritoriul statului membru respectiv.

Grupul de lucru a clarificat deja faptul că noțiunea de a „recurge" presupune două elemente: un anumit tip de activitate a operatorului și intenția clară a acestuia de a prelucra datele cu caracter personal[25]. Prin urmare, în timp ce nu toate tipurile de utilizare a mijloacelor în cadrul UE/SEE conduc la aplicarea directivei, nu este necesar ca operatorul să își exercite dreptul de proprietate sau întregul control asupra mijloacelor pentru prelucrarea care intră sub incidența directivei.

Trebuie amintit faptul că există o diferență între cuvântul utilizat în versiunea în limba engleză a articolului 4 alineatul (1) litera (c), „echipamente", și cuvântul utilizat în alte versiuni lingvistice ale articolului 4 alineatul (1) litera (c), care se apropie mai mult de cuvântul „mijloace" din limba engleză. De asemenea, terminologia utilizată în alte versiuni lingvistice ale articolului 4 alineatul (1) litera (c) este compatibilă cu formularea de la articolul 2 litera (d) care definește operatorul: persoana care stabilește scopurile și „mijloacele" prelucrării.

Având în vedere considerațiile de mai sus, grupul de lucru înțelege cuvântul „echipamente" drept „mijloace"[26]. De asemenea, acesta remarcă faptul că, în conformitate cu directiva, mijloacele pot fi „automate sau neautomate".

Aceasta conduce la o interpretare largă a criteriului, care include, prin urmare, intermediarii umani și/sau tehnici, cum se întâmplă în cadrul anchetelor sau al investigațiilor. În consecință, criteriul se aplică colectării de informații care utilizează chestionare, cum este cazul, de exemplu, al anumitor teste farmaceutice.

Apare întrebarea dacă activitățile de externalizare, desfășurate pe teritoriul UE/SEE în special de către persoanele împuternicite în numele operatorilor stabiliți în afara SEE pot fi considerate drept „mijloace". Interpretarea largă promovată mai sus conduce la un răspuns pozitiv, cu condiția ca persoanele împuternicite de către operator să nu acționeze în cadrul activităților operatorului cu sediul pe teritoriul SEE – caz în care s-ar aplica articolul 4 alineatul (1) litera (a). Cu toate acestea, trebuie luate în considerare

[25] WP56, op. cit.

[26] De asemenea, trebuie amintit faptul că textul în limba engleză al directivei din versiunile anterioare (de exemplu, în propunerea modificată din 1992 - COM (92) 422 final) utiliza, în egală măsură, termenul „mijloace", chiar dacă acesta a fost modificat în cursul negocierilor, într-o etapă ulterioară, fiind înlocuit cu termenul „echipamente", astfel cum se poate observa în textul poziției comune din martie 1995.

consecinţele uneori nedorite ale unei astfel de interpretări, astfel cum sunt cele dezvoltate la punctul III.4 de mai jos: dacă operatorii stabiliţi în diferite ţări din lume prelucrează datele pe teritoriul unui stat membru al UE, acolo unde sunt situate bazele de date şi persoana împuternicită de către operator, operatorii în cauză vor trebui să respecte dreptul intern privind protecţia datelor al statului membru respectiv.

Este necesară o evaluare de la caz la caz în care să se analizeze modul în care sunt utilizate în fapt mijloacele pentru colectarea şi prelucrarea datelor cu caracter personal. Din aceste motive, grupul de lucru a recunoscut posibilitatea ca o colectare a datelor cu caracter personal prin intermediul calculatoarelor utilizatorilor, cum este cazul, de exemplu, al aşa-numitelor „cookies" sau „bannere" Javascript, să determine aplicarea articolului 4 alineatul (1) litera (c) şi, prin urmare, a dreptului UE privind protecţia datelor pentru furnizorii de servicii stabiliţi în ţări terţe[27].

Această interpretare a dispoziţiei „recurge la mijloace" favorizează un domeniu larg de aplicare. Cu toate acestea, astfel cum s-a menţionat anterior, această interpretare subliniază, de asemenea, anumite consecinţe care nu sunt satisfăcătoare în momentul în care rezultatul constă în faptul că dreptul european privind protecţia datelor este aplicabil în cazurile în care există o conexiune limitată cu UE (de exemplu, un operator stabilit în afara UE prelucrează datele rezidenţilor non-UE doar prin intermediul mijloacelor de pe teritoriul UE). Există în mod evident necesară mai multă claritate şi condiţii suplimentare privind aplicarea acestui criteriu pentru a oferi o mai mare siguranţă viitorului cadru de protecţie a datelor. Acest punct va fi dezvoltat mai jos în partea de concluzii a prezentului document.

Ca altă ilustrare, măsura în care terminalele de telecomunicaţii sau părţi din acestea ar trebui considerate drept mijloace nu este clară. Faptul că instrumentul este proiectat sau utilizat în principal pentru colectarea sau prelucrarea ulterioară a datelor cu caracter personal poate fi considerat drept un indicator în acest sens. Cu toate acestea, faptul că un operator colectează în mod conştient datele cu caracter personal, chiar şi în mod incidental, prin folosirea anumitor mijloace în cadrul UE, determină, de asemenea, aplicarea directivei.

Exemplul 7: Servicii de localizare geografică

O întreprindere localizată în Noua Zeelandă utilizează automobile la nivel mondial, inclusiv în statele membre ale UE, pentru a colecta informaţii privind punctele de acces Wi-Fi (inclusiv informaţii privind echipamentele terminale private ale persoanelor fizice), cu scopul de a furniza clienţilor săi un serviciu de localizare geografică. O astfel de activitate implică, în numeroase cazuri, prelucrarea datelor cu caracter personal.

Aplicarea Directivei privind protecţia datelor va fi determinată în două moduri:
- În primul rând, automobilele care colectează informaţii Wi-Fi în timpul circulaţiei pe străzi pot fi considerate drept mijloace în temeiul articolului 4 alineatul (1) litera (c);
- În al doilea rând, în timpul furnizării serviciului de localizare geografică către persoanele fizice, operatorul va utiliza, de asemenea, dispozitivul mobil al persoanelor fizice în cauză (prin intermediul software-ului dedicat instalat în interiorul dispozitivului) drept echipament pentru furnizarea de informaţii reale privind locaţia dispozitivului şi a utilizatorului său.

