GRUPUL DE LUCRU PENTRU PROTECȚIA DATELOR INSTITUIT ÎN TEMEIUL ARTICOLULUI 29

00264/10/RO
GL 169

Avizul nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator”

Adoptat la 16 februarie 2010

CUPRINS

Rezumat

Conceptul de operator de date și interacțiunea acestuia cu conceptul de persoană împuternicită să prelucreze datele au un rol esențial în aplicarea Directivei 95/46/CE, deoarece acestea stabilesc cine este responsabil de respectarea normelor de protecție a datelor, care este legislația națională aplicabilă și cât de eficient pot opera autoritățile de protecție a datelor.

Diferențierea organizațională în sectorul public și în cel privat, dezvoltarea TIC și globalizarea prelucrării datelor sporesc complexitatea modului în care datele personale sunt prelucrate și necesită clarificarea acestor concepte, pentru a asigura aplicarea eficientă și conformitatea lor în practică.

Conceptul de operator este autonom, în sensul că ar trebui interpretat în principal în conformitate cu legislația comunitară privind protecția datelor și funcțional, în sensul că urmărește să aloce responsabilitățile acolo unde există o influență efectivă, bazându-se astfel pe o analiză a faptelor și nu pe o analiză formală.

Definiția din directivă cuprinde trei elemente esențiale:
- aspectul privind persoana („*persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism*”);
- posibilitatea unui control multiplu („*care, singur sau împreună cu altele*”); și
- elementele esențiale care fac deosebirea dintre operator și alți actori („*stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal*”).

Analiza acestor piloni conduce la o serie de concluzii, care au fost prezentate pe scurt la punctul IV al prezentului aviz.

Prezentul aviz analizează, de asemenea, conceptul de persoană împuternicită, a cărei existență depinde de decizia pe care o ia operatorul, care poate decide fie să prelucreze datele în cadrul organizației sale, fie să delege toate activitățile de prelucrare sau o parte din acestea unei organizații externe. Persoana împuternicită de operator trebuie să îndeplinească două condiții de bază: pe de o parte, aceasta trebuie să fie o entitate juridică distinctă în raport cu operatorul și, pe de altă parte, să prelucreze datele personale în numele acestuia.

Grupul de lucru recunoaște dificultățile întâmpinate în aplicarea definițiilor din directivă într-un mediu complex, în care pot fi imaginate numeroase scenarii care implică operatori și persoane împuternicite de aceștia, singuri sau împreună, cu diferite grade de autonomie și răspundere.

În analiza sa, Grupul de lucru a pus accentul pe necesitatea alocării responsabilităților în așa fel încât conformitatea cu normele de protecție a datelor să fie suficient asigurată în practică. Totuși, nu a găsit niciun motiv să considere că distincția actuală dintre operatori și persoanele împuternicite de aceștia nu ar mai fi relevantă și aplicabilă în acest sens.

În consecință, Grupul de lucru își exprimă speranța că explicațiile din prezentul aviz, ilustrate prin exemple specifice din experiența zilnică a autorităților de protecție a datelor, vor contribui la o orientare eficace cu privire la modul de interpretare a acestor definiții de bază din directivă.

instituit în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30 alineatele (1) litera (a) și (3) din directiva menționată și articolul 15 alineatul (3) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002,

având în vedere regulamentul său de procedură,

adoptă următorul aviz:

I. Introducere

Conceptul de operator de date și interacțiunea acestuia cu conceptul de persoană împuternicită pentru prelucrarea datelor are un rol esențial în aplicarea Directivei 95/46/CE, deoarece acestea stabilesc cine este responsabil de respectarea normelor de protecție a datelor și modul în care persoanele vizate își pot exercita drepturile în practică. Conceptul de operator de date este, de asemenea, esențial pentru stabilirea legislației naționale aplicabile și pentru exercitarea efectivă a sarcinilor de supraveghere de către autoritățile de protecție a datelor.

În consecință, este deosebit de important ca sensul exact al acestor concepte și criteriile privind utilizarea lor corectă să fie suficient de clare și împărtășite de toate persoanele din statele membre care joacă un rol în implementarea directivei și în aplicarea, evaluarea și executarea dispozițiilor naționale care o pun în aplicare.

Au apărut semnale potrivit cărora ar putea exista o lipsă de claritate, cel puțin în ceea ce privește anumite aspecte ale acestor concepte, și unele opinii divergente printre specialiștii din diferite state membre, care ar putea duce la diferite interpretări ale aceloraşi principii și definiții introduse în scopul armonizării la nivel european. De aceea, Grupul de lucru instituit în temeiul articolului 29 a decis, în cadrul programului său strategic de lucru pe 2008-2009, să acorde o atenție specială elaborării unui document care să stabilească o abordare comună a acestor probleme.

Grupul de lucru recunoaște faptul că aplicarea concretă a acestor concepte privind operatorul de date și persoana împuternicită pentru prelucrarea datelor devine tot mai complexă. Acest fapt se datorează în principal complexității tot mai mari a mediului în care sunt utilizate, în special tendinței crescânde, atât în sectorul privat, cât și în cel public, către diferențierea organizațională, alături de dezvoltarea TIC și globalizare, ceea ce poate duce la apariția unor probleme noi, dificile și, uneori, la diminuarea nivelului de protecție a persoanelor vizate.

Deși dispozițiile directivei au fost formulate într-un mod neutru din punct de vedere tehnologic și au rezistat până acum contextului în plină evoluție, aceste situații complexe ar putea duce într-adevăr la incertitudini în ceea ce privește alocarea responsabilităților și domeniul de aplicare al legislației naționale aplicabile. Aceste incertitudini ar putea avea un impact negativ asupra respectării normelor de protecție a datelor în domenii cruciale și

asupra eficacității legislației privind protecția datelor în general. Grupul de lucru a abordat deja câteva dintre aceste aspecte legate de chestiuni specifice[1], dar consideră necesar să ofere acum îndrumări mai ample și specifice, în vederea asigurării unei abordări consecvente și armonizate.

În consecință, Grupul de lucru a decis să ofere în prezentul aviz – așa cum a procedat și în Avizul privind conceptul de date cu caracter personal[2] - o serie de clarificări și exemple concrete[3] cu privire la conceptele de operator de date și de persoană împuternicită pentru prelucrarea datelor.

II. Observații generale și aspecte legate de politică

Mai multe dispoziții ale directivei fac referire explicită la conceptul de operator. Definițiile „operatorului" și „persoanei împuternicite de către operator" din articolul 2 literele (d) și (e) din Directiva 95/46/CE (denumită în continuare „directiva") au următoarea formulare:

> *„operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele de prelucrare sunt stabilite prin acte cu putere de lege naționale sau comunitare, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul național sau comunitar;*
>
> *„persoana împuternicită de către operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care prelucrează datele cu caracter personal pe seama operatorului.*

Aceste definiții au fost trasate în timpul negocierilor pentru proiectul de propunere privind directiva de la începutul anilor 1990, iar conceptul de „operator" a fost în esență preluat din Convenția 108 a Consiliului Europei încheiată în 1981. În timpul negocierilor, au avut loc o serie de modificări importante.

În primul rând, „operatorul dosarului" din Convenția 108 a fost înlocuit cu termenul de „operator", în legătură cu „prelucrarea datelor cu caracter personal". Aceasta este o noțiune largă, definită în articolul 2 litera (b) din directivă ca fiind „orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea". Astfel, conceptul de „operator" nu a mai fost utilizat în legătură cu un obiect static („dosarul"), ci în legătură cu activități care reflectă ciclul de viață al informațiilor, de la colectarea la distrugerea acestora, aceasta necesitând o analiză

---

1 A se vedea de exemplu Avizul 10/2006 privind prelucrarea datelor cu caracter personal de către Societatea Internațională pentru Telecomunicații Financiare Interbancare (SWIFT), adoptat la 22 noiembrie 2006 (GL 128) și , mai recent, Avizul 5/2009 privind rețelele de socializare online, adoptat la 12 iunie 2009 (GL 163).

2 Avizul 4/2007 privind conceptul datelor cu caracter personal, adoptat la 20 iunie 2007 (GL 136).

3 Aceste exemple se bazează pe practica națională sau europeană actuală și este posibil să fi fost modificate sau adaptate pentru a asigura o mai bună înțelegere.

detaliată și cuprinzătoare („operațiune sau serie de operațiuni”). Deși, în multe cazuri, este posibil ca rezultatul să fi fost același, conceptul a primit astfel un înțeles și un domeniu de aplicare mult mai larg și mai dinamic.

Alte modificări au inclus introducerea posibilității „controlului multiplu” („singur sau împreună cu altele”), obligația ca operatorul să „stabilească scopurile și mijloacele de prelucrare” și ideea că acest lucru poate fi stabilit de legislația națională sau comunitară sau altfel. Directiva a introdus, de asemenea, conceptul de „persoană împuternicită de operator”, care nu este menționat în Convenția 108. Acestea, alături de alte modificări, vor fi analizate mai amănunțit în prezentul aviz.

II.1. Rolul conceptelor

În timp ce conceptul de operator (al dosarului) are un rol extrem de limitat[4] în Convenția 108, în directivă, lucrurile stau cu totul altfel. Articolul 6 alineatul (2) prevede în mod explicit faptul că „Operatorul are obligația să asigure respectarea alineatului (1).” Acesta se referă la principalele principii privind calitatea datelor, inclusiv principiul menționat în articolul 6 alineatul (1) litera (a) potrivit căruia „datele cu caracter personal trebuie să fie prelucrate în mod corect și legal”. Aceasta înseamnă de fapt că toate dispozițiile care stabilesc condițiile privind prelucrarea legală se adresează în esență operatorului, chiar dacă acest lucru nu este întotdeauna precizat în mod clar.

În plus, dispozițiile privind drepturile persoanei vizate la informații, de a accesa, rectifica, șterge și bloca informațiile și de a se opune prelucrării datelor cu caracter personal (articolele 10-12 și 14), au fost concepute în așa fel încât să creeze obligații pentru operator. Operatorul ocupă, de asemenea, un loc central în dispozițiile privind notificarea și controlul prealabil (articolele 18-21). În sfârșit, nu este de mirare că operatorul este cel care răspunde, în principiu, de prejudiciile cauzate de o prelucrare ilegală (articolul 23).

Aceasta înseamnă că primul și cel mai important rol al conceptului de operator este acela de a stabili cine va fi responsabil de respectarea normelor de protecție a datelor și modul în care persoanele vizate își pot exercita drepturile în practică[5]. Cu alte cuvinte: alocarea responsabilității.

Aceasta este esența Directivei, principalul obiectiv al acesteia fiind „protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal”. Acest obiectiv poate fi realizat și pus în aplicare în practică numai dacă persoanele responsabile cu prelucrarea datelor pot fi motivate îndeajuns prin mijloace legale sau prin alte mijloace, pentru a lua toate măsurile necesare în vederea asigurării unei protecții efective. Acest aspect este confirmat în articolul 17 alineatul (1) din directivă, care prevede „*aplicarea obligatorie de către operator a unor măsuri tehnice și organizatorice de protecție adecvate pentru*

---

4 Nu este utilizat în nicio dispoziție de fond, cu excepția articolului 8.a cu privire la dreptul de a fi informat (principiul transparenței). Operatorul, ca parte responsabilă, este vizibil numai în anumite părți ale expunerii de motive.

5 A se vedea, de asemenea, considerentul 25 al Directivei 95/46/CE: „*Întrucât principiile protecției trebuie să se reflecte, pe de o parte, în obligațiile impuse persoanelor, autorităților publice, întreprinderilor, agenților sau altor organisme care prelucrează date, în special în materie de calitatea datelor, siguranța tehnică, notificarea autorității de supraveghere, circumstanțele în care poate fi efectuată prelucrarea și, pe de altă parte, în dreptul conferit persoanelor ale căror date fac obiectul prelucrării de a fi informate cu privire la aceasta, de a putea avea acces la date, de a putea solicita corectarea lor și chiar de a se opune prelucrării în anumite circumstanțe*”.

protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat, în special atunci când prelucrarea presupune transmiterea datelor într-o rețea, precum și împotriva oricărei alte forme de prelucrare ilegală".

Mijloacele de stimulare a responsabilității pot fi proactive și reactive. În primul caz, acestea urmăresc să asigure aplicarea eficientă a măsurilor de protecție a datelor și mijloace suficiente de tragere la răspundere a operatorilor. În al doilea caz, acestea pot implica răspunderea civilă și sancțiuni, pentru a asigura compensarea oricăror prejudicii relevante și luarea unor măsuri adecvate în vederea corectării erorilor sau greșelilor.

Conceptul de operator este de asemenea un element esențial în ceea ce privește stabilirea legislației naționale aplicabile unei operațiuni sau unei serii de operațiuni de prelucrare. Principala normă a legislației aplicabile în conformitate cu articolul 4 alineatul (1) litera (a) din directivă este faptul că fiecare stat membru aplică dispozițiile sale naționale cu privire la „*prelucrarea datelor cu caracter personal, atunci când (...) este efectuată în cadrul activităților operatorului cu sediul pe teritoriul statului membru"*. Această dispoziție continuă după cum urmează: „*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*". Aceasta înseamnă că sediul/sediile operatorului este/sunt de asemenea determinant(e) pentru stabilirea legislației naționale aplicabile și, eventual, pentru o serie de legi naționale aplicabile diferite și modul în care relaționează unele cu altele[6].

