GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECŢIA DATELOR

844/14/RO
WP 217

Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date prevăzută la articolului 7 din Directiva 95/46/CE

Adoptat la 9 aprilie 2014

Cuprins

Rezumat

Prezentul aviz analizează criteriile stabilite la articolul 7 din Directiva 95/46/CE privind legitimitatea prelucrării datelor. Concentrându-se asupra interesului legitim al operatorului, avizul oferă orientări cu privire la modul de aplicare a articolului 7 litera (f) în cadrul juridic actual și formulează recomandări pentru îmbunătățiri ulterioare.

Articolul 7 litera (f) reprezintă ultimul dintre cele șase temeiuri pentru prelucrarea legală a datelor cu caracter personal. În fapt, acesta solicită punerea în balanță a interesului legitim al operatorului sau al oricăror terți cărora le sunt comunicate datele cu interesul sau drepturile fundamentale ale persoanei vizate. Rezultatul unui astfel de test comparativ va stabili dacă articolul 7 litera (f) poate fi invocat ca temei juridic pentru prelucrare.

WP29 recunoaște importanța și utilitatea criteriului de la articolul 7 litera (f), care, în condițiile potrivite și sub rezerva unor garanții adecvate, poate contribui la prevenirea dependenței exagerate de alte temeiuri juridice. Articolul 7 litera (f) nu ar trebui să fie considerat o soluție de „ultimă instanță" pentru situațiile rare sau neprevăzute în care se consideră că nu se aplică alte temeiuri pentru prelucrarea legitimă. Cu toate acestea, articolul în cauză nu ar trebui să fie ales în mod automat, iar utilizarea sa nu ar trebui să fie prelungită în mod nejustificat pe baza percepției că acesta este mai puțin constrângător decât celelalte temeiuri.

O bună evaluare în temeiul articolului 7 litera (f) nu este un test comparativ facil constând în simpla cântărire a două opțiuni ușor cuantificabile și comparabile una cu cealaltă. Mai degrabă, un astfel de test necesită luarea în considerare pe deplin a unei serii de factori, astfel încât să se asigure că interesele și drepturile fundamentale ale persoanelor vizate sunt avute în vedere în mod corespunzător. În același timp, evaluarea este scalabilă, putând varia de la simplă la complexă și nu trebuie să fie nejustificat de împovărătoare. Printre factorii care trebuie luați în considerare atunci când se efectuează testul comparativ se numără:

- natura și sursa interesului legitim și faptul dacă prelucrarea datelor este necesară pentru exercitarea unui drept fundamental, este în alt mod în interesul public sau beneficiază de recunoaștere în comunitatea în cauză;

- impactul asupra persoanei vizate și așteptările rezonabile ale acesteia cu privire la ce se va întâmpla cu datele sale, precum și natura datelor și modul în care acestea sunt prelucrate;

- garanțiile suplimentare care ar putea limita impactul nejustificat asupra persoanei vizate, cum ar fi minimizarea datelor, tehnologiile menite să sporească protecția vieții private; creșterea transparenței, dreptul general și necondiționat de excludere voluntară și portabilitatea datelor.

Pentru viitor, WP29 recomandă punerea în aplicare a unui considerent din propunerea de regulament cu privire la factorii-cheie care trebuie luați în considerare atunci când se aplică testul comparativ. WP29 recomandă, de asemenea, adăugarea unui considerent prin care să se solicite operatorului, atunci când este cazul, să își documenteze evaluarea pentru a asigura o mai mare responsabilizare. În cele din urmă, WP29 va sprijini, de asemenea, o dispoziție de fond conform căreia operatorii trebuie