Atât colectarea informaţiilor în vederea furnizării serviciului, cât şi furnizarea serviciului de localizare geografică vor trebui să respecte dispoziţiile directivei.

[27] WP56, op. cit., p. 10, litera (f).

Exemplul nr. 8: Informatică dematerializată

În cazul în care datele cu caracter personal sunt prelucrate și stocate în servere în diferite părți ale lumii, informatica dematerializată este un exemplu complex pentru aplicarea dispozițiilor directivei. Locul exact în care sunt situate datele nu este întotdeauna cunoscut și se poate modifica în timp, dar acest lucru nu este decisiv în identificarea dreptului aplicabil. Este suficient ca operatorul să efectueze prelucrarea în cadrul unui sediu de pe teritoriul UE sau ca mijloacele relevante să fie situate pe teritoriul UE pentru a determina aplicarea dreptului UE, astfel cum se prevede la articolul 4 alineatul (1) litera (c) din directivă.

Primul pas decisiv va consta în identificarea operatorului și a activităților care au loc la un anumit nivel. Pot fi identificate două perspective:

Utilizatorul serviciului de dematerializare este un operator de date: de exemplu, o întreprindere utilizează un serviciu de agendă online pentru a organiza anumite reuniuni cu clienții. În cazul în care întreprinderea utilizează serviciul în cadrul activităților sediului său de pe teritoriul UE, dreptul aplicabil acestei prelucrări de date prin intermediul agendei online va fi dreptul UE, în temeiul articolului 4 alineatul (1) litera (a). Întreprinderea trebuie să se asigure că serviciul oferă garanții adecvate de protecție a datelor, în special în ceea ce privește securitatea datelor cu caracter personal stocate în nor. De asemenea, aceasta trebuie să-și informeze clienții în legătură cu scopul și condițiile de utilizare a datelor lor.

În anumite circumstanțe, furnizorul de servicii de dematerializare poate, de asemenea, să fie operator de date: acesta ar fi cazul în care furnizorul pune la dispoziție o agendă online în care entitățile private își pot încărca toate programările personale și oferă servicii cu valoare adăugată, cum ar fi sincronizarea programărilor și a contactelor. În cazul în care furnizorul de servicii de dematerializare recurge la mijloace situate pe teritoriul UE, acesta va face obiectul dreptului UE privind protecția datelor în temeiul articolului 4 alineatul (1) litera (c). Astfel cum se arată mai jos, aplicarea directivei nu ar fi determinată de mijloacele folosite numai în vederea tranzitului, ci de mijloace mai specifice, de exemplu, dacă serviciul utilizează facilități de calculare, scripturi java sau instalează cookies în vederea stocării și recuperării datelor cu caracter personal ale utilizatorilor. Furnizorul de servicii de dematerializare va trebui apoi să furnizeze utilizatorilor informații privind modul în care sunt prelucrate, stocate și posibil accesate datele de către terți și să garanteze măsurile corespunzătoare de securitate pentru a proteja informațiile respective.

Exemplul nr. 9: Operatorul publică listele cu pedofili pentru fiecare țară în parte

Un operator stabilit într-un stat membru al UE/SEE publică liste cu persoanele suspectate sau acuzate de infracțiuni împotriva minorilor pentru fiecare țară în parte. În ceea ce privește dreptul la protecția datelor cu caracter personal al persoanelor enumerate, dreptul aplicabil – în temeiul căruia ar trebui evaluată legalitatea acestei prelucrări – este dreptul intern privind protecția datelor al statului membru în care este stabilit operatorul.

Este irelevant pentru stabilirea dreptului aplicabil privind protecția datelor dacă operatorul utilizează mijloace situate în alte state membre (cum ar fi serverele internet cu diferite nume de domenii de nivel 1, inclusiv .fr., .it, .pl. etc.) sau dacă activitățile sale îi vizează direct pe cetățenii din alte țări ale UE (de exemplu, prin publicarea unor

liste cu nume specifice unor anumite ţări în limba ţărilor respective) în prelucrarea datelor în acest scop.

Autorităţii de supraveghere a statului membru în care se află sediul i se poate solicita, în orice caz, de către celelalte autorităţi de supraveghere să coopereze prin luarea de măsuri în urma primirii unei plângeri din partea persoanelor fizice situate pe teritoriul altor state membre.

Bineînţeles, pot fi aplicate criterii diferite de legătură şi, prin urmare, dreptul aplicabil în alte domenii juridice, cum ar fi, de exemplu, acţionarea în justiţie pentru defăimare în conformitate cu dreptul penal sau civil.

c) „…cu excepţia cazului în care aceste mijloace sunt folosite numai în vederea tranzitului pe teritoriul Comunităţii…”

Aplicarea dreptului intern al unui stat membru al UE este exclusă în cazul în care mijloacele folosite de către operator şi situate pe teritoriul statului membru respectiv sunt folosite numai în vederea asigurării tranzitului pe teritoriul Uniunii, cum ar fi, de exemplu, cazul reţelelor (cablurilor) de telecomunicaţii sau al serviciilor poştale care nu fac decât să asigure tranzitul comunicaţiilor pe teritoriul Uniunii pentru a ajunge la ţările terţe.

Întrucât aceasta constituie o excepţie de la criteriul privind mijloacele, ea trebuie să facă obiectul unei interpretări mai restrânse. Trebuie amintit faptul că aplicarea efectivă a acestei excepţii devine din ce în ce mai rară: în practică, tot mai multe servicii de telecomunicaţii combină simplul tranzit şi serviciile cu valoare adăugată, inclusiv, de exemplu, filtrarea mesajelor electronice nesolicitate sau alte manipulări de date cu ocazia transmiterii acestora. Simpla transmisie prin cablu „punct la punct” începe treptat să dispară. Acest lucru nu trebuie pierdut din vedere la momentul revizuirii cadrului privind protecţia datelor.

d) „… trebuie să desemneze un reprezentant stabilit pe teritoriul statului membru …” [articolul 4 alineatul (2)]

Directiva obligă operatorul să desemneze „un reprezentant” pe teritoriul statului membru al cărui drept intern este aplicabil în temeiul folosirii de către operator a mijloacelor situate pe teritoriul statului membru respectiv în vederea prelucrării datelor cu caracter personal. Acest lucru se întâmplă „fără să aducă atingere acţiunilor în justiţie care ar putea fi introduse împotriva operatorului însuşi”.