În sfârșit, trebuie remarcat că conceptul de operator apare în numeroase dispoziții diferite ale directivei ca un element al domeniului de aplicare al acestora sau al unei condiții specifice care se aplică în temeiul acestora: de exemplu, articolul 7 prevede că datele cu caracter personal pot fi prelucrate numai dacă: „*(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului, (e) prelucrarea este necesară pentru aducerea la îndeplinire a unei sarcini de interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul sau terțul căruia îi sunt comunicate datele sau (f) prelucrarea este necesară pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți, cu condiția ca acest interes să nu prejudicieze …*" . Identitatea operatorului este, de asemenea, un element important al informațiilor care trebuie furnizate persoanei vizate, în conformitate cu articolele 10 și 11.

Conceptul de „persoană împuternicită de operator" joacă un rol important în contextul confidențialității și securității prelucrării (articolele 16-17), deoarece contribuie la identificarea responsabilităților persoanelor care sunt implicate mai îndeaproape în prelucrarea datelor cu caracter personal, fie sub autoritatea directă a operatorului, fie în altă parte, în numele acestuia. Distincția dintre „operator" și „persoană împuternicită de operator" servește în principal pentru a face diferența dintre persoanele care sunt responsabile în calitate de operatori și cele care acționează în numele acestora. Din nou, este vorba în principal de modul în care sunt alocate responsabilitățile. De aici pot să decurgă alte consecințe, cu privire la legislația aplicabilă sau în alte privințe.

---

6 Grupul de lucru intenționează să adopte un alt aviz privind „legislația aplicabilă" în cursul anului 2010. Atunci când instituțiile și organismele comunitare prelucrează date cu caracter personal, evaluarea controlului este de asemenea relevantă în ceea ce privește posibila aplicare a Regulamentului (CE) 45/2001 sau a altor instrumente juridice relevante ale UE.

Totuși, în cazul unei persoane împuternicite de operator, mai există o consecință – atât pentru operator, cât și pentru persoana împuternicită – faptul că, în conformitate cu articolul 17 din directivă, legislația aplicabilă pentru securitatea prelucrărilor este legislația națională a statului membru în care este stabilită persoana împuternicită.[7]

În sfârșit, astfel cum se prevede la articolul 2 litera (f), „*«terț» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice organism altul decât persoana vizată, operatorul, persoana împuternicită de către operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de către operator, sunt autorizate să prelucreze date*". Operatorul, persoana împuternicită și personalul acestora sunt în consecință considerați „cercul central al prelucrării datelor" și nu fac obiectul unor dispoziții speciale cu privire la terți.

II.2. Contextul relevant

Ca urmare a diferitelor evoluții înregistrate în mediul relevant, aceste aspecte au devenit mai urgente și mai complexe decât înainte. La momentul semnării Convenției 108 și, în mare măsură, la adoptarea Directivei 95/46/CE, contextul prelucrării datelor era încă relativ clar și simplu, însă această situație s-a schimbat.

Aceasta se datorează, în primul rând, tendinței din ce în ce mai pronunțate către diferențierea organizațională în majoritatea sectoarelor relevante. În sectorul privat, distribuirea riscurilor financiare și a altor riscuri a dus la o diversificare continuă a corporațiilor, care se amplifică prin fuziuni și achiziții. În sectorul public, o diferențiere similară are loc în contextul descentralizării sau separării departamentelor decizionale de agențiile executive. În ambele sectoare, se pune tot mai mult accentul pe dezvoltarea lanțurilor de livrare sau a prestărilor de servicii în cadrul organizațiilor și pe subcontractarea sau externalizarea serviciilor, pentru a beneficia de servicii specializate și eventualele economii de scară. Prin urmare, există o creștere în ceea ce privește diversele servicii, oferite de furnizori care nu se consideră întotdeauna responsabili sau răspunzători. Datorită opțiunilor organizaționale ale întreprinderilor (și contractanților sau subcontractanților acestora), pot să existe baze de date relevante în una sau mai multe țări din cadrul sau din afara Uniunii Europene.

Dezvoltarea tehnologiilor informației și comunicațiilor („TIC") a facilitat în mare măsură aceste schimbări organizaționale și a condus și la alte schimbări. Responsabilitățile de la diferite nivele – adesea determinate de diferențierea organizațională – de obicei necesită și îndeamnă la utilizarea TIC în mare măsură. Dezvoltarea și extinderea produselor și serviciilor TIC determină crearea unor noi roluri și responsabilități distincte, care nu interacționează întotdeauna cu responsabilitățile existente sau în curs de formare din organizațiile cliente. În consecință, este important să se conștientizeze existența unor diferențe relevante și să se clarifice responsabilitățile, după caz. Introducerea microtehnologiei – precum cipurile RFID pentru produsele destinate consumatorilor – ridică probleme similare legate de transferul de responsabilități. Pe de altă parte, utilizarea unui sistem informatic distribuit, în special a informaticii de tip „cloud computing" și a „rețelelor informatice"[8] implică probleme noi și dificile.

---

[7] A se vedea articolul 17 alineatul (3), a doua liniuță: „obligațiile … așa cum sunt definite de legislația statului membru în care este stabilită persoana împuternicită îi revin acesteia".

[8] „Cloud computing" este un tip de informatică în care capacitățile IT extensibile și flexibile sunt furnizate sub forma unui serviciu, mai multor clienți, care utilizează tehnologii de internet. Serviciile caracteristice de tip „cloud computing" furnizează aplicații de business obișnuite online, care sunt accesate de pe un browser de internet, în timp ce programul și datele sunt stocate pe servere. În acest

Globalizarea este un alt factor al complexității. Atunci când diferențierea organizațională și dezvoltarea TIC implică mai multe jurisdicții, așa cum se întâmplă adesea pe Internet, apar inevitabil probleme legate de legislația aplicabilă, nu numai în UE sau SEE, ci și în legătură cu țările terțe. Un exemplu în acest sens poate fi găsit în contextul antidoping, în care Agenția Mondială Antidoping (WADA), cu sediul în Elveția, operează o bază de date care include informații referitoare la sportivi (ADAMS) și care este gestionată din Canada, în colaborare cu organizațiile antidoping naționale din lume. GL29 a semnalat faptul că alocarea responsabilităților și atribuirea controlului ridică dificultăți specifice[9].

Aceasta înseamnă că problemele principale care sunt abordate în acest aviz au o relevanță practică semnificativă și ar putea avea consecințe importante.

II.3. Anumite provocări esențiale

În termeni de obiective ale directivei, cel mai important lucru este să se asigure că responsabilitatea în ceea ce privește prelucrarea datelor este clar stabilită și poate fi aplicată eficient.

În cazul în care nu este suficient de clar cui trebuie să îi fie atribuite cerințele – de exemplu, dacă nicio persoană nu este responsabilă sau există mai mulți operatori posibili – există riscul evident să nu fie luate suficiente măsuri, în cazul în care sunt luate măsuri, iar dispozițiile juridice să nu producă efecte. De asemenea, este posibil ca ambiguitățile în ceea ce privește interpretarea să ducă la revendicări concurente sau la alte controverse, caz în care efectele pozitive vor fi sub așteptări sau ar putea fi diminuate sau eclipsate de consecințe negative neprevăzute.

În toate aceste cazuri, provocarea esențială este astfel să se asigure o claritate suficientă, pentru a permite și a asigura aplicarea eficientă și conformitatea în practică. În cazul în care există îndoieli, soluția care ar determina cel mai probabil aceste efecte ar putea fi opțiunea preferată.

Totuși, aceleași criterii care asigură o transparență suficientă ar putea conduce, de asemenea, la o complexitate și mai mare și la consecințe nedorite. De exemplu, diferențierea controlului, în conformitate cu realitățile organizaționale, ar putea determina o complexitate a legislației naționale aplicabile, atunci când sunt implicate jurisdicții diferite.

În consecință, analiza ar trebui să urmărească atent diferența dintre consecințele acceptabile în conformitate cu normele actuale și posibila necesitate de ajustare a normelor actuale, pentru a se asigura eficacitatea continuă și pentru a se evita consecințele necorespunzătoare în circumstanțe diferite.

Aceasta înseamnă că analiza actuală are o importanță strategică majoră și ar trebui aplicată cu atenție, conștientizându-se pe deplin posibilele interconexiuni dintre diferitele aspecte.

---

sens, norul („cloud”) nu este o insulă, ci un element global de legătură între informațiile și utilizatorii din întreaga lume. În ceea ce privește „rețelele informatice”, a se vedea exemplul 19 de mai jos.

9 Avizul nr. 3/2008 din 1 august 2008 privind proiectul de standard internațional cu privire la protecția vieții private al Codului mondial antidoping, GL156

III. Analiza definițiilor

III.1. Definiția operatorului

Definiția operatorului din directivă cuprinde trei piloni, care vor fi analizați separat, în sensul avizului. Aceștia sunt:

- „persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism”
- „care, singur sau împreună cu altele,”
- „stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal”.

Primul pilon se referă la aspectul personal al definiției. Al treilea pilon cuprinde elemente esențiale de diferențiere a operatorului de alți actori, în timp ce al doilea pilon analizează posibilitatea „controlului multiplu”. Aceste pietre de temelie sunt foarte strâns interrelaționate. Totuși, având în vedere metodologia care trebuie urmată în prezentul aviz, fiecare dintre aceste elemente va fi tratat separat.

Din motive practice, este de preferat să începem cu *primul element* al celui de-al treilea pilon – adică sensul cuvântului „stabilește” – să continuăm cu restul celui de-al treilea pilon și doar ulterior să abordăm primul și al doilea pilon.

III.1.a) Element preliminar: „stabilește”

Astfel cum s-a menționat deja mai sus, conceptul de operator avea un rol minor în Convenția 108. În temeiul articolului 2 din Convenție, „operatorul dosarului” era definit ca fiind organismul „competent …să decidă”. Convenția subliniază necesitatea unei competențe, stabilite „în conformitate cu legislația națională”. Astfel, Convenția făcea referire la legislația națională privind protecția datelor care, conform expunerii de motive, ar cuprinde „criterii exacte de stabilire a persoanei competente”.

În timp ce prima propunere a Comisiei reflectă această dispoziție, propunerea modificată a Comisiei se referă în schimb la organismul „care decide”, eliminând astfel necesitatea stabilirii prin lege a competenței de decizie: aceasta este posibilă, dar nu mai este necesară. Aceasta este apoi confirmată prin poziția comună a Consiliului și prin textul adoptat, ambele referindu-se la organismul „care stabilește”.

În acest context, evoluția istorică scoate în evidență două elemente importante: în primul rând, faptul că este posibil ca o persoană să fie operator, indiferent dacă are sau nu o anumită competență sau autoritate de operare a datelor, conferită prin lege; în al doilea rând, faptul că în timpul adoptării Directivei 95/46/CE, stabilirea operatorului devine un concept comunitar, un concept care are înțelesul său propriu, independent, în dreptul comunitar, care nu variază în funcție de prevederile, posibil divergente, ale legislațiilor naționale. Cel de-al doilea element este esențial pentru a asigura aplicarea cu eficacitate a directivei și un nivel ridicat de protecție în statele membre, ceea ce necesită o interpretare uniformă și autonomă a unui concept cheie precum conceptul de „operator”, care dobândește în directivă o importanță pe care nu o avea în Convenția 108.

În acest sens, directiva încheie această evoluție stabilind faptul că, deși capacitatea de a „stabili” ar putea fi reieși dintr-o atribuție specifică conferită prin lege, aceasta decurge de obicei din analiza elementelor sau a circumstanțelor faptice ale cazului: ar trebui să analizăm operațiunile de prelucrare în cauză și să înțelegem cine le determină,

răspunzând într-o primă etapă la întrebările: „De ce are loc această prelucrare de date? Cine a inițiat-o?”.

Existența unui operator este în primul rând consecința faptului că o entitate a decis să prelucreze datele cu caracter personal în propriile scopuri. Într-adevăr, un simplu criteriu formal nu ar fi suficient, cel puțin din două motive: în unele cazuri, ar lipsi pur și simplu numirea oficială a unui operator – de exemplu, prin lege, într-un contract sau într-o notificare trimisă autorității de protecție a datelor; în alte cazuri, este posibil ca numirea oficială să nu reflecte realitatea, atribuind în mod oficial funcția de operator unui organism care nu este în măsură să „stabilească”.

Relevanța influenței efective este de asemenea prezentată în cazul SWIFT[10], în care SWIFT a fost considerată oficial ca fiind persoana împuternicită să prelucreze datele, însă avea de fapt rolul - cel puțin într-o anumită măsură - de operator de date. În acest caz, s-a clarificat faptul că deși numirea unei părți în calitatea de operator sau persoană împuternicită în cadrul unui contract ar putea dezvălui informații relevante cu privire la statutul juridic al părții respective, această numire nu este decisivă pentru stabilirea statutului real al acesteia, care trebuie să se bazeze pe circumstanțe concrete.

Această abordare faptică este, de asemenea, susținută de considerentul că directiva prevede ca operatorul să fie cel care „stabilește” și nu cel care „stabilește în mod legal” scopul și mijloacele. Identificarea efectivă a controlului este decisivă, chiar dacă numirea operatorului pare să fie nelegitimă sau prelucrarea datelor este exercitată în mod nelegal. Nu este relevant dacă decizia de prelucrare a datelor a fost sau nu „legală”, în sensul în care entitatea care a luat această decizie avea capacitatea legală de a face acest lucru, sau operatorul a fost numit în mod oficial conform unei anumite proceduri. Chestiunea legalității prelucrării datelor cu caracter personal va fi totuși relevantă într-o altă etapă și va fi evaluată în temeiul altor articole (în special articolele 6-8) ale directivei. Cu alte cuvinte, este important să se asigure, chiar și atunci când datele sunt prelucrate în mod nelegal, că operatorul poate fi găsit ușor și că acesta va răspunde de prelucrarea datelor.