În acest ultim caz, problema acţionării în justiţie a reprezentantului aduce în discuţie aspecte practice, astfel cum o arată experienţa statelor membre. Acesta ar fi cazul, de exemplu, în care singurul reprezentant al operatorului pe teritoriul UE este un cabinet de avocatură. În dreptul intern de punere în aplicare nu există un răspuns uniform la întrebarea dacă reprezentantul poate fi tras la răspundere şi sancţionat din punct de vedere civil sau penal în numele operatorului. Natura relaţiei dintre reprezentant şi operator este, în acest caz, decisivă. În anumite state membre, reprezentantul înlocuieşte operatorul inclusiv în ceea ce priveşte punerea în aplicare şi sancţiunile, în timp ce în alte state membre acesta are doar un simplu mandat. Anumite legislaţii naţionale prevăd în

mod explicit amenzi aplicabile reprezentanților[28], în timp ce această posibilitate nu este avută în vedere de alte state membre[29].

În acest sens, este necesară armonizarea la nivel european, cu scopul de a eficientiza rolul reprezentantului. În special, persoanele vizate ar trebui să aibă posibilitatea de a-și exercita drepturile împotriva reprezentantului, fără să aducă atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului însuși.

III.4. Considerații privind consecințele practice ale aplicării articolului 4 alineatul (1) litera (c)

Un aspect decisiv privind aplicarea articolului 4 alineatul (1) litera (c) face referire la consecințele practice ale acestuia pentru operatorii de date. Chiar dacă operatorul de date este stabilit în afara UE/SEE, acesta va trebui să aplice principiile directivei dacă folosește mijloacele situate pe teritoriul UE pentru operațiunile de prelucrare a datelor cu caracter personal. Se poate pune întrebarea dacă principiile se aplică doar pentru partea operațiunii de prelucrare care este efectuată pe teritoriul UE sau pentru operator ca atare, pentru toate etapele prelucrării, inclusiv pentru cele care au loc într-o țară terță. Astfel de întrebări au o importanță semnificativă în mediile de rețea, cum ar fi informatica dematerializată sau în cadrul întreprinderilor multinaționale.

Să luăm în considerare, de exemplu, implicațiile pentru operatorii stabiliți în diferite țări din lume și care prelucrează datele în Franța, unde sunt localizate bazele de date și mijloacele de prelucrare. Dacă diverșii operatori utilizează infrastructura din Franța, articolul 4 alineatul (1) litera (c) este aplicabil, iar toți operatorii ar trebui să respecte dreptul francez. Acest lucru poate avea consecințe nedorite în ceea ce privește impactul economic și punerea în aplicare.

Din motive practice ar fi necesară o moderare a aplicării criteriilor privind „echipamentele/mijloacele", însă aceasta este contrabalansată de faptul că principiile privind protecția datelor vizează protejarea unui drept fundamental. Limitarea drepturilor persoanelor fizice la anumite părți din procesul de prelucrare a datelor acestora nu pare admisibilă. De asemenea, reducerea obiectivului privind protecția datelor la persoanele cu domiciliul în UE nu este acceptabilă deoarece o persoană beneficiază de dreptul fundamental privind protecția datelor cu caracter personal indiferent de naționalitate sau reședință. În consecință, criteriile articolului 4 alineatul (1) litera (c) au ca rezultat aplicarea principiilor directivei pentru operatorii ca atare, pentru toate etapele de prelucrare a datelor, inclusiv pentru cele care au loc într-o țară terță.

Aplicarea directivei pentru un operator, pentru întregul proces de prelucrare ar trebui susținută atât timp cât legătura cu UE este efectivă și nu insuficientă (cum ar fi folosirea mai mult neglijentă decât premeditată a mijloacelor pe teritoriul unui stat membru).

Având în vedere „vizarea" relevantă a persoanelor fizice, un factor de legătură mai specific drept completare la criteriile privind „echipamentele/mijloacele" poate fi util în ceea ce privește securitatea juridică, astfel cum se dezvoltă ulterior în concluzii. Un astfel

---

[28] Legea belgiană privind protecția datelor din 8 decembrie 1992, JO 18.3.1993; Actul olandez din 6 iulie 2000 privind protecția datelor cu caracter personal, Buletinul actelor, ordinelor și decretelor (Staatsblad) nr. 302, 20 iulie 2000. A se vedea, de asemenea, legislația elenă [articolul 3 alineatul (3) litera (b) coroborat cu articolul 21 alineatul (1) din Legea 2472/1997].

[29] Legea franceză 78/17 din 6 ianuarie 1978, de exemplu, nu prevede astfel de amenzi pentru reprezentanți.

de criteriu nu este nou, acesta fiind utilizat și în alte contexte în cadrul UE[30] și în legislația Statelor Unite privind protecția online a copiilor[31]. De asemenea, acesta este cazul anumitor legislații naționale care transpun Directiva 2000/31/CE privind comerțul electronic[32], conform căreia furnizorii care nu sunt stabiliți pe teritoriul SEE intră sub incidența legislațiilor naționale respective în momentul în care își îndreaptă serviciile în special către teritoriul lor.

Aplicarea unui criteriu similar pentru legislația privind protecția datelor în UE poate fi reflectată pe parcursul discuțiilor viitoare referitoare la revizuirea cadrului privind protecția datelor.

O altă consecință practică privind aplicarea articolului 4 alineatul (1) litera (c) vizează interacțiunea dintre această dispoziție și articolele 25 și 26 din directivă. Faptul că operatorul stabilit în afara UE/SEE folosește mijloace situate pe teritoriul UE/SEE – prin urmare, trebuie să respecte toate dispozițiile relevante ale directivei – implică, de asemenea, aplicarea posibilă a articolelor 25 și 26. Cu toate acestea, implicațiile exacte ale unui astfel de scenariu pot fi dificil de stabilit în practică.

De exemplu, dacă un operator X cu sediul în afara SEE colectează date cu caracter personal prin intermediul mijloacelor localizate pe teritoriul UE (de exemplu, prin folosirea așa-numitelor „cookies" sau prin intermediul unei persoane împuternicite), acesta trebuie să respecte directiva în toate etapele de prelucrare. În acest caz, există o anumită paralelă cu situația în care un operator stabilit pe teritoriul SEE transferă date cu caracter personal către o persoană împuternicită situată în afara SEE: de asemenea, în acest caz, operatorul și persoana împuternicită stabiliți în afara teritoriului SEE vor avea anumite obligații în temeiul directivei. Cu toate acestea, modul în care sunt puse în practică aceste principii în temeiul cerințelor de conformitate ale articolelor 25 și 26 din directivă în scenariul de la articolul 4 alineatul (1) litera (c) referitor la operatorul stabilit în afara SEE nu este complet clar. Grupul de lucru consideră că instrumentele existente care reglementează condițiile privind transferurile ar trebui analizate ulterior pentru a acoperi mai bine această situație.

III.5. Dreptul aplicabil măsurilor de securitate [articolul 17 alineatul (3)]

Articolul 17 alineatul (3) prevede că contractul sau actul juridic care leagă persoana împuternicită de operator trebuie să asigure, de asemenea, respectarea măsurilor de securitate „*așa cum sunt definite de legislația statului membru în care este stabilită persoana împuternicită*".

Motivul care stă la baza acestui principiu constă în asigurarea unor cerințe uniforme în cadrul aceluiași stat membru cu privire la măsurile de securitate, precum și facilitarea punerii în aplicare. Cu toate acestea, trebuie amintit că, din perspectivă europeană,

---

30 Conform articolului 15 alineatul (1) litera (c) din Regulamentul (CE) nr. 44/2001 al Consiliului din 22 decembrie 2000 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială (JO L 12, 16.1.2001, p.1), iar pentru interpretarea sa a se vedea concluziile avocatului general Trstenjak, 18 mai 2010, în C-144/09, *Hotel Alpenhof* .

31 Aplicarea COPPA poate fi într-adevăr determinată de stabilirea unui editor pe teritoriul S.U.A. sau de faptul că site-ul internet vizează copiii din S.U.A.: site-urile internet străine și serviciile online trebuie să respecte regulamentul COPPA dacă acestea vizează, colectează sau divulgă în mod conștient informații cu caracter personal referitoare la copiii din Statele Unite. A se vedea 16 CFR 312.2, disponibilă la http://www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59912.

32 Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (Directiva privind comerțul electronic) JO L 178 , 17.7.2000, p.1

cerințele de securitate diferă considerabil de la un stat membru la altul: unele prevăd norme foarte detaliate, în timp ce altele nu au făcut decât să copieze formularea generală a directivei. În cazul în care legislațiile naționale sunt generale, iar formularea acestora este extrasă din directivă, acest lucru nu va avea consecințe practice. Persoana împuternicită nu va întâmpina probleme în ceea ce privește respectarea obligațiilor mai detaliate impuse de către operator în conformitate cu dreptul său intern sau, alternativ, un operator va accepta cu ușurință cerințele mai detaliate în temeiul dreptului persoanei împuternicite. Doar în cazurile în care normele detaliate sunt diferite sau conflictuale, articolul 17 alineatul (3) hotărăște în favoarea dreptului aplicabil persoanei împuternicite de către operator[33]. Cu toate acestea, se recomandă ca armonizarea ulterioară a obligațiilor privind securitatea să fie inclusă în obiectivul discuțiilor referitoare la revizuirea cadrului privind protecția datelor.

III.6. Competențele și cooperarea autorităților de supraveghere [articolul 28 alineatul (6)]

Astfel cum se menționează mai sus (a se vedea punctul II.2.e), articolul 28 alineatul (6) are ca scop reducerea decalajului posibil dintre dreptul aplicabil și competența judiciară de supraveghere care poate rezulta în domeniul protecției datelor pe piața internă.

În conformitate cu această dispoziție, autoritățile naționale pentru protecția datelor au competența de a supraveghea punerea în aplicare a legislației privind protecția datelor pe teritoriul statului membru unde își au sediul, însă dacă dreptul intern al unui alt stat membru ar fi aplicabil pe teritoriul lor, puterile executorii ale autorităților pentru protecția datelor nu ar fi limitate: criteriile privind dreptul aplicabil ale directivei prevăd posibilitatea ca autoritatea pentru protecția datelor să fie autorizată să verifice și să intervină în operațiunile de prelucrare care sunt efectuate pe teritoriul său, chiar dacă dreptul aplicabil este dreptul unui alt stat membru.

III.6.a) „…fiecare autoritate de supraveghere are competența, indiferent de dreptul intern aplicabil…”

Această dispoziție abilitează autoritățile naționale de supraveghere să acționeze întotdeauna în limitele jurisdicției teritoriale, indiferent dacă dreptul aplicabil este dreptul lor intern privind protecția datelor sau dreptul intern al unui alt stat membru privind protecția datelor.

III.6.b) „…să exercite pe teritoriul statului membru din care provin competențele…”

De asemenea, în cazul în care este aplicabil dreptul intern al unui alt stat membru privind protecția datelor, fiecare autoritate de supraveghere are competența să exercite pe teritoriul statului membru din care provine competențele conferite de sistemul juridic intern. Aceasta include puterile de investigație, puterile de intervenție, puterea de a participa la procedurile juridice, puterea de a impune sancțiuni.

În cazul în care sunt implicate mai multe autorități pentru protecția datelor, inclusiv autoritatea locală pentru protecția datelor și autoritățile pentru protecția datelor al căror drept intern este dreptul aplicabil, este esențială organizarea cooperării și clarificarea rolului fiecărei autorități pentru protecția datelor. Prin urmare, trebuie soluționate anumite aspecte, inclusiv:

[33] S-ar evita astfel numirea unei persoane împuternicite în altă țară cu obligații reduse care ar fi considerate drept o încălcare a obligațiilor operatorului de date.

- aspectele procedurale, cum ar fi identificarea autorității principale, precum și modul în care aceasta urmează că colaboreze cu alte autorități pentru protecția datelor;
- domeniul de aplicare a competențelor care urmează să fie exercitate de fiecare autoritate pentru protecția datelor. În special, în ce măsură își va exercita autoritatea locală pentru protecția datelor puterile cu privire la aplicarea principiilor de fond și a sancțiunilor? Ar trebui aceasta să-și limiteze puterile la verificarea faptelor sau poate să adopte măsuri provizorii de executare sau chiar măsuri definitive? Poate autoritatea locală pentru protecția datelor oferi propria interpretare a dispozițiilor de drept aplicabil sau aceasta este o competență a autorității pentru protecția datelor din statul membru al cărui drept intern este dreptul aplicabil? Trebuie amintit în acest sens că nu toate legislațiile naționale prevăd posibilitatea de a impune sancțiuni tuturor părților interesate[34].