O ultimă caracteristică a conceptului de operator este autonomia acestuia, în sensul că, deși sursele legale externe pot ajuta la identificarea operatorului, conceptul ar trebui interpretat în principal în conformitate cu legislația privind protecția datelor[11]. Conceptul de operator nu ar trebui prejudiciat de conceptele din alte domenii legislative, care uneori sunt opuse sau coincid, precum conceptul de autor sau titular al drepturilor de proprietate intelectuală. Calitatea de titular de drepturi de proprietate intelectuală nu exclude posibilitatea de a fi și „operator” și de a face obiectul obligațiilor care decurg în conformitate cu legislația privind protecția datelor.

Necesitatea unei tipologii

Conceptul de operator este un concept funcțional, menit să aloce responsabilitățile acolo unde există o influență efectivă, fiind astfel bazat pe o analiză faptică și nu pe o analiză formală. În consecință, stabilirea controlului ar putea necesita uneori investigații

[10] Cazul se referă la transferul către autoritățile SUA a datelor bancare colectate prin SWIFT utilizate pentru realizarea tranzacțiilor financiare în numele băncilor și al instituțiilor financiare, în vederea combaterii finanțării terorismului.

[11] A se vedea în text interferența cu conceptele din alte domenii legislative (de exemplu, conceptul de titular al drepturilor de proprietate intelectuală sau de cercetare științifică sau responsabilitatea în temeiul legislației civile).

amănunțite și îndelungate. Totuși, necesitatea de a asigura eficacitatea impune adoptarea unei abordări pragmatice, în vederea asigurării predictibilității controlului. În acest sens, pentru aplicarea legislației privind protecția datelor în mod orientat și simplificat, este nevoie de metode empirice și de ipoteze practice.

Astfel, directiva trebuie interpretată astfel încât să se asigure că „organismul de stabilire" poate fi identificat ușor și precis în majoritatea situațiilor, prin referire la circumstanțele - legale și/sau de fapt – din care poate decurge în mod normal influența efectivă, exceptând cazurile în care alte elemente indică contrariul.

Aceste circumstanțe pot fi analizate și clasificate în funcție de următoarele trei categorii de situații, care permit o abordare sistematică a acestor aspecte:

1) *Control care decurge din competența legală explicită.* Acesta este, *inter alia,* cazul la care se face referire în a doua parte a definiției, și anume atunci când operatorul sau criteriile specifice pentru desemnarea acestuia sunt stabilite conform legislației naționale sau comunitare. Desemnarea explicită a operatorului prin lege nu este frecventă și nu pune în general probleme mari. În unele țări, legislația națională prevede ca autoritățile publice să fie responsabile pentru prelucrarea datelor cu caracter personal ca parte a îndatoririlor acestora.

Totuși, mai frecvent este cazul în care legislația nu desemnează direct un operator sau nu stabilește criteriile pentru desemnarea acestuia, ci stabilește o îndatorire sau obligă o persoană să colecteze și să prelucreze anumite date. De exemplu, o entitate are anumite îndatoriri publice (de exemplu, securitatea socială), care nu pot fi realizate fără colectarea unor date cu caracter personal, și creează un registru în vederea îndeplinirii acestora. În acest caz, operatorul este desemnat prin lege. În termeni mai generali, legislația poate obliga entitățile publice sau private să păstreze sau să furnizeze anumite date. Aceste entități ar fi considerate în mod normal ca având rolul de operator pentru prelucrarea oricăror date cu caracter personal în acest context.

2) *Control care decurge din competența implicită*. Acesta este cazul în care capacitatea de a stabili nu este prevăzută explicit prin lege și nici consecința directă a unor dispoziții legale explicite, dar decurge din dispozițiile legale comune sau din practica legală consacrată în diferite domenii (dreptul civil, dreptul comercial, dreptul muncii etc.). În acest caz, rolurile tradiționale existente care implică în mod normal o anumită răspundere vor ajuta la identificarea operatorului: de exemplu, angajatorul în ceea ce privește datele referitoare la angajații acestuia, editorul în ceea ce privește datele referitoare la abonați, asociația în ceea ce privește datele referitoare la membrii sau colaboratorii acesteia.

În toate aceste cazuri, capacitatea de a stabili activitățile de prelucrare poate fi considerată ca făcând parte integrantă din rolul funcțional al unei organizații (private), ducând în cele din urmă la crearea unor responsabilități și din punctul de vedere al protecției datelor. În termeni juridici, această situație ar fi valabilă indiferent dacă organismele juridice menționate ar avea capacitatea de stabilire, dacă aceasta ar fi exercitată de instituțiile corespunzătoare care acționează în nume propriu sau de către o persoană fizică într-un rol similar [a se vedea mai jos, primul element de la litera (c)]. Totuși, aceeași situație ar fi valabilă și în cazul unei autorități publice cu anumite îndatoriri administrative, dintr-o țară în care legislația nu este explicită cu privire la răspunderea acesteia în ceea ce privește protecția datelor.

Exemplul nr. 1: Operatorii de telecomunicaţii

Un exemplu interesant de orientări juridice pentru sectorul privat este cel al rolului operatorilor de telecomunicaţii: considerentul 47 al Directivei 95/46/CE precizează că „*dacă se transmite un mesaj care conţine date cu caracter personal printr-un serviciu de telecomunicaţii sau de poştă electronică al cărui unic scop este de a transmite mesaje de acest tip, operatorul datelor cu caracter personal cuprinse într-un mesaj este în mod normal considerată persoana care expediază mesajul, nu cea care oferă serviciul de transmitere a acestuia; (...) cu toate acestea, persoanele care oferă aceste servicii sunt în mod normal considerate operatori ai prelucrării datelor cu caracter personal suplimentare necesare funcţionării serviciului”*. În consecinţă, furnizorul de servicii de telecomunicaţii ar trebui considerat, în principiu, operator numai pentru datele de trafic şi facturare şi nu pentru datele transmise[12]. Aceste îndrumări juridice furnizate de organul legislativ al Comunităţii sunt în deplină conformitate cu abordarea funcţională a prezentului aviz.

3) *Control care decurge din influenţa efectivă.* Acesta este cazul în care responsabilitatea funcţiei de operator este atribuită pe baza evaluării circumstanţelor reale. Adeseori, aceasta implică evaluarea relaţiilor contractuale dintre diferitele părţi implicate. În urma acestei evaluări se pot trage concluzii externe, iar rolul de operator şi responsabilităţile aferente pot fi atribuite uneia sau mai multor părţi. Aceasta poate fi deosebit de utilă în special în mediile complexe, în care se utilizează adesea tehnologii informaţionale noi şi în care părţile relevante tind adesea să se considere „mediatori” şi nu operatori responsabili.

Este posibil ca un contract să nu specifice cine este operatorul, dar să cuprindă suficiente elemente pentru atribuirea responsabilităţii de operator unei părţi care exercită, aparent, un rol hotărâtor în această privinţă. De asemenea, contractul poate fi mai explicit în ceea ce priveşte operatorul. Dacă nu există niciun motiv de îndoială că un contract reflectă întocmai realitatea, nu există motive pentru nerespectarea condiţiilor acestuia. Totuşi, condiţiile unui contract nu sunt decisive în toate cazurile, deoarece aceasta le-ar permite pur şi simplu părţilor să aloce responsabilităţile aşa cum consideră că este mai potrivit.

Faptul în sine că o persoană stabileşte modul în care datele personale sunt prelucrate poate atrage calificarea ca operator de date, chiar dacă aceasta se produce în afara sferei unei relaţii contractuale sau este exclusă în mod explicit prin contract. Un exemplu evident a fost cazul SWIFT, în care întreprinderea în cauză a luat decizia de a pune la dispoziţie anumite date – care au fost iniţial prelucrate în scopuri comerciale în numele unor instituţii financiare - şi în scopul combaterii finanţării terorismului, aşa cum s-a solicitat prin citaţiile emise de Trezoreria SUA.

[12] O APD (autoritate pentru protecţia datelor) s-a confruntat cu problema controlului într-un caz înaintat de o persoană care reclama faptul că primeşte reclame nesolicitate prin e-mail. În cererea sa, persoana vizată a solicitat furnizorului reţelei de comunicaţii să confirme sau să infirme trimiterea e-mailul publicitar. APD a afirmat că o societate care asigură doar accesul clientului la o reţea de comunicaţii, deci care nu iniţiază transmisia de date, nu selectează adresele şi nu modifică informaţiile transmise, nu poate fi considerată operator de date.

În cazul în care există îndoieli, pentru stabilirea operatorului pot fi folosite și alte elemente decât condițiile contractuale, cum ar fi gradul efectiv de control exercitat de o parte, imaginea oferită subiecților și așteptările rezonabile ale subiecților, bazate pe această percepție [a se vedea, de asemenea, mai jos, al treilea element de la litera (b)]. Această categorie are o importanță deosebită deoarece permite abordarea și alocarea responsabilităților și în cazurile de comportament nelegal, în care activitățile efective de prelucrare pot fi realizate chiar împotriva interesului și intenției anumitor părți.

Concluzie preliminară

Dintre aceste categorii, primele două permit în principiu o indicare mai sigură a organismului de decizie și ar putea acoperi peste 80% din situațiile practice relevante. Totuși, numirea legală oficială ar trebui să fie în conformitate cu normele privind protecția datelor, asigurând faptul că organismul desemnat deține efectiv controlul asupra operațiunilor de prelucrare sau, cu alte cuvinte, că numirea legală reflectă situația reală.

Categoria a 3-a necesită o analiză mai complexă și este mai probabil să conducă la interpretări divergente. Condițiile contractuale pot adesea să contribuie la clarificarea problemei, însă nu sunt decisive în toate circumstanțele. Tot mai mulți actori nu se consideră factori determinanți pentru activitățile de prelucrare și, astfel, responsabili pentru acestea. Singura opțiune posibilă în aceste cazuri este să se ia în considerare influența efectivă. Aspectul legalității acestei prelucrări va fi continua să fie evaluat în temeiul altor articole (6-8).

Dacă nu este aplicabilă niciuna dintre categoriile susmenționate, desemnarea unui operator ar trebui să fie considerată „nulă și neavenită". Într-adevăr, un organism care nu are influență nici de drept, nici de fapt în stabilirea modului de prelucrare a datelor cu caracter personal nu poate fi considerat ca având calitatea de operator.

Din punct de vedere formal, un considerent care vine în sprijinul acestei abordări este faptul că definiția operatorului de date ar trebui considerată o dispoziție legală obligatorie, de la care părțile nu se pot pur și simplu deroga sau abate. Dintr-o perspectivă strategică, o astfel de numire s-ar opune aplicării eficiente a legislației privind protecția datelor și ar anula răspunderea aferentă prelucrării datelor.

III.1.b) <u>Al treilea element: „scopurile și mijloacele de prelucrare"</u>

Al treilea element reprezintă partea principală a testului: ceea ce o parte ar trebui să demonstreze pentru a se califica pentru funcția de operator.

Istoricul acestei dispoziții arată numeroase evoluții. Convenția 108 făcea referire la scopul fișierelor automatizate de date, la categoriile de date cu caracter personal și la operațiunile aferente acestora. Comisia a preluat aceste elemente esențiale, cu mici modificări lingvistice și a adăugat competența de a decide care terți pot avea acces la date. Propunerea modificată a Comisiei a făcut un pas înainte, trecând de la „scopurile dosarului", la „scopurile și obiectivul prelucrării", de la o definiție statică legată de un dosar, la o definiție dinamică legată de o activitate de prelucrare. Propunerea modificată s-a referit totuși la patru elemente (scopuri/obiectiv, date cu caracter personal, operațiuni și terți care au acces la acestea), care au fost reduse la două elemente („scopuri și mijloace") numai prin poziția comună a Consiliului.

În dicționare, „scopul” este definit ca fiind „un rezultat anticipat care este urmărit sau spre care se îndreaptă acțiunile dumneavoastră planificate”, iar „mijloacele” sunt definite ca fiind „modalitatea prin care se obține un rezultat sau prin care se atinge un scop”.

Pe de altă parte, directiva stabilește că datele trebuie colectate în scopuri precise, explicite și legitime și nu trebuie prelucrate într-un mod care să contravină acestor scopuri. În consecință, stabilirea „scopurilor” prelucrării și a „mijloacelor” utilizate pentru atingerea lor este extrem de importantă.

Se poate spune, de asemenea, că stabilirea scopurilor și a mijloacelor este echivalentă cu stabilirea motivului și a metodei anumitor activități de prelucrare. În acest sens și luând în considerare că cele două elemente sunt legate, trebuie stabilit când se poate califica o entitate în funcția de operator, și anume ce grad de influență trebuie aceasta să aibă asupra motivului și a metodei de lucru.

În ceea ce privește evaluarea stabilirii scopurilor și a mijloacelor în vederea atribuirii rolului de operator de date, chestiunea esențială este așadar nivelul de detaliere la care o persoană ar trebui să stabilească scopurile și mijloacele pentru a fi considerată operator. De asemenea, în corelație cu cele de mai sus, evaluarea trebuie să aibă în vedere marja de manevră pe care o poate avea persoana împuternicită să prelucreze datele în conformitate cu directiva. Aceste definiții devin deosebit de relevante atunci când în prelucrarea datelor sunt implicate diverse părți și când trebuie stabilit care dintre acestea au rolul de operator de date (singur sau împreună cu altele) și care au rolul de persoane împuternicite să prelucreze datele - dacă este cazul.