Un nivel ridicat de armonizare a puterilor de supraveghere conferite autorităților de supraveghere în conformitate cu articolul 28 din directivă este condiția esențială pentru a garanta respectarea protecției transfrontaliere a datelor într-un mod eficient și nediscriminatoriu. Acest aspect merită o analiză ulterioară, grupul de lucru urmând să ofere orientări în acest sens într-un document separat.

Exemplul nr. 10: Prelucrarea transfrontalieră în interiorul UE a datelor cu caracter personal

Prelucrarea datelor este efectuată în Regatul Unit, însă în cadrul activităților operatorului cu sediul pe teritoriul Germaniei. Aceasta are următoarele consecințe:

- dreptul german va fi dreptul aplicabil prelucrării din Regatul Unit;
- autoritatea britanică pentru protecția datelor trebuie să aibă competența de a inspecta sediile de pe teritoriul Regatului Unit și de a trage anumite concluzii pe care să le comunice apoi către autoritatea germană pentru protecția datelor;
- autoritatea germană pentru protecția datelor ar trebui să aibă posibilitatea de a impune sancțiuni operatorului stabilit pe teritoriul Germaniei în baza concluziilor transmise de autoritatea britanică pentru protecția datelor.

Ca element suplimentar, daca sediul din Regatul Unit este o persoană împuternicită de către operator, aspectele privind securitatea prelucrării fac obiectul cerințelor dreptului britanic privind protecția datelor. Aceasta conduce apoi la întrebarea cum pot fi puse în aplicare în mod corespunzător cerințele dreptului respectiv.

III.6.c) „…cooperează în măsura necesară îndeplinirii îndatoririlor lor…”

Autoritățile de supraveghere au obligația de a coopera („cooperează”), dar, în același timp, această obligație este limitată la ceea ce este necesar pentru a-și îndeplini îndatoririle. Prin urmare, cererile de cooperare trebuie corelate cu exercitarea competențelor lor și, de obicei, cu cazurile transfrontaliere relevante.

Dispoziția face referire în special la schimbul de „informații utile”, care poate fi corelat, de exemplu, cu informațiile privind dispozițiile relevante și instrumentele juridice aplicabile unui caz specific. Cu toate acestea, cooperarea poate avea loc la diferite niveluri: gestionarea plângerilor transfrontaliere, colectarea probelor pentru alte autorități pentru protecția datelor sau impunerea de sancțiuni.

[34] Legea elenă, de exemplu, prevede sancțiuni doar pentru operatorii de date și reprezentanții acestora, nu și pentru persoanele împuternicite de către operator.

Chestiunea este și mai acută într-un context internațional în care operatorii de date operează la nivel mondial, solicitând îmbunătățiri în ceea ce privește cooperarea pentru aplicarea legislației. Inițiative precum „Rețeaua globală de aplicare a dreptului la viață privată (GPEN)”, care implică autorități responsabile de protecția datelor de pe diverse continente, reprezintă un pas necesar și binevenit în acest sens.

Exemplul nr. 11: Rețeaua socială are sediul principal într-o țară terță și un sediu pe teritoriul UE

O platformă de rețele sociale are sediul principal într-o țară terță și un sediu pe teritoriul unui stat membru. Sediul definește și pune în aplicare politici referitoare la prelucrarea datelor cu caracter personal ale rezidenților UE. Rețeaua socială vizează în mod activ rezidenți din toate statele membre ale UE, ceea ce constituie o porțiune semnificativă a clienților și veniturilor sale. Aceasta instalează, de asemenea, „cookies” pe calculatoarele utilizatorilor din UE.

În acest caz, în conformitate cu articolul 4 alineatul (1) litera (a), dreptul aplicabil va fi dreptul privind protecția datelor al statului membru pe teritoriul căruia este stabilită întreprinderea în cadrul UE. Întrebarea dacă rețeaua socială recurge la mijloacele situate pe teritoriul unui alt stat membru este irelevantă, întrucât prelucrarea are loc în cadrul activităților unui singur sediu, iar directiva exclude aplicarea cumulativă a articolului 4 alineatul (1) litera (a) și a articolului 4 alineatul (1) litera (c).

Cu toate acestea, autoritatea de supraveghere a statului membru în care este stabilită rețeaua socială pe teritoriul UE va fi obligată – în conformitate cu articolul 28 alineatul (6) – să coopereze cu alte autorități de supraveghere, de exemplu, pentru a soluționa cererile sau plângerile trimise de rezidenții din alte state ale UE.

Exemplul nr. 12: Platforma europeană de servicii de sănătate online

Se creează o platformă la nivel european pentru a facilita prelucrarea transfrontalieră a registrelor medicale ale pacienților. Platforma permite schimbul de seturi de date privind fișele, registrele medicale și rețetele pacienților cu scopul de a facilita serviciile medicale pe perioada călătoriilor.

În timp ce platforma facilitează schimbul de informații, datele pacienților vor fi prelucrate în continuare în cadrul activităților unuia sau mai multor sedii de pe teritoriul unui anumit stat membru. De exemplu, dacă un rezident bulgar care călătorește în Portugalia necesită tratament de urgență, registrul său medical va fi prelucrat prin intermediul platformei de către serviciile medicale din Portugalia în conformitate cu dreptul portughez privind protecția datelor. Dacă la întoarcerea în Bulgaria pacientul dorește să depună o plângere referitoare la prelucrarea datelor sale de către operatorul portughez, acesta trebuie înainte de toate să trimită plângerea către autoritatea pentru protecția datelor din Bulgaria. Autoritățile bulgare pentru protecția datelor vor colabora apoi cu autoritățile portugheze pentru protecția datelor pentru a stabili faptele și pentru a verifica dacă a existat o încălcare în temeiul legislației portugheze.

În cazul în care Comisia Europeană intervine în funcționarea platformei prin organizarea fluxurilor de date cu caracter personal și prin garantarea securității sistemului, aceasta poate fi considerată, de asemenea, drept prelucrare a datelor cu caracter personal, fapt care ar declanșa aplicarea Regulamentului (CE) nr. 45/2001. În acest exemplu, dacă cetățeanul de origine bulgară a depus o plângere referitoare la încălcarea securității datelor sale medicale, autoritățile bulgare pentru protecția datelor vor colabora apoi cu AEPD pentru a identifica condițiile și consecințele încălcării.

IV. Concluzii

Prezentul aviz vizează clarificarea domeniului de aplicare a Directivei 95/46/CE, în special în ceea ce privește articolul 4 din directivă. De asemenea, avizul evidențiază anumite domenii care pot suferi îmbunătățiri ulterioare. Principalele rezultate în acest sens sunt sintetizate în continuare.

IV.1. Clarificarea dispozițiilor actuale

Stabilirea aplicării dreptului UE în ceea ce privește prelucrarea datelor cu caracter personal servește la clarificarea domeniului de aplicare a dreptului UE privind protecția datelor atât în cadrul UE/SEE, cât și într-un context internațional mai larg. Înțelegerea clară a dreptului aplicabil va contribui la asigurarea securității juridice pentru operatori și a unui cadru clar pentru persoanele fizice și alte părți interesate. De asemenea, înțelegerea corectă a dispozițiilor privind dreptul aplicabil ar trebui să asigure absența lacunelor privind nivelul ridicat de protecție a datelor cu caracter personal prevăzut de Directiva 95/46.

Dispoziția esențială privind dreptul aplicabil o constituie articolul 4, care stabilește dreptul (drepturile) intern(e) privind protecția datelor adoptat(e) în temeiul directivei aplicabil(e) în ceea ce privește prelucrarea datelor cu caracter personal.

În conformitate cu articolul 4 alineatul (1) litera (a), un stat membru trebuie să aplice dreptul intern privind protecția datelor în cazul în care prelucrarea este efectuată în cadrul activităților operatorului cu sediul pe teritoriul statului membru respectiv. Esențial pentru identificarea sediului relevant în temeiul articolului 4 alineatul (1) litera (a) este faptul dacă organizarea în cauză conduce la exercitarea efectivă și reală a activităților. În plus, trimiterea la „un" sediu înseamnă că aplicabilitatea dreptului unui stat membru este determinată de situarea sediului operatorului pe teritoriul statului membru respectiv, în timp ce aplicabilitatea drepturilor interne ale altor state membre poate fi determinată de situarea altor sedii aparținând aceluiași operator în statele membre respective.

Noțiunea „în cadrul activităților" – și nu locația datelor – este un factor esențial în identificarea domeniului de aplicare a dreptului aplicabil. Noțiunea „în cadrul activităților" presupune că dreptul aplicabil nu este dreptul statului membru în care este stabilit *operatorul*, ci al statului membru în care în cadrul *sediului* operatorului se desfășoară *activități* care presupun prelucrarea datelor cu caracter personal. În acest context, gradul de implicare a sediului (sediilor) în cadrul activităților de prelucrare a datelor cu caracter personal este decisiv. În plus, trebuie avută în vedere natura activităților sediilor și necesitatea garantării protecției eficiente a drepturilor persoanelor fizice. Pentru analizarea acestor criterii trebuie avută în vedere o abordare funcțională: mai mult decât evaluarea teoretică efectuată de către părți în legătură cu dreptul aplicabil, comportamentul practic și interacțiunea acestora ar trebui să reprezinte factorii decisivi.

Articolul 4 alineatul (1) litera (b) abordează cazul mai rar întâlnit în care dreptul intern al unui stat membru privind protecția datelor se aplică atunci când „operatorul nu este stabilit pe teritoriul statului membru, ci într-un loc în care se aplică dreptul intern al acestuia, în temeiul dreptului internațional public". Criteriile externe care rezultă din dreptul internațional public pot stabili, în situații specifice, gradul de aplicabilitate a dreptului intern privind protecția datelor în afara granițelor naționale, cum se întâmplă, de exemplu, în cazul ambasadelor sau al navelor.

Articolul 4 alineatul (1) litera (c) urmărește să asigure dreptul la protecția datelor cu caracter personal prevăzut de directiva UE inclusiv în cazul în care operatorul nu este stabilit pe teritoriul UE/SEE, însă prelucrarea datelor cu caracter personal are o legătură clară cu teritoriul respectiv. Pentru a asigura compatibilitatea cu articolul 4 și pentru a evita lacunele în aplicarea dreptului privind protecția datelor, grupul de lucru consideră că aplicarea articolului 4 alineatul (1) litera (c) nu trebuie împiedicată de existența unui sediu al operatorului pe teritoriul Comunității în cazul în care sediul respectiv nu este relevant în temeiul articolului 4 alineatul (1) litera (a). În schimb, dispoziția „recurge la mijloace" a articolului 4 alineatul (1) litera (c) ar trebui să se aplice în cazurile în care nu există un sediu pe teritoriul UE/SEE *care să determine aplicarea articolului 4 alineatul (1) litera (a)* sau în care prelucrarea *nu este efectuată în cadrul* activităților desfășurate la un astfel de sediu.

Elementul esențial care determină aplicabilitatea articolului 4 alineatul (1) litera (c) și, prin urmare, a dreptului intern privind protecția datelor al unui stat membru este recurgerea la mijloace situate pe teritoriul statului membru respectiv. Conceptul de „recurgere" presupune două elemente: un anumit tip de activitate a operatorului și intenția clară a acestuia de a prelucra date cu caracter personal. Prin urmare, în timp ce nu toate tipurile de utilizare de mijloace în cadrul UE/SEE conduc la aplicarea directivei, nu este necesar ca operatorul să își exercite dreptul de proprietate sau întregul control asupra unor astfel de mijloace pentru prelucrarea care intră sub incidența directivei.

În ceea ce privește noțiunea de „echipamente", redarea sa prin intermediul expresiei „mijloace" în alte limbi ale UE ar conduce la o interpretare mai largă a criteriilor în cauză, favorizând un domeniu larg de aplicare. O astfel de interpretare poate, în unele cazuri, să aibă ca rezultat aplicarea dreptului european privind protecția datelor atunci când prelucrarea respectivă nu are o legătură reală cu teritoriul UE/SEE. În orice caz, prelucrarea datelor cu caracter personal de către un operator stabilit în afara UE/SEE, prin intermediul mijloacelor situate pe teritoriul UE/SEE, determină aplicarea directivei în conformitate cu articolul 4 alineatul (1) litera (c), ceea ce înseamnă că toate celelalte dispoziții relevante ale directivei vor fi, de asemenea, aplicabile.