Importanța care se acordă scopurilor și mijloacelor poate varia în funcție de contextul specific în care are loc prelucrarea.

Este nevoie de o abordare pragmatică, care să pună accentul pe libertatea de decizie, în ceea ce privește stabilirea scopurilor și pe libertatea de acțiune, în ceea ce privește luarea deciziilor. În aceste cazuri, întrebarea este de ce sunt prelucrate datele și care este rolul posibilelor părți implicate, precum furnizorii de servicii externalizate: ar fi fost datele prelucrate de întreprinderea către care au fost externalizate serviciile dacă operatorul nu i-ar fi cerut acest lucru și în ce condiții? O persoană împuternicită să prelucreze datele ar putea acționa dincolo de îndrumările generale în ceea ce privește scopurile și ar putea să nu intre prea mult în amănunte în ceea ce privește mijloacele.

Exemplul nr. 2: Marketingul prin poștă

Întreprinderea ABC încheie contracte cu diferite organizații în vederea realizării campaniilor sale de marketing prin poștă și a întocmirii statelor de plată. Aceasta oferă instrucțiuni clare (ce material de marketing trebuie trimis și cui trebuie trimis, cine trebuie plătit, ce sume, până la ce dată etc.). Deși organizațiile au o anumită libertate de decizie (inclusiv referitor la programul pe care să-l utilizeze), îndatoririle lor sunt destul de clar și de bine stabilite și, chiar dacă serviciul poștal ar putea da orientări (de exemplu, o recomandare împotriva trimiterii de mesaje publicitare în luna august), acestea acționează conform instrucțiunilor întreprinderii ABC. Mai mult, o singură entitate, întreprinderea ABC, are dreptul să utilizeze datele prelucrate – toate celelalte entități trebuie să se bazeze pe temeiul juridic al întreprinderii ABC în cazul în care este investigată capacitatea lor legală de a prelucra datele. În acest caz, este evident că întreprinderea ABC are rolul de operator de date, iar fiecare dintre organizațiile separate poate fi considerată persoană împuternicită pentru prelucrarea datelor, cu privire la prelucrarea specifică a datelor pe care o realizează în numele său.

În ceea ce privește stabilirea mijloacelor, termenul „mijloace” cuprinde, în mod evident, elemente de natură foarte diferită, fapt ilustrat și de istoricul acestei definiții. În propunerea inițială, rolul de operator ar decurge din stabilirea a patru elemente (scopuri/obiectiv, date cu caracter personal, operațiuni și terți care au acces la acestea). Formularea finală a prevederii, care se referă numai la „scopuri și mijloace”, nu poate fi interpretată ca fiind în contradicție cu versiunea anterioară, deoarece nu există nicio îndoială cu privire la faptul că operatorul este cel care trebuie să stabilească ce date trebuie prelucrate pentru scopul propus/scopurile propuse. În consecință, ultima definiție trebuie înțeleasă mai degrabă ca fiind doar o versiune prescurtată care cuprinde însă sensul versiunii anterioare. Cu alte cuvinte, „mijloacele” nu se referă la modalitățile tehnice de prelucrare a datelor cu caracter personal, ci și la modul de realizare a prelucrării, care include întrebări precum: „ce date trebuie prelucrate”, „care terți au acces la aceste date”, „când vor fi șterse datele” etc.

În consecință, stabilirea „mijloacelor” include atât întrebări tehnice și organizaționale, pentru care deciziile pot fi delegate persoanelor împuternicite (cum ar fi, de exemplu, „ce hardware și software trebuie să se utilizeze?”), cât și elemente esențiale care sunt de regulă și inerent stabilite de operator, cum ar fi „ce date trebuie prelucrate?”, „pentru cât timp vor fi prelucrate?”, „cine va avea acces la ele?” etc.

În acest context, în timp ce stabilirea scopului prelucrării ar determina în orice caz calificarea de operator, stabilirea mijloacelor ar implica un controlul doar în situațiile în care stabilirea vizează elementele esențiale ale mijloacelor.

În acest sens, este foarte posibil ca mijloacele tehnice și organizatorice să fie stabilite exclusiv de către persoana împuternicită să prelucreze datele.

În aceste cazuri – în care scopurile sunt bine definite, dar orientările privind mijloacele tehnice și organizaționale sunt foarte puține sau nu există - mijloacele ar trebui să reprezinte o modalitate rezonabilă de atingere a scopului/scopurilor, iar operatorul de date ar trebui să fie pe deplin informat cu privire la mijloacele utilizate. În cazul în care un contractant ar avea o influență asupra scopului și ar prelucra datele (și) în scopuri proprii, de exemplu utilizând datele cu caracter personal primite în vederea generării unor servicii cu valoare adăugată, acesta ar fi un operator (sau un operator asociat) pentru o altă activitate de prelucrare și s-ar supune tuturor obligațiilor legislației aplicabile privind protecția datelor.

Exemplul nr. 3: Întreprindere cu titlu de persoană împuternicită să prelucreze datele, dar care acționează ca un operator de date

Întreprinderea MarketinZ oferă servicii de publicitate promoțională și de marketing direct mai multor întreprinderi. Întreprinderea GoodProductZ încheie un contract cu MarketinZ, conform căruia cea de-a doua întreprindere asigură publicitatea comercială pentru clienții GoodProductZ și este considerată ca fiind persoana împuternicită să prelucreze datele. Totuși, MarketinZ decide să utilizeze baza de date cuprinzând clienții GoodProducts și în scopul promovării produselor altor clienți. Această decizie, de a adăuga încă un scop pe lângă scopul pentru care au fost transferate datele cu caracter personal, schimbă statutul întreprinderii MarketinZ în operator de date pentru această operațiune de prelucrare. Chestiunea legitimității acestei prelucrări va fi totuși evaluată în temeiul altor articole (6-8).

În anumite sisteme juridice, deciziile cu privire la măsurile de securitate sunt deosebit de importante, deoarece măsurile de securitate sunt considerate în mod explicit ca fiind o caracteristică esențială care trebuie stabilită de operator. Astfel, apare întrebarea privind ce decizii referitoare la securitate pot atrage calificarea ca operator a unei întreprinderi către care a fost externalizată prelucrarea.

Concluzie preliminară

Stabilirea „scopului" prelucrării este rezervată „operatorului". Oricine ia această decizie devine astfel operatorul (*de facto*). Stabilirea „mijloacelor" de prelucrare poate fi delegată de operator, în ceea ce privește chestiunile tehnice sau organizatorice. Chestiunile de fond, care sunt esențiale pentru legalitatea prelucrării sunt rezervate operatorului. O persoană sau o entitate care decide, de exemplu, perioada de timp în care vor fi stocate datele sau persoanele care au acces la datele prelucrate are rolul de „operator" în ceea ce privește această parte și trebuie, în consecință, să se supună tuturor obligațiilor aferente operatorului.

III.1.c) Primul element: „persoana fizică, juridică sau orice alt organism"

Primul element al definiției se referă la aspectul personal: cine poate fi operator și considerat astfel responsabil în ultimă instanță pentru obligațiile care decurg din directivă. Definiția reflectă exact formularea din articolul 2 al Convenției 108 și nu a făcut obiectul unei discuții specifice în procesul de luare a deciziilor referitor la directivă. Aceasta vizează o gamă largă de persoane care pot juca rolul de operator, de la persoane fizice la persoane juridice, inclusiv „orice alt organism".

Este important ca interpretarea acestui element să asigure aplicarea efectivă a directivei, favorizând pe cât posibil o identificare clară și explicită a operatorului în toate cazurile, indiferent dacă s-a efectuat sau s-a publicat o numire oficială.

În primul rând, este important să se urmeze cât mai îndeaproape practica stabilită atât în sectorul public, cât și în cel privat de alte domenii de drept, precum dreptul civil, administrativ și penal. În majoritatea cazurilor, aceste dispoziții vor arăta căror persoane sau organisme ar trebui să le fie alocate responsabilitățile și vor ajuta în principiu la identificarea operatorului de date.

În perspectiva strategică a alocării responsabilităților și pentru ca persoanele vizate să beneficieze de o entitate de referință mai stabilă și mai de încredere în exercitarea drepturilor lor în conformitate cu directiva, ar trebui să se considere de preferință că întreprinderea sau organismul în sine are de operator și nu o anumită persoană din cadrul întreprinderii sau al organismului. Exceptând cazul în care există elemente clare care indică responsabilitatea unei persoane fizice, se va considera în ultimă instanță că organismul sau întreprinderea este responsabilă pentru prelucrarea datelor și pentru respectarea obligațiilor ce decurg în temeiul legislației privind protecția datelor. În general, ar trebui să se presupună că organismul public sau întreprinderea este responsabilă pentru activitățile de prelucrare care au loc în domeniul său de activități și riscuri.

Uneori, întreprinderile și organismele publice desemnează o anumită persoană ca fiind responsabilă pentru punerea în aplicare a operațiunilor de prelucrare. Totuși, chiar și în cazul în care este desemnată o anumită persoană fizică pentru asigurarea conformității cu principiile de protecție a datelor sau pentru prelucrarea de date cu caracter personal, aceasta din urmă nu va avea rolul de operator, ci va acționa în numele entității juridice (întreprinderea sau organismul public) care, în calitatea sa de operator, va fi răspunzătoare în cazul încălcării principiilor[13].

În special în cazul structurilor mari și complexe, este esențial din perspectiva „guvernanței protecției datelor" să se asigure atât o responsabilitate clară a persoanei fizice care reprezintă întreprinderea, cât și responsabilități funcționale concrete în cadrul structurii, de exemplu prin desemnarea altor persoane care să acționeze în calitate de reprezentanți sau puncte de contact pentru persoanele vizate.

În cazurile în care o persoană fizică din cadrul unei persoane juridice utilizează date în scopuri proprii, în afara domeniului de activitate și a controlului posibil al activităților persoanei juridice, se impune realizarea unei analize speciale. În astfel de situații, persoana fizică în cauză ar fi operatorul în legătură cu prelucrarea asupra căreia s-a luat decizia și ar fi responsabilă pentru această utilizare a datelor cu caracter personal. Totuși, operatorul inițial ar putea să poarte o anumită responsabilitate dacă noua prelucrare ar avea loc, din cauza lipsei unor măsuri adecvate de securitate.

Astfel cum s-a menționat deja mai sus, rolul operatorului este esențial și deosebit de relevant în ceea ce privește stabilirea responsabilității și aplicarea sancțiunilor. Chiar dacă răspunderea și sancțiunile vor varia în funcție de statul membru în cauză, deoarece sunt impuse în conformitate cu legislațiile naționale, necesitatea identificării precise a persoanei fizice sau juridice responsabile pentru încălcarea legislației privind protecția datelor este, fără îndoială, o condiție prealabilă esențială pentru aplicarea eficientă a directivei.

Identificarea „operatorului" din punctul de vedere al protecției datelor va fi legată, în practică, de normele dreptului civil, administrativ sau penal care prevăd alocarea responsabilităților sau sancțiunile care pot fi impuse unei persoane fizice sau juridice[14].

Răspunderea civilă nu ar trebui să ridice probleme specifice în acest context, întrucât se aplică în principiu atât persoanelor juridice, cât și persoanelor fizice. Cu toate acestea, răspunderea penală și/sau administrativă se poate aplica uneori numai în cazul persoanelor fizice, în funcție de legislațiile naționale. În cazul în care legislația națională respectivă prevede sancțiuni penale sau administrative pentru încălcarea protecției datelor, aceasta va decide în mod normal și cine este responsabil: atunci când răspunderea penală sau administrativă a persoanelor juridice nu este recunoscută, aceasta ar putea fi preluată de funcționarii persoanelor juridice, în conformitate cu nomele specifice ale legislației naționale[15].

---

13 Un raționament similar se aplică cu privire la Regulamentul (CE) 45/2001, care în articolul 2 litera (d) se referă la „instituția sau organul comunitar, direcția generală, unitatea sau orice altă entitate organizațională". Practica de supraveghere a arătat că funcționarii instituțiilor și organismelor UE, care au fost desemnați ca „operatori", acționează în numele organismului pentru care lucrează.

14 A se vedea „Studiul comparativ al situației din cele 27 de state membre privind legea aplicabilă obligațiilor necontractuale rezultate din încălcarea vieții private și a drepturilor personalității", redactat de Comisie, în februarie 2009, disponibil la http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

15 Aceasta nu exclude posibilitatea ca legislațiile naționale să prevadă răspunderea penală sau administrativă nu numai pentru operator, ci și pentru orice persoană care încalcă legislația privind protecția datelor.

Legislația europeană conține exemple utile de criterii de atribuire a răspunderii penale[16], în special atunci când o infracțiune este comisă în folosul persoanei juridice: răspunderea poate fi atribuită în acest caz oricărei persoane, „acționând fie individual, fie ca parte a unui organ al persoanei juridice, care deține o poziție de conducere în cadrul persoanei juridice, bazată pe unul dintre următoarele elemente:
(a) puterea de reprezentare a persoanei juridice;
(b) puterea de a lua decizii în numele persoanei juridice; sau
(c) puterea de a exercita controlul în cadrul persoanei juridice."

Concluzie preliminară

Rezumând cele de mai sus, se poate concluziona că persoana responsabilă în cazul unei încălcări în ceea ce privește protecția datelor este întotdeauna operatorul, adică persoana juridică (întreprinderea sau organismul public) sau persoana fizică identificată în mod oficial în conformitate cu criteriile directivei. În cazul în care o persoană fizică din cadrul unei întreprinderi sau unui organism public utilizează datele în scopuri proprii, în afara activităților întreprinderii, persoana respectivă va fi considerată operatorul de facto și va răspunde ca atare.

Exemplul nr. 4: Monitorizarea secretă a angajaților

Un membru al consiliului director al unei întreprinderi decide să monitorizeze în secret angajații întreprinderii, chiar dacă această decizie nu este susținută în mod oficial de consiliu. Întreprinderea ar trebui considerată operator, putând face obiectul posibilelor reclamații și răspunderii pe care o implică acest lucru în relație cu angajații săi, ale căror date cu caracter personal au fost utilizate abuziv.

Răspunderea întreprinderii apare în special deoarece, în calitate de operator, aceasta are obligația de a asigura respectarea normelor de securitate și de confidențialitate. Utilizarea abuzivă de către un funcționar al întreprinderii sau de către un angajat ar putea fi considerată ca fiind rezultatul unor măsuri de securitate necorespunzătoare. Aceasta, indiferent dacă, mai târziu, respectivul membru al consiliului director sau alte persoane fizice din cadrul întreprinderii ar putea fi, de asemenea, considerate răspunzătoare, atât din punct de vedere al dreptului civil – și față de întreprindere - cât și din punct de vedere al dreptului penal. Această situație poate apărea, de exemplu, dacă respectivul membru al consiliului director ar utiliza datele colectate în scopul obținerii unor favoruri personale din partea angajaților: el ar trebui considerat ca având rolul de „operator" și răspunzător pentru utilizarea acestor date.

III.1.d) Al doilea element: „singur sau împreună cu altele"

Acest paragraf, care se bazează pe analiza anterioară a caracteristicilor tipice ale operatorului, va aborda acele cazuri în care în prelucrarea datelor cu caracter personal

[16] A se vedea, de exemplu Directiva 2008/99/CE din 19 noiembrie 2008 privind protecția mediului prin dreptul penal, Decizia-cadru a Consiliului din 13 iunie 2002 privind combaterea terorismului. Instrumentele juridice sunt fie bazate pe articolul 29 articolul 31 litera (e) și articolul 34 alineatul (2) litera (b) din TUE, fie corespund temeiurilor juridice pentru instrumentele utilizate în primul pilon, rezultând din jurisprudența CEJ în cauzele C-176/03, COM/Consiliu, Rec. 2005, p. I-7879 și C-440/05, COM/Consiliu, Clg. 2007, p. I-9097. A se vedea, de asemenea, comunicarea COM (2005) 583 final.

interacționează mai multe părți. Într-adevăr, există tot mai multe cazuri în care diferite părți acționează în calitate de operatori, iar definiția pe care o prevede directiva ia în considerare acest lucru.

Posibilitatea ca operatorul să acționeze „singur sau împreună cu altele" nu a fost menționată în Convenția 108 și a fost de fapt introdusă de Parlamentul European numai înainte de adoptarea directivei. În avizul Comisiei cu privire la amendamentul PE, Comisia face referire la posibilitatea ca „*pentru o singură operațiune de prelucrare, mai multe părți să poată stabili împreună scopul și mijloacele de prelucrare" și ca, în acest caz, „să se considere că fiecare dintre operatorii asociați este supus obligațiilor impuse prin directivă, în vederea protejării persoanelor fizice la care se referă datele prelucrate".*

Avizul Comisiei nu a reflectat pe deplin complexitatea reală a prelucrării datelor, întrucât s-a concentrat numai pe cazul în care toți operatorii stabilesc și sunt responsabili în egală măsură pentru o singură operațiune de prelucrare. În realitate, însă, acesta este numai unul dintre posibilele cazuri de „control pluralist". În acest sens, „împreună" trebuie interpretat ca însemnând „alături de" sau „nu singur", în diferite forme și combinații.

În primul rând, ar trebui remarcat faptul că probabilitatea implicării mai multor părți în prelucrarea datelor cu caracter personal este legată în mod firesc de diferitele tipuri de activități care, conform directivei, pot constitui „prelucrarea" și care, în ultimă instanță, reprezintă obiectul „controlului comun". Definiția prelucrării, conform articolului 2 litera (b) din directivă nu exclude posibilitatea implicării mai multor părți în diferite operațiuni sau serii de operațiuni privind datele cu caracter personal. Aceste operațiuni pot avea loc simultan sau în diferite etape.

Într-un mediu atât de complex, este și mai important ca rolurile și responsabilitățile să poată fi alocate cu ușurință, astfel încât complexitatea controlului comun să nu determine o distribuție inaplicabilă a responsabilităților, care ar limita eficacitatea legislației privind protecția datelor. Din păcate, din cauza diversității cazurilor posibile, este imposibil să se realizeze o listă sau o clasificare exhaustivă „închisă" a diferitelor tipuri de „control comun". Totuși, este util ca în acest context să se ofere orientări, prin prezentarea unor categorii și exemple de control comun și a unor elemente de fapt care pot indica existența unui control comun.

În general, evaluarea controlului comun ar trebui să reflecte evaluarea controlului „exclusiv" prezentat mai sus, la punctul III.1.a - c. În același sens, pentru evaluarea controlului comun ar trebui să se adopte un mod de abordare concret și funcțional, așa cum se arată mai sus, care să analizeze dacă scopurile și mijloacele sunt sau nu stabilite de mai multe părți.

Exemplul nr. 5: Instalarea unor camere de supraveghere video

Proprietarul unui imobil încheie un contract cu o societate de securitate, solicitându-i instalarea unor camere video în diverse părți ale imobilului, în numele operatorului. Scopul supravegherii video și modul în care imaginile sunt colectate și stocate sunt stabilite exclusiv de proprietarul imobilului, care trebuie astfel considerat operatorul exclusiv pentru această operațiune de prelucrare.

De asemenea, în acest context acordurile contractuale pot fi utile pentru evaluarea controlului comun, însă acestea ar trebui întotdeauna comparate cu relația efectivă dintre părți.

Exemplul nr. 6: Societăți de recrutare de personal

Societatea Headhunterz Ltd ajută întreprinderea Enterprize Inc în recrutarea de personal. Contractul precizează în mod clar că „Headhunterz Ltd va acționa în numele întreprinderii Enterprize, iar în ceea ce privește prelucrarea datelor cu caracter personal, are rolul de persoană împuternicită pentru prelucrarea datelor. Enterprize este operatorul de date exclusiv". Totuși, Headhunterz Ltd se află într-o poziție ambiguă: pe de o parte, aceasta are rolul de operator în raport cu persoanele aflate în căutarea unui loc de muncă, iar pe de altă parte își asumă rolul de persoană împuternicită care acționează în numele operatorilor, precum Enterprize Inc și alte întreprinderi care recrutează personal prin intermediul său. În plus, Headhunterz – și renumitul său serviciu cu valoare adăugată „plasare a forței de muncă la nivel global" - caută candidați potriviți atât consultând CV-urile primite direct de Enterprize, cât și cele pe care le are deja în baza sa amplă de date. Astfel, societate Headhunterz, care conform contractului este plătită numai pentru contractele efectiv semnate, crește probabilitatea de plasare a forței de muncă, sporindu-și astfel veniturile. Conform celor de mai sus, se poate concluziona că, în pofida calificării conform contractului, se consideră că Headhunterz Ltd are rolul de operator, controlând împreună cu întreprinderea Enterprize Inc cel puțin acele serii de operațiuni care se referă la recrutarea personalului pentru Enterprize.

Din această perspectivă, controlul comun apare atunci când mai multe părți stabilesc în ceea ce privește anumite operațiuni de prelucrare fie scopul, fie acele elemente esențiale ale mijloacelor care îl caracterizează pe operator (a se vedea alineatele III.1.a- c de mai sus).

Totuși, în contextul controlului comun, participarea părților la stabilirea în comun poate lua diferite forme și nu trebuie să fie în proporție egală. Într-adevăr, în cazul mai multor părți, acestea pot avea o relație foarte strânsă (repartizându-și, de exemplu, toate scopurile și mijloacele unei prelucrări) sau o relație mai puțin strânsă (repartizându-și, de exemplu, numai scopurile sau numai mijloacele, sau o parte dintre acestea). În consecință, pentru face față complexității reale a prelucrării de date, ar trebui să se ia în considerare o gamă largă de tipologii privind controlul comun, iar consecințele acestora ar trebui evaluate, cu un anumit grad de flexibilitate.

În acest context, se impune abordarea diferitelor niveluri posibile de interacțiune dintre părți pentru prelucrarea datelor cu caracter personal.

În primul rând, simplul fapt că mai multe persoane colaborează pentru prelucrarea datelor cu caracter personal, de exemplu în lanț, nu înseamnă că acestea sunt neapărat și operatori asociați, întrucât schimbul de date dintre două părți, fără ca acestea să își repartizeze scopurile sau mijloacele într-o serie comună de operațiuni, ar trebui considerat doar un transfer de date dintre doi operatori distincți.

Exemplul nr. 7: Agenție de turism (1)

O agenție de turism transmite datele personale ale clienților săi unor linii aeriene și lanțuri hoteliere, în vederea efectuării unor rezervări pentru un pachet de călătorie. Linia aeriană și hotelul confirmă disponibilitatea locurilor și camerelor solicitate. Agenția de turism emite documentele de călătorie și cupoanele pentru clienții săi. În acest caz, agenția de turism, linia aeriană și hotelul vor fi trei operatori de date distincți, fiecare dintre aceștia având obligații privind protecția datelor în legătură cu propriile procese de prelucrare.

Totuși, evaluarea poate fi diferită atunci când mai multe părți decid să creeze o infrastructură comună în vederea realizării scopurilor lor proprii. Atunci când pentru crearea acestei infrastructuri, părțile implicate stabilesc elementele esențiale ale mijloacelor care vor fi utilizate, acestea sunt calificate drept operatori asociați de date - în orice caz, într-o anumită măsură - chiar dacă nu au neapărat aceleași scopuri.

Exemplul nr. 8: Agenție de turism (2)

Agenția de turism, lanțul hotelier și linia aeriană decid să creeze o platformă comună prin internet, pentru a-și îmbunătăți cooperarea cu privire la procesul de rezervare a călătoriilor. Acestea convin asupra elementelor importante ale mijloacelor care vor fi utilizate, cum ar fi datele care vor fi stocate, modul în care vor fi alocate și confirmate rezervările și persoanele care pot avea acces la informațiile stocate. În plus, acestea decid să utilizeze în comun datele privind clienții lor, în vederea realizării unor acțiuni de marketing integrate.

În acest caz, agenția de turism, linia aeriană și lanțul hotelier vor controla în comun modul în care sunt prelucrate datele personale ale clienților lor și vor avea astfel rolul de operatori asociați în ceea ce privește operațiunile de prelucrare în legătură cu platforma comună de rezervări prin internet. Totuși, fiecare va deține controlul exclusiv în ceea ce privește alte activități de prelucrare, de exemplu cele legate de managementul resurselor umane.

În unele cazuri, mai multe părți prelucrează aceleași date personale pe rând. În aceste cazuri, la nivel micro, diferitele operațiuni de prelucrare ar putea părea a avea nicio legătură, deoarece fiecare ar putea avea un alt scop. Totuși, este necesar să se mai verifice încă o dată dacă la nivel macro aceste operațiuni de prelucrare nu ar trebui considerate „serii de operațiuni”, care au un scop comun sau utilizează niște mijloace stabilite în comun.

Următoarele două exemple clarifică această idee, prezentând două posibile scenarii diferite.

Exemplul nr. 9: Transfer de date privind angajații către autoritățile fiscale

Întreprinderea XYZ colectează și prelucrează date cu caracter personal cu privire la angajații săi în scopul gestionării salariilor, îndatoririlor, asigurărilor de sănătate etc. Totuși, conform legii, întreprinderea trebuie să transmită toate datele cu privire la salarii către autoritățile fiscale, în vederea consolidării controlului fiscal.

În acest caz, chiar dacă întreprinderea XYZ și autoritățile fiscale prelucrează aceleași date cu privire la salarii, lipsa unui scop comun sau a unor mijloace comune cu privire la prelucrarea datelor va conduce la considerarea celor două entități ca doi operatori de date distincți.

Exemplul nr. 10: Tranzacții financiare

Să luăm în schimb cazul unei bănci care utilizează un agent financiar pentru realizarea tranzacțiilor sale financiare. Banca și agentul convin asupra mijloacelor de prelucrare a datelor financiare. Prelucrarea datelor personale cu privire la tranzacțiile financiare este realizată inițial de către instituția financiară și numai ulterior de agentul financiar. Totuși, chiar dacă la nivel micro fiecare subiect își urmărește propriul scop, la nivel macro, diferitele etape, scopurile și mijloacele de prelucrare sunt strâns legate. În acest caz, atât banca, cât și agentul pot fi considerați operatori asociați.

În alte cazuri, diferitele părți implicate stabilesc în comun, uneori într-o anumită măsură, scopurile și/sau mijloacele unei operațiuni de prelucrare.

Există cazuri în care fiecare operator răspunde numai de o parte a prelucrării, dar informațiile sunt compilate și prelucrate în cadrul unei platforme.

Exemplul nr. 11: Portaluri de e-guvernare

Portalurile de e-guvernare au rolul de intermediari între cetățeni și unitățile de administrație publică: portalul transferă cererile cetățenilor și păstrează documentele unității de administrație publică până când acestea sunt solicitate de cetățean. Fiecare unitate de administrație publică rămâne operatorul datelor prelucrate în scopuri proprii. Cu toate acestea, portalul în sine poate fi de asemenea considerat operator. Într-adevăr, acesta prelucrează (colectează și transferă către unitatea competentă) cererile cetățenilor și documentele publice (le păstrează și reglementează accesul la acestea, ca de exemplu descărcarea lor de către cetățeni) pentru alte scopuri (facilitarea serviciilor de e-guvernare) decât cele pentru care datele sunt prelucrate inițial de fiecare unitate de administrație publică. Printre obligațiile acestor operatori se numără obligația de a se asigura că sistemul de transfer al datelor cu caracter personal de la utilizator în sistemul administrației publice este sigur, întrucât, la nivel macro, acest transfer reprezintă o parte esențială a seriei de operațiuni de prelucrare realizate prin intermediul portalului.

O altă structură posibilă este „abordarea bazată pe origine”, care apare atunci când fiecare operator este responsabil pentru datele pe care le introduce în sistem. Este cazul unor baze de date la nivelul UE, unde controlul - și astfel obligația de a da curs cererilor de acces și rectificare – este atribuit pe baza originii naționale a datelor personale.

Rețelele de socializare online oferă un alt scenariu interesant.

Exemplul nr. 12: Rețelele de socializare

Furnizorii de servicii de socializare în rețea oferă platforme de comunicare online care le permit utilizatorilor să publice și să facă schimb de informații. Acești furnizori de servicii sunt operatori de date, întrucât stabilesc atât scopurile, cât și mijloacele de prelucrare a acestor informații. Utilizatorii acestor rețele, care încarcă și date personale ale unor terți, ar putea juca rolul de operatori cu condiția ca activitățile lor să nu facă obiectul așa-numitei „excepții privind activitățile domestice”[17].

După analizarea acelor cazuri în care diferiții subiecți stabilesc împreună doar o parte din scopuri și mijloace, un caz foarte precis și care nu ridică probleme este cel în care mai mulți subiecți stabilesc în comun și au aceleași scopuri și mijloace de prelucrare, având astfel un control comun deplin.

În ultimul caz, este ușor de stabilit cine este competent și în măsură să asigure drepturile persoanelor vizate și să se supună obligațiilor privind protecția datelor. Totuși, sarcina de a stabili care operator este competent - și răspunzător – pentru ce drepturi și obligații ale persoanelor vizate este mult mai complexă atunci când diferiții operatori asociați împărtășesc scopurile și mijloacele de prelucrare în mod asimetric.

Necesitatea de a clarifica distribuția controlului

În primul rând, ar trebui să se precizeze că, în special în cazurile în care există un control comun, incapacitatea de îndeplinire directă a tuturor obligațiilor aferente operatorului (asigurarea informațiilor, dreptul de acces etc.) nu exclude statutul de operator. Practic, acele obligații ar putea fi cu ușurință îndeplinite de alte părți, care sunt uneori mai apropiate de persoana vizată, în numele operatorului. Totuși, operatorul este cel care va răspunde în cele din urmă de îndeplinirea obligațiilor și care va fi răspunzător în cazul încălcării acestora.

Conform unui text anterior prezentat de Comisie în timpul procesului de adoptare a directivei, accesul la anumite date cu caracter personal ar determina calificarea de operator (asociat) în legătură cu aceste date. Totuși, textul final nu a păstrat această formulare, iar experiența arată că, pe de o parte, accesul la date nu determină controlul, în timp ce, pe de altă parte, accesul la date nu este o condiție esențială pentru funcția de operator. În consecință, în sistemele complexe, în care sunt implicate mai multe părți, accesul la datele personale și alte drepturi privind persoanele vizate pot fi asigurate la diferite niveluri de către diverși actori.

Consecințele juridice sunt legate și de răspunderea operatorilor, punându-se în special problema dacă acel „controlul comun” prevăzut în directivă atrage întotdeauna răspunderea în solidar. Articolul 26 cu privire la răspundere utilizează termenul de „operator” la singular, ceea ce indică un răspuns pozitiv. Totuși, așa cum s-a menționat deja, în realitate pot exista diferite moduri de a acționa „împreună”. Aceasta ar putea determina în anumite cazuri răspunderea în solidar, însă nu în mod necesar: de multe ori, diferiții operatori pot fi responsabili - și astfel răspunzători – pentru prelucrarea datelor personale în diferite etape și în grade diferite.

[17] Pentru mai multe detalii și exemple, a se vedea Avizul 5/2009 privind socializarea în rețea online, al Grupului de lucru instituit în temeiul articolului 29, adoptat la 12 iunie 2009 (GL 163)

Concluzia este că ar trebui să se asigure că și în cazul mediilor complexe de prelucrare a datelor, în care diferiți operatori au un anumit rol în prelucrarea datelor cu caracter personal, respectarea normelor de protecție a datelor și răspunderea determinată de posibila încălcare a acestor norme sunt repartizate în mod clar, pentru a evita diminuarea protecției datelor personale sau apariția unui „conflict negativ de competență" și a unor lacune din cauza cărora unele obligații sau drepturi care decurg din directivă nu sunt asigurate de oricare dintre părți.

În aceste cazuri, mai mult decât oricând, este important ca persoanele vizate să fie informate clar cu privire la diferitele etape și diferitele părți implicate în prelucrare. În plus, ar trebui precizat dacă fiecare operator are competența de a respecta toate drepturile persoanei vizate sau ce drept intră în sfera de competență a fiecărui operator.

Exemplul nr. 13: Bănci și resurse comune de informații privind clienții restanțieri

Mai multe bănci ar putea stabili un „fond comun de informații" – în cazul în care legislația națională permite acest lucru – în cadrul căruia fiecare bancă contribuie cu informații (date) privind clienții restanțieri și toate băncile au acces deplin la informații. Unele legislații prevăd ca toate cererile persoanelor vizate, de exemplu privind accesul la date sau ștergerea acestora, să se adreseze numai unui „punct de intrare", furnizorul. Furnizorul răspunde de identificarea corectă a unui operator și de asigurarea unor răspunsuri adecvate pentru persoana vizată. Identitatea furnizorului este publicată în Registrul de prelucrare a datelor. În alte jurisdicții, aceste resurse comune de informații ar putea fi operate de entități juridice distincte acționând în calitate de operator, iar cererile privind accesul persoanelor vizate vor fi tratate de băncile participante, în calitate de intermediar al operatorului.

Exemplul nr. 14: Publicitatea comportamentală

Publicitatea comportamentală utilizează informațiile cu privire la comportamentul de navigare pe internet al unei persoane, cum ar fi paginile vizitate sau căutările efectuate, în vederea selectării mesajelor publicitare pentru acea persoană. Atât editorii, care închiriază adesea spații publicitare pe site-urile lor, cât și furnizorii de rețele publicitare, care publică în aceste spații mesaje publicitare adresate unui anumit public, pot colecta și schimba informații privind utilizatorii, în funcție de acordurile contractuale în cauză.

Din punctul de vedere al protecției datelor, editorul trebuie considerat ca fiind un operator autonom, în măsura în care colectează date cu caracter personal de la utilizator (profilul utilizatorului, adresa IP, amplasamentul, limba sistemului de operare etc.) în scopuri proprii. Furnizorul rețelei publicitare va avea de asemenea rolul de operator în măsura în care stabilește scopurile (monitorizarea utilizatorilor pe site-uri) sau mijloacele esențiale pentru prelucrarea datelor. În funcție de condițiile colaborării dintre editor și furnizorul rețelei publicitare, de exemplu dacă editorul permite transferul de date personale către furnizorul rețelei publicitare, inclusiv printr-o redirecționare a utilizatorului către pagina de internet a furnizorului rețelei publicitare, , de exemplu, aceștia ar putea avea rolul de operatori asociați pentru setul de operațiuni de prelucrare care conduc la publicitatea comportamentală.

În orice caz, operatorii (asociați) se asigură că aspectele tehnice și complexitatea sistemului publicității comportamentale nu îi împiedică să își respecte obligațiile care le revin în calitate de operatori și să asigure drepturile persoanelor vizate.

Aceasta ar include, în special, următoarele:

- *informarea* utilizatorului cu privire la faptul că datele acestuia pot fi accesate de un terț: această operațiune ar putea fi realizată cu mai mare eficiență de către editor, deoarece acesta este principalul interlocutor al utilizatorului,
- și condițiile de *acces* la datele cu caracter personal: societatea publicitară ar trebui să răspundă la cererile utilizatorilor cu privire la modul în care se realizează publicitatea adresată unui anumit public pe baza datelor utilizatorilor și să răspundă cererilor de rectificare și de ștergere.

În plus, editorii și furnizorii de rețele publicitare ar putea să se supună și altor obligații, în temeiul legislației privind protecția civilă și protecția consumatorilor, inclusiv legislația privind responsabilitatea civilă delictuală și practicile comerciale neloiale.

Concluzie preliminară

Părțile care acționează în comun au un anumit grad de flexibilitate în ceea ce privește repartizarea și alocarea obligațiilor și responsabilităților, cu condiția ca acestea să asigure o conformitate deplină. Normele privind modul în care sunt exercitate responsabilitățile comune ar trebui să fie, în principiu, stabilite de către operatori. Totuși, în acest caz ar trebui să se țină seama și de circumstanțele efective, pentru a se stabili dacă acordurile reflectă realitatea prelucrării datelor de bază.

În acest sens, evaluarea controlului comun ar trebui să ia în considerare, pe de o parte, necesitatea respectării depline a normelor privind protecția datelor și, pe de altă parte, faptul că creșterea numărului de operatori ar putea determina, de asemenea, situații complexe nedorite și o posibilă lipsă de claritate în ceea ce privește alocarea responsabilităților. Aceasta ar putea conduce la o situație în care întregul proces ar fi nelegal din cauza lipsei de transparență, încălcându-se astfel principiului privind prelucrarea echitabilă a datelor.

Exemplul nr. 15: Platforme de gestionare a datelor medicale

Într-un stat membru, o autoritate publică instituie un punct național de centralizare care reglementează schimbul de date privind pacienții dintre furnizorii de servicii medicale. Existența mai multor operatori – zeci de mii – determină o situație atât de ambiguă pentru persoanele vizate (pacienți), încât protecția drepturilor acestora este pusă în pericol. Într-adevăr, persoanele vizate nu ar ști cui să se adreseze în caz de reclamații, întrebări, cereri de informații, rectificări sau în cazul accesului la datele personale. În plus, autoritatea publică răspunde de prelucrarea efectivă și de modul în care este utilizată. Aceste elemente conduc la concluzia că autoritatea publică care instituie punctul național de centralizare este considerată ca având rolul de operator asociat, precum și de punct de contact pentru solicitările persoanelor vizate.

În acest context, se poate afirma că răspunderea solidară a tuturor părților implicate ar trebui considerată un mijloc de eliminare a incertitudinilor și ar trebui astfel asumată numai în măsura în care părțile implicate nu au stabilit o altă modalitate alternativă la fel de eficientă de alocare a obligațiilor și a responsabilităților sau aceasta nu decurge în mod evident din circumstanțele de fapt.

III.2. Definiția persoanei împuternicite de către operator

Conceptul de persoană împuternicită de către operator nu era prevăzut în Convenția 108. Rolul persoanei împuternicite este pentru prima dată recunoscut în prima propunere a Comisiei, însă fără ca acest concept să fie introdus, în vederea „*evitării situațiilor în care prelucrarea datelor de către un terț, în numele operatorului dosarului, duce la reducerea nivelului de protecție de care se bucură persoana vizată"*. Conceptul de persoană împuternicită de către operator este precizat în mod explicit și autonom numai odată cu propunerea modificată a Comisiei și în urma unei propuneri din partea Parlamentului European, înainte de formularea actuală din poziția comună a Consiliului.

În aceeași măsură ca în cazul definiției operatorului, definiția persoanei împuternicite de operator are în vedere o gamă largă de actori care pot avea rolul de persoană împuternicită de către operator („…persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism").

Existența unei persoane împuternicite de către operator depinde de decizia operatorului, care poate decide fie să prelucreze datele în cadrul propriei sale organizații, de exemplu prin intermediul personalului autorizat să prelucreze datele sub directa sa autoritate [a se vedea *a contrario* articolul 2 litera (f)], fie să delege toate activitățile de prelucrare sau o parte dintre acestea unei organizații externe, adică – așa cum se precizează în expunerea de motive din propunerea modificată a Comisiei – „o persoană juridică distinctă care acționează în numele său".

În consecință, persoana împuternicită de operator trebuie să îndeplinească două condiții de bază – pe de o parte, să fie o entitate juridică distinctă în raport cu operatorul și, pe de altă parte, să prelucreze datele personale în numele acestuia. Această activitate de prelucrare se poate limita la o sarcină foarte specifică sau la un context foarte specific sau poate fi mai generală și mai extinsă.

În plus, rolul persoanei împuternicite de către operator nu se bazează pe tipul entității care prelucrează datele, ci pe activitățile sale concrete dintr-un anumit context. Cu alte cuvinte, aceeași entitate poate avea în același timp rolul de operator pentru anumite operațiuni de prelucrare și rolul de persoană împuternicită pentru altele, iar calificarea acesteia ca operator sau persoană împuternicită trebuie evaluată în raport cu anumite serii de date sau de operațiuni.

Exemplul nr. 16: Furnizorii de servicii de internet de găzduire

Un furnizor de servicii de internet (ISP) care oferă servicii de găzduire este în principiu o persoană împuternicită în ceea ce privește datele personale publicate online de către clienții săi care utilizează acest ISP pentru găzduirea și întreținerea site-ului lor internet. Totuși, dacă furnizorul de servicii de internet prelucrează datele cuprinse în site-urile web în scopuri personale, atunci acesta are rolul de operator de date cu privire la acea operațiune de prelucrare. Această analiză este diferită de cazul unui ISP care oferă servicii de e-mail sau de acces la internet (a se vedea, de asemenea, exemplul nr. 1: operatorii de telecomunicații).

Cel mai important element este dispoziția conform căreia persoana împuternicită acționează „…în numele operatorului…". A acționa în numele cuiva înseamnă a servi interesul acelei persoane și amintește de conceptul juridic de „delegare". În cazul legislației privind protecția datelor, persoana împuternicită este numită pentru a aplica

instrucțiunile emise de operator cel puțin în ceea ce privește scopul operațiunii de prelucrare și elementele esențiale ale mijloacelor.

În acest sens, caracterul legal al activității de prelucrare a persoanei împuternicite se stabilește în funcție de mandatul încredințat de operator. Persoana împuternicită care își depășește atribuțiile și care dobândește un rol semnificativ în ceea ce privește stabilirea scopurilor sau a mijloacelor esențiale ale operațiunii de prelucrare are mai degrabă rolul de operator (asociat) și nu de persoană împuternicită. Problema legitimității acestei operațiuni de prelucrare va fi totuși evaluată în temeiul altor articole (6-8). Totuși, delegarea poate implica un anumit grad de libertate de decizie cu privire la modul în care interesele operatorului pot fi cât mai bine servite, persoana împuternicită putând alege mijloacele tehnice și organizaționale cele mai adecvate.

Exemplul nr. 17: Externalizarea serviciilor poștale

Mai multe organisme private furnizează servicii poștale în numele unor agenții (publice) – de exemplu, expedierea prin poștă a alocațiilor familiale și a alocațiilor de maternitate, în numele agenției naționale de securitate socială. În acest caz, o autoritate de protecție a datelor a precizat că organismele private respective ar trebui să aibă rolul de persoane împuternicite, având în vedere că îndatorirea acestora, deși exercitată cu un anumit grad de autonomie, se limitează doar la o parte din operațiunile de prelucrare necesare în scopul stabilit de operatorul de date.

Tot pentru a asigura că externalizarea și delegarea atribuțiilor nu determină un standard mai puțin strict de protecție a datelor, directiva cuprinde două prevederi care se adresează în mod specific persoanei împuternicite și care stabilesc foarte amănunțit obligațiile acesteia cu privire la confidențialitate și securitate.

- Articolul 16 stabilește că persoana împuternicită, precum și orice persoană care acționează sub autoritatea acesteia și care are acces la datele cu caracter personal, nu trebuie să le prelucreze decât dacă operatorul solicită acest lucru.

- Articolul 17, privind securitatea prelucrărilor, stabilește necesitatea unui contract sau a unui instrument juridic obligatoriu care să reglementeze relațiile dintre operatorul de date și persoana împuternicită. Acest contract este în formă scrisă, pentru a fi păstrat ca dovadă și are un conținut minimal, stipulând în special că persoana împuternicită acționează numai la cererea operatorului și pune în aplicare măsurile tehnice și organizatorice în vederea protejării adecvate a datelor cu caracter personal. Contractul ar trebui să includă o descriere suficient de detaliată a împuternicirii acordate persoanei în cauză.

În acest sens, ar trebui remarcat că în multe cazuri furnizorii de servicii specializați în anumite prelucrări de date (de exemplu, plata salariilor) vor stabili servicii și contracte standard pentru operatorii de date, stabilind de fapt o modalitate standard de prelucrare a datelor cu caracter personal[18]. Totuși, faptul că un contract și condițiile detaliate ale acestuia sunt redactate de către furnizorul de servicii și nu de către operator nu reprezintă *în sine* un temei suficient pentru a concluziona că furnizorul de servicii ar trebui considerat ca având rolul de operator, în măsura în care operatorul a acceptat de bună voie condițiile contractuale, acceptând astfel deplina responsabilitate în acest sens.

[18] Elaborarea condițiilor contractuale de furnizorul de servicii nu aduce atingere faptului că aspectele esențiale ale prelucrării, astfel cum se arată la punctul III.1.b, sunt stabilite de operator.

Din aceeași perspectivă, diferența dintre puterea contractuală a unui mic operator de date în raport cu marii furnizori de servicii nu ar trebui să justifice acceptarea de către operator a unor clauze și condiții contractuale neconforme cu legislația privind protecția datelor.

Exemplul nr. 18: Platforme de e-mail

John Smith caută o platformă de e-mail pentru el și pentru cei cinci angajați ai întreprinderii sale. Acesta descoperă că o platformă adecvată, ușor de utilizat - și de altfel singura gratuită - păstrează datele personale un timp foarte îndelungat și le transferă în țări terțe fără să fie adoptate măsuri de siguranță adecvate. În plus, condițiile contractuale nu sunt negociabile.

În acest caz, dl Smith ar trebui fie să caute un alt furnizor, fie – în cazul unei presupuse nerespectări a normelor privind protecția datelor sau a absenței altor furnizori adecvați pe piață – să sesizeze autoritățile competente, precum autoritățile de protecție a datelor, autoritățile antitrust etc., cu privire la această problemă.

Faptul că directiva impune existența un contract scris pentru a asigura securitatea prelucrării nu înseamnă că nu pot exista relații între operatorii/persoanele împuternicite în lipsa unor contracte prealabile. În acest sens, contractul nu este nici esențial, nici decisiv, chiar dacă ar putea ajuta la o înțelegere mai bună a relațiilor dintre părți[19]. Prin urmare, chiar și în acest caz, se adoptă o abordare funcțională, care analizează elementele efective ale relațiilor dintre diferiții subiecți și felul în care sunt stabilite scopurile și mijloacele de prelucrare. În cazul în care pare să existe o relație între operator și persoana împuternicită, aceste părți sunt obligate să încheie un contract în conformitate cu legea (a se vedea articolul 17 din directivă).

Existența mai multor persoane împuternicite

Există din ce mai multe cazuri în care operatorul externalizează prelucrarea datelor personale mai multor persoane împuternicite. Aceste persoane pot avea o relație directă cu operatorul de date sau pot fi subcontractanți, cărora persoanele împuternicite le-au delegat o parte din activitățile de prelucrare care le-au fost încredințate.

Odată cu dezvoltarea unor noi tehnologii, există tot mai multe structuri complexe (care se desfășoară pe mai multe niveluri sau sunt larg răspândite) de prelucrare a datelor personale, iar unele legislații naționale fac referire explicită la acestea. Directiva nu prevede ca, din motive organizaționale, să nu poată fi desemnate mai multe entități în calitate de persoane împuternicite sau de subcontractanți, prin subdivizarea sarcinilor relevante. Totuși, în cadrul prelucrării datelor, toate aceste persoane trebuie să respecte instrucțiunile operatorului de date.

[19] Totuși în anumite cazuri, existența unui contract scris poate constitui o condiție necesară pentru calificarea automată a unei persoane împuternicite în anumite situații. În Spania, de exemplu, raportul privind centrele de apel stabilește că toate centrele de apel din țările terțe au rolul de persoane împuternicite, cu condiția să respecte contractul. Acest lucru este valabil chiar dacă persoana împuternicită întocmește contractul, iar operatorul doar îl „acceptă".

Exemplul nr. 19: Rețele informatice

Marile infrastructuri de cercetare utilizează tot mai mult sistemele informatice distribuite, în special rețelele informatice, pentru a beneficia de capacitatea de calcul și de stocare. Rețelele sunt instalate în diferite infrastructuri de cercetare stabilite în diverse țări. De exemplu, o rețea europeană poate cuprinde mai multe rețele naționale care, la rândul lor, se află sub responsabilitatea unui organism național. Este posibil însă ca această rețea europeană să nu aibă un organism central, responsabil de funcționarea sa. Cercetătorii care utilizează o astfel de rețea nu pot de obicei stabili unde anume sunt prelucrate datele lor și astfel cine este persoana responsabilă de prelucrarea datelor (situația este și mai complicată dacă există infrastructuri de rețele în țări terțe). Dacă o infrastructură de rețele utilizează datele în mod neautorizat, această parte poate fi considerată operatorul de date, în cazul în care nu acționează în numele cercetătorilor.

Aspectul strategic în cazul de față este faptul că, având în vedere că există mai multe părți implicate în acest proces, obligațiile și responsabilitățile care decurg din legislația privind protecția datelor ar trebui alocate în mod clar și nu dispersate de-a lungul lanțului de furnizori de servicii externalizate/subcontractanți. Cu alte cuvinte, ar trebui să se evite existența unui lanț de subcontractanți, care ar diminua sau chiar ar împiedica controlul eficient și responsabilitatea clară pentru activitățile de prelucrare, ci excepția cazului în care responsabilitățile diferitelor părți din cadrul lanțului sunt clar stabilite.

Din aceeași perspectivă, în același sens cu alineatul III.1.b de mai sus – deși nu este necesar ca operatorul să stabilească și să aprobe toate detaliile privind mijloacele utilizate pentru atingerea scopurilor propuse – totuși, acesta ar trebui cel puțin informat cu privire la elementele principale ale structurii prelucrării (de exemplu, cu privire la persoanele implicate, măsurile de securitate, garanțiile prelucrării în țările terțe etc.), astfel încât să fie în măsură să controleze datele prelucrate în numele său.

Ar trebui, de asemenea, să se aibă în vedere că deși directiva stabilește ca răspunderea să îi revină operatorului, aceasta nu împiedică legislațiile naționale privind protecția datelor să prevadă ca persoana împuternicită să fie de asemenea responsabilă în anumite cazuri.

Pentru a stabili dacă diferitele persoane implicate se califică sau nu, există câteva criterii care pot fi utile:

- nivelul instrucțiunilor emise de operatorul de date, care stabilesc marja de manevră a persoanei împuternicite ;

- monitorizarea de către operatorul de date a modului în care serviciile sunt executate. În cazul în care operatorul efectuează o supraveghere constantă și atentă, pentru a se asigura că persoana împuternicită respectă pe deplin instrucțiunile clauzelor contractuale înseamnă că acesta deține încă un control deplin și exclusiv al operațiunilor de prelucrare;

- vizibilitatea/imaginea pe care operatorul o oferă persoanei vizate și așteptările persoanelor vizate pe baza acestei vizibilități.

Exemplul nr. 20: Centre de apeluri

Un operator de date își externalizează o parte din operațiuni către un centru de apeluri care utilizează identitatea operatorului de date atunci când apelează clienții acestuia. În acest caz, având în vedere așteptările clienților și modul în care operatorul se prezintă prin intermediul societății care prestează serviciile externalizate, se poate formula concluzia că societatea respectivă funcționează ca persoană împuternicită în numele operatorului.

- Expertiza părților: în anumite cazuri, rolul tradițional și expertiza profesională a furnizorului de servicii are un rol predominant, care poate atrage calificarea acestuia ca operator.

Exemplul nr. 21: Avocați

Un avocat își reprezintă clientul în instanță și, în acest sens, prelucrează datele personale legate de cazul clientului său. Temeiul juridic pe baza căruia utilizează informațiile necesare este împuternicirea din partea clientului. Totuși, împuternicirea nu se concentrează pe prelucrarea datelor, ci pe reprezentarea clientului în instanță, activitate pentru care astfel de profesii au în mod tradițional propriul temei juridic. În consecință, persoanele care exercită astfel de profesii trebuie considerate „operatori" independenți atunci când prelucrează datele în timpul reprezentării legale a clienților lor.

Într-un context diferit, o evaluare mai detaliată a mijloacelor utilizate pentru atingerea scopurilor ar putea fi, de asemenea, decisivă.

Exemplul nr. 22: Site-uri internet pentru obiecte pierdute și găsite

Un site web pentru obiecte pierdute și găsite a fost prezentat ca având simplul rol de „persoană împuternicită", deoarece persoanele care publică obiectele pierdute stabilesc conținutul său și, la nivel micro, scopul (de exemplu, găsirea unei broșe, a unui papagal etc.). O autoritate de protecție a datelor a respins acest argument. Site-ul a fost înființat în scopul obținerii unui profit din publicarea obiectelor pierdute, iar faptul că acesta nu a stabilit ce obiecte anume urmau să fi publicate (spre deosebire de categorii de obiecte) nu era esențial, deoarece definiția „operatorului de date" nu include în mod expres obligația de a stabili conținutul. Site-ul stabilește condițiile de publicare etc. și răspunde de caracterul adecvat al conținutului.

Deși ar fi putut exista o tendință generală de identificare a furnizorilor de servicii externalizate ca persoane împuternicite, în prezent situațiile și evaluările sunt adesea mult mai complexe.

Exemplul nr. 23: Contabilii

Calificarea contabililor poate varia în funcție de context. În cazul în care contabilii oferă servicii publicului general și micilor comercianți pe baza unor instrucțiuni foarte generale („pregătiți declarațiile mele de venit”), aceștia – la fel ca avocații care acționează în circumstanțe similare și din motive similare – vor avea rolul de operatori de date. Totuși, atunci când contabilul este angajat de o firmă și trebuie să se supună instrucțiunilor detaliate ale contabilului firmei, cum ar fi realizarea unui audit detaliat, atunci acesta, dacă nu este un angajat permanent, va avea rolul de persoană împuternicită, având în vedere instrucțiunile clare și libertatea sa limitată de acțiune. Totuși, există o condiție majoră, și anume faptul că atunci când contabilii consideră că au detectat practici ilegale pe care sunt obligați să le raporteze, având în vedere obligațiile lor profesionale, aceștia acționează independent în calitate de operatori.

Uneori, având în vedere complexitatea operațiunilor de prelucrare, se poate pune mai mult accentul pe marja de manevră a persoanelor cărora le-a fost încredințată prelucrarea datelor cu caracter personal, de exemplu atunci când prelucrarea acestor date implică un anumit risc asupra vieții private. Introducerea unor noi mijloace de prelucrare ar putea determina mai degrabă calificarea ca operator de date decât ca persoană împuternicită. Aceste cazuri ar putea determina de asemenea clarificarea - și desemnarea operatorului – în mod explicit, prin lege.

Exemplul nr. 24: Prelucrarea în scopuri istorice, științifice și statistice

Legislația națională ar putea introduce, cu privire la prelucrarea datelor cu caracter personal în scopuri istorice, științifice și statistice, noțiunea de organizație intermediară, pentru a desemna organismul responsabil pentru transformarea datelor necodificate în date codificate, astfel încât operatorul prelucrării în scopuri istorice, științifice și statistice să nu poată reidentifica persoanele vizate.

Dacă mai mulți operatori din cadrul operațiunilor inițiale de prelucrare transmit date către unul sau mai mulți terți, în vederea prelucrării ulterioare a acestora în scopuri istorice, științifice sau statistice, datele sunt în primul rând codificate de o organizație intermediară. În acest caz, organizația intermediară poate fi considerată ca având rolul de operator, în conformitate cu anumite reglementări naționale, făcând obiectul tuturor obligațiilor aferente (relevanța datelor, informarea persoanei vizate, notificare etc.). Aceasta se justifică prin faptul că atunci când datele provenite din diferite surse sunt puse împreună, protecția datelor poate fi pusă în pericol, justificând responsabilitatea organizației intermediare. În consecință, se consideră că aceasta nu are simplul rol de persoană împuternicită, ci rolul deplin de operator, în conformitate cu legislația națională.

În același sens, puterea autonomă de luare a deciziilor a diferitelor părți implicate în prelucrare are un rol semnificativ. Cazul testelor clinice asupra medicamentelor arată că relația dintre societățile sponsor și entitățile externe care au primit sarcina de a efectua testele depinde de libertatea de acțiune a entităților externe cu privire la prelucrarea datelor. Aceasta înseamnă că pot exista mai mulți operatori, dar și mai multe persoane împuternicite să realizeze prelucrarea.

Exemplul nr. 25: Studiile clinice pentru medicamente

Societatea farmaceutică XYZ sponsorizează o serie de studii clinice pentru anumite medicamente și alege centrele de studiu candidate evaluând eligibilitatea și interesele acestora; aceasta întocmește protocolul studiului, transmite centrelor îndrumările necesare cu privire la prelucrarea datelor și verifică respectarea de către centre a protocolului și a procedurilor interne respective.

Deși sponsorul nu colectează datele în mod direct, acesta obține datele cu privire la pacienți de la centrele de testare și le prelucrează în diferite moduri (evaluând informațiile din documentele medicale, primind datele cu privire la reacțiile adverse, introducând aceste date în baza de date relevantă, realizând analize statistice în vederea obținerii rezultatelor testului). Centrul de studiu efectuează studiul în mod autonom – respectând însă îndrumările sponsorului, îi informează pe pacienți și obține acordul acestora cu privire la prelucrarea datelor lor, le permite colaboratorilor sponsorului să acceseze documentele medicale originale ale pacienților în vederea monitorizării acestora și este responsabil de păstrarea în siguranță a documentelor. În consecință, se pare că responsabilitățile revin unor părți distincte.

În acest context, atât centrele de studiu, cât și sponsorii iau hotărâri importante cu privire la modul în care sunt prelucrate datele cu caracter personal în legătură cu studiile clinice. Prin urmare, se poate considera că aceștia au rolul de operatori de date asociați. Relația dintre sponsor și centrele de studiu ar putea fi interpretată diferit în cazurile în care sponsorul stabilește scopurile și elementele esențiale ale mijloacelor, iar cercetătorului nu îi rămâne decât o marjă foarte limitată de manevră.

III.3. Definiția terțului

Conceptul de „terț” nu a fost prevăzut în Convenția 108, ci a fost introdus în propunerea modificată a Comisiei în urma unui amendament propus de Parlamentul European. Conform expunerii de motive, amendamentul a fost reformulat pentru a preciza că terții nu includ persoana vizată, operatorul sau orice persoană autorizată să prelucreze datele sub autoritatea directă a operatorului sau în numele acestuia, astfel cum se întâmplă în cazul persoanei împuternicite. Aceasta înseamnă că „*persoanele care lucrează pentru o altă organizație, chiar dacă aceasta aparține aceluiași grup sau holding, vor fi în general considerate părți terțe”* în timp ce, pe de altă parte, „*filialele unei bănci care se ocupă de conturile clienților sub autoritatea directă a băncii centrale nu sunt considerate părți terțe”*.

Directiva utilizează termenul de „terț” într-un mod care nu diferă de modul în care acest concept este utilizat în mod normal în dreptul civil, unde terțul este de obicei o persoană care nu face parte dintr-o entitate sau parte la un acord. În contextul protecției datelor, acest concept ar trebui interpretat cu referire la orice persoană care nu are o autoritate sau o autorizare specifică - care are putea decurge, de exemplu, din calitatea acesteia de operator, persoană împuternicită sau angajat al acestora – cu privire la prelucrarea datelor cu caracter personal.

Directiva utilizează acest concept în numeroase prevederi, de obicei în vederea stabilirii unor interdicții, restricții și obligații pentru situațiile în care datele personale ar putea fi prelucrate de alte părți care cărora nu li se permite prelucrarea anumitor date personale.

În acest context, se poate concluziona că un terț care primește date cu caracter personal – în mod legal sau ilegal – ar fi în principiu un nou operator, cu condiția să fie respectate celelalte condiții pentru calificarea ca operator și legislația privind protecția datelor.

Exemplul nr. 26: Accesul neautorizat al unui angajat

Un angajat al unei societăți ajunge să cunoască, în îndeplinirea sarcinilor sale, date personale pe care nu are dreptul să le acceseze. În acest caz, acest angajat ar trebui considerat „terț" în raport cu angajatorul său, cu toate consecințele și responsabilitățile aferente în termeni de legalitate a comunicării și prelucrării datelor.

IV. Concluzii

Conceptul de operator de date și interacțiunea acestuia cu conceptul de persoană împuternicită au un rol esențial în aplicarea Directivei 95/46/CE, deoarece acestea stabilesc cine va fi responsabil de respectarea normelor privind protecția datelor, modul în care persoanele vizate își pot exercita drepturile, care este legislația națională aplicabilă și cât de eficient pot opera autoritățile de protecție a datelor.

Diferențierea organizațională atât în sectorul public, cât și în cel privat, dezvoltarea TIC și globalizarea prelucrării datelor sporesc complexitatea modului în care sunt prelucrate datele personale și necesită clarificarea acestor concepte, pentru a asigura aplicarea eficientă și conformitatea în practică.

Conceptul de operator este autonom, în sensul că ar trebui interpretat în principal în conformitate cu legislația comunitară privind protecția datelor și funcțional, în sensul că urmărește să aloce responsabilitățile acolo unde există o influență efectivă, bazându-se astfel pe o analiză de fapt și nu pe o analiză formală.

Definiția din directivă cuprinde trei piloni principali: aspectul personal („*persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism*"); posibilitatea unui control pluralist („*care, singur sau împreună cu altele*"); și elementele esențiale care fac deosebirea dintre operator și alți actori („*stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal*").

Analiza acestor piloni conduce la următoarele concluzii principale:

- Capacitatea de a „*stabili* scopurile și mijloacele …" ar putea decurge din diferitele circumstanțe juridice și/sau de fapt: o competență juridică explicită, atunci când legea desemnează un operator sau îi atribuie o sarcină sau o îndatorire legată de prelucrarea anumitor date; prevederi legale comune sau roluri tradiționale existente care implică în mod normal o anumită responsabilitate în cadrul organizațiilor (de exemplu, angajatorul în raport cu datele angajaților săi); circumstanțe de fapt și alte elemente (precum relațiile contractuale, controlul efectiv exercitat de o parte, vizibilitatea în raport cu persoanele vizate etc.).

  Dacă niciuna dintre aceste categorii nu este aplicabilă, desemnarea unui operator ar trebui să fie considerată „nulă și neavenită". Într-adevăr, un organism care nu are nici influență legală, nici influență de fapt în stabilirea modului de prelucrare a datelor cu caracter personal nu poate fi considerat ca având calitatea de operator.

Stabilirea „scopului” prelucrării determină calificarea drept operator (*de facto*). În schimb, stabilirea „mijloacelor” de prelucrare poate fi delegată de operator, în ceea ce privește chestiunile tehnice și organizatorice. Totuși, aspectele esențiale pentru legalitatea prelucrării – precum datele care trebuie prelucrate, durata stocării, accesul etc. – sunt stabilite de operator.

- Aspectul *personal* al definiției se referă la o serie largă de persoane care pot juca rolul de operator. Totuși, din punctul de vedere strategic al alocării responsabilităților, ar trebui, de preferință, să se considere că societatea sau organismul respectiv deține funcția de operator și nu o anumită persoană din cadrul societății sau organismului. Societatea sau organismul va răspunde în ultimă instanță pentru prelucrarea datelor și pentru respectarea obligațiilor care decurg din legislația privind protecția datelor, exceptând cazul în care există elemente clare care indică responsabilitatea unei persoane fizice, de exemplu atunci când o persoană fizică care lucrează în cadrul unei societăți sau al unui organism public utilizează datele în scopuri personale, în afara activităților societății.

- Posibilitatea unui *control pluralist* are în vedere numărul tot mai mare de situații în care diferitele părți implicate acționează ca operatori. Evaluarea acestui control comun ar trebui să reflecte evaluarea controlului „exclusiv”, adoptând o abordare concretă și funcțională și urmărind să determine dacă scopurile și elementele esențiale ale mijloacelor sunt stabilite de mai multe părți.

  Participarea părților la stabilirea scopurilor și a mijloacelor de prelucrare în contextul controlului comun poate lua diferite forme și nu trebuie să fie împărțită egal. În acest aviz există numeroase exemple diferite, în care controlul comun este exercitat în proporții diferite. Gradul diferit de exercitare a controlului poate determina diferite grade de responsabilitate și de răspundere, iar răspunderea solidară nu poate fi asumată în toate cazurile. Mai mult, este foarte posibil ca în sistemele complexe în care sunt implicate mai multe părți, accesul la datele personale și exercitarea drepturilor altor persoane vizate să poată fi asigurate la diferite niveluri, de către diverse părți.

Prezentul aviz analizează și conceptul de persoană împuternicită, a cărei existență depinde de decizia pe care o ia operatorul, care poate decide fie să prelucreze datele în cadrul organizației, fie să delege toate activitățile de prelucrare sau o parte dintre acestea unei organizații externe. În consecință, persoana împuternicită de operator trebuie să îndeplinească două condiții de bază: pe de o parte, aceasta trebuie să fie o entitate juridică distinctă în raport cu operatorul și, pe de altă parte, trebuie să prelucreze datele personale în numele operatorului. Această activitate de prelucrare se poate limita la o sarcină foarte specifică sau la un context foarte specific sau poate implica un anumit grad de libertate de decizie cu privire la modul în care interesele operatorului pot fi cât mai bine servite, persoana împuternicită putând alege mijloacele tehnice și organizaționale cele mai adecvate.

În plus, rolul persoanei împuternicite nu este determinat de calitatea persoanei care prelucrează datele personale, ci de activitățile concrete ale acesteia într-un context anume și cu privire la anumite serii de date sau de operațiuni. Câteva criterii pot fi utile pentru a stabili dacă diferitele persoane implicate în prelucrare se califică sau nu: nivelul instrucțiunilor prealabile furnizate de operatorul de date; monitorizarea calității

serviciilor de către operatorul de date; vizibilitatea în raport cu persoanele vizate; expertiza părților; puterea autonomă de luare a deciziilor pe care o au diversele părți.

Ultima categorie, „terțul", este definită ca orice persoană care nu are o autoritate sau o autorizare specifică - care ar putea decurge, de exemplu, din calitatea acestuia de operator, persoană împuternicită sau angajat al acestora – cu privire la prelucrarea datelor cu caracter personal.

* * *

Grupul de lucru recunoaște dificultățile întâmpinate în aplicarea definițiilor directivei într-un mediu complex, în care pot fi imaginate numeroase scenarii care implică operatori și persoane împuternicite de aceștia, singuri sau împreună, cu diferite grade de autonomie și răspundere.

În analiza sa, acesta a pus accentul pe necesitatea alocării responsabilității astfel încât conformitatea cu normele de protecție a datelor să fie suficient asigurată în practică. Totuși, nu a fost găsit niciun motiv pentru a se considera că distincția actuală dintre operatori și persoanele împuternicite de aceștia nu ar mai fi relevantă și aplicabilă în acest sens.

În consecință, grupul de lucru speră că explicațiile din prezentul aviz, ilustrate prin exemple specifice din experiența zilnică a autorităților de protecție a datelor, vor contribui la o orientare efectivă cu privire la modul de interpretare a acestor definiții de bază cuprinse în prezenta directivă.

Adoptat la Bruxelles, la 16 februarie 2010

Pentru Grupul de lucru,
Președintele
Jacob KOHNSTAMM