Aplicarea legislației naționale a unui stat membru este exclusă în cazul în care mijloacele folosite de către operator și situate pe teritoriul statului membru respectiv sunt folosite numai în vederea asigurării tranzitului pe teritoriul Comunității, cum ar fi, de exemplu, cazul rețelelor (cablurilor) de telecomunicații sau al serviciilor poștale care nu fac decât să asigure tranzitul comunicațiilor pe teritoriul Comunității pentru a ajunge la țările terțe.

Articolul 4 alineatul (2) obligă operatorul să desemneze un reprezentant pe teritoriul statului membru al cărui drept intern este aplicabil în temeiul folosirii de către operator a mijloacelor pe teritoriul statului membru respectiv în vederea prelucrării datelor cu caracter personal. În acest ultim caz, acționarea în justiție a reprezentantului poate constitui o provocare.

Articolul 17 alineatul (3) prevede că contractul sau actul juridic care leagă persoana împuternicită de operator ar trebui să stipuleze, de asemenea, că persoana împuternicită trebuie să respecte măsurile de securitate „*definite de dreptul intern al statului membru pe teritoriul căruia este stabilită persoana împuternicită de către operator*". Motivul care stă la baza acestui principiu constă în asigurarea unor cerințe uniforme pe teritoriul unui stat membru în ceea ce privește măsurile de securitate și facilitarea punerii lor în aplicare.

Articolul 28 alineatul (6) are drept scop reducerea decalajului posibil dintre dreptul aplicabil și competența judiciară de supraveghere care poate rezulta în domeniul protecției datelor pe piața internă prin stabilirea faptului că o autoritate pentru protecția datelor ar trebui să aibă posibilitatea de a-și utiliza puterile de a verifica și a interveni în operațiunile de prelucrare care au loc pe teritoriul său, chiar dacă dreptul aplicabil este dreptul intern al unui alt stat membru.

IV.2. Îmbunătățirea dispozițiilor actuale

Deși indicațiile și exemplele dezvoltate mai sus ar trebui să contribuie la consolidarea securității juridice și a protecției drepturilor persoanelor fizice la momentul definirii dreptului aplicabil în materie de prelucrare a datelor cu caracter personal, pe parcursul dezvoltării acestora au fost identificate anumite deficiențe.

Formularea utilizată în directivă și coerența dintre diferitele secțiuni ale articolului 4 ar beneficia de pe urma clarificării ulterioare ca parte a revizuirii cadrului general privind protecția datelor. Grupul de lucru a identificat necesitatea unor clarificări ulterioare în mai multe domenii:

a. Este necesară abordarea incoerențelor dintre formularea utilizată la articolul 4 alineatul (1) litera (a) și articolul 4 alineatul (1) litera (c) referitoare la cuvântul „sediu" și noțiunea potrivit căreia operatorul „nu este stabilit" pe teritoriul UE. Pentru a fi coerent cu articolul 4 alineatul (1) litera (a), care utilizează criteriul privind „sediul", articolul 4 alineatul (1) litera (c) ar trebui să se aplice în toate cazurile în care nu există un *sediu* pe teritoriul UE *care să determine aplicarea articolului 4 alineatul (1) litera (a)* sau în care prelucrarea *nu este efectuată în cadrul* activităților unui astfel de sediu.

b. De asemenea, ar fi utilă o clarificare a noțiunii „în cadrul activităților" sediului. Grupul de lucru a subliniat importanța evaluării *gradului de implicare* a sediului (sediilor) în activitățile de prelucrare a datelor cu caracter personal sau, cu alte cuvinte, trebuie să se verifice „cine și ce face" în cadrul unui anumit sediu. Acest criteriu este interpretat pe baza lucrărilor de redactare a directivei și a obiectivului stabilit la momentul respectiv, și anume de a păstra abordarea distributivă a drepturilor interne aplicabile pentru diferitele sedii ale operatorului pe teritoriul UE. Grupul de lucru consideră că articolul 4 alineatul (1) litera (a) în vigoare conduce la o soluție fezabilă, deși uneori complexă, care pare să susțină o abordare mai centralizată și mai armonizată.

c. Modificarea avută în vedere pentru simplificarea normelor de stabilire a dreptului aplicabil ar consta într-o reorientare către principiul țării de origine: toate sediile unui operator din cadrul UE ar aplica, prin urmare, aceeași legislație, indiferent de teritoriul pe care sunt situate acestea. Din această perspectivă, situarea sediului principal al operatorului ar fi primul criteriu aplicat. Existența simultană a mai

multor sedii pe teritoriul UE nu ar declanșa aplicarea distributivă a drepturilor interne.

d. Cu toate acestea, acest lucru este acceptabil doar dacă nu există diferențe semnificative între drepturile interne ale statelor membre. Aplicarea efectivă a principiului țării de origine ar conduce, în caz contrar, la un fenomen de căutare a instanței celei mai favorabile („forum shopping") în beneficiul statelor membre ale căror drepturi interne sunt considerate drept permisive în ceea ce-i privește pe operatorii de date. Aceasta ar afecta, în mod evident, persoanele vizate. Securitatea juridică pentru operatorii de date și pentru persoanele vizate ar fi garantată doar dacă este atinsă o armonizare cuprinzătoare a legislațiilor naționale, inclusiv armonizarea obligațiilor în materie de securitate. Prin urmare, grupul de lucru susține armonizarea solidă a principiilor de protecție a datelor drept condiție a orientării posibile către principiul țării de origine.

e. Criterii suplimentare pot fi aplicabile în cazul în care operatorul este stabilit în afara UE, pentru a se asigura existența unei conexiuni suficiente cu teritoriul UE, evitându-se în același timp utilizarea teritoriului UE pentru desfășurarea activităților ilegale de prelucrare a datelor de către operatorii stabiliți pe teritoriul țărilor terțe. În acest sens, pot fi dezvoltate următoarele două criterii:

   – Vizarea persoanelor fizice sau „abordarea orientată spre servicii": aceasta ar presupune introducerea unui criteriu pentru aplicarea dreptului UE privind protecția datelor potrivit căruia activitatea care implică prelucrarea datelor cu caracter personal este orientată către persoanele fizice din cadrul UE. Acest criteriu ar trebui să constea în vizarea materială care are la bază sau care ia în considerare legătura efectivă dintre persoana vizată și o țară specifică a UE. Următoarele exemple ilustrează în ce poate consta vizarea respectivă: faptul că un operator de date colectează date cu caracter personal în cadrul serviciilor accesibile sau orientate în mod explicit către rezidenții UE prin intermediul afișării de informații în diverse limbi ale UE, furnizarea de servicii sau produse în țări ale UE, accesibilitatea serviciului în funcție de utilizarea unui card de credit european, trimiterea de reclame în limba utilizatorului sau pentru produse și servicii disponibile pe teritoriul UE. Grupul de lucru amintește că acest criteriu este deja utilizat în domeniul protecției consumatorului: aplicarea acestuia în contextul protecției datelor ar consolida securitatea juridică pentru operatori, întrucât aceștia ar fi nevoiți să aplice același criteriu pentru activitățile care declanșează adesea aplicarea normelor privind protecția consumatorului și a datelor**.**

   – Criteriul privind echipamentele/mijloacele: acest criteriu s-a dovedit a avea consecințe nedorite, cum ar fi posibila aplicare universală a dreptului UE. Cu toate acestea, este necesară prevenirea situațiilor în care lacunele juridice permit utilizarea Uniunii Europene drept paravan de date, de exemplu, în cazul în care activitatea de prelucrare implică aspecte etice inadmisibile. Prin urmare, criteriul privind echipamentele/mijloacele poate fi păstrat din perspectiva drepturilor fundamentale și într-o formă reziduală. Acesta s-ar aplica, în consecință, doar ca o a treia posibilitate, în cazul în care celelalte două posibilități nu se aplică: acesta vizează cazurile de referință (date referitoare la persoane vizate care nu fac parte din UE, operatorii neavând vreo legătură cu UE) în care există o infrastructură relevantă în cadrul UE legată de prelucrarea informațiilor. În acest ultim caz, ar putea exista

opțiunea de a prevedea aplicabilitatea exclusivă a anumitor principii privind protecția datelor – cum ar fi legitimitatea sau măsurile de securitate. Această abordare, care ar face în mod evident obiectul dezvoltărilor și prelucrărilor ulterioare, ar soluționa probabil majoritatea problemelor existente în prezent la articolul 4 alineatul (1) litera (c).

f. Ca ultimă recomandare, grupul de lucru solicită o mai mare armonizare a obligațiilor operatorilor stabiliți în țări terțe în ceea ce privește desemnarea unui reprezentant pe teritoriul UE, cu scopul de a eficientiza rolul acestuia. În special, trebuie clarificată măsura în care persoanele vizate ar trebui să dispună de posibilitatea de a-și exercita efectiv drepturile împotriva reprezentantului.

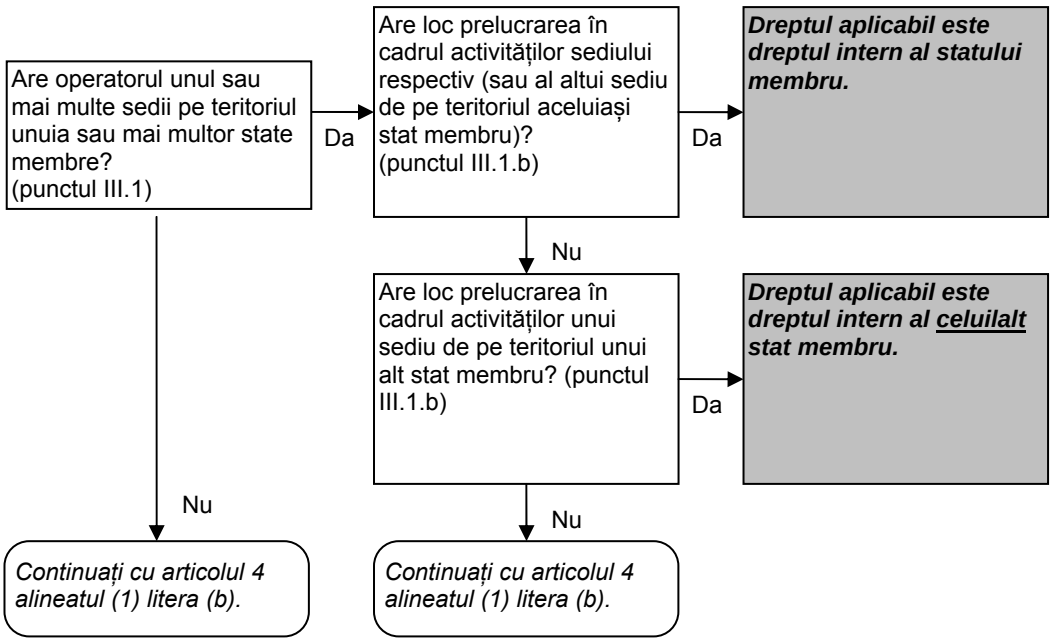
Adoptat la Bruxelles, la 16 decembrie 2010

Pentru grupul de lucru,

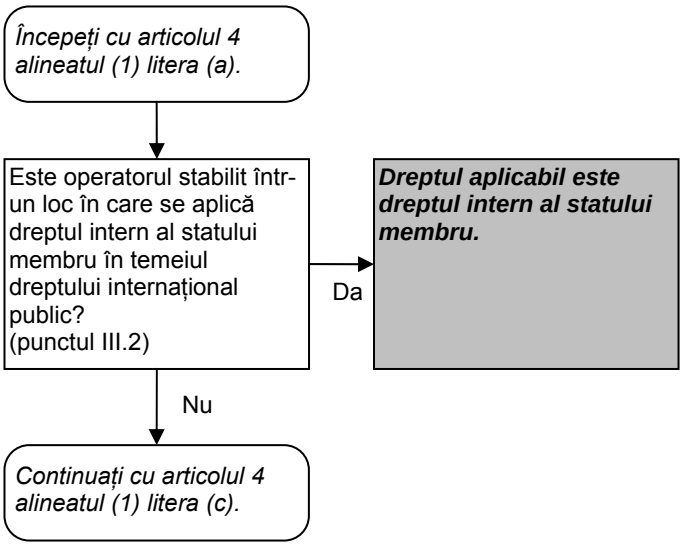
Președintele
Jacob KOHNSTAMM

ANEXĂ

Articolul 4 alineatul (1) litera (a)



Articolul 4 alineatul (1) litera (b)



Articolul 4 alineatul (1) litera (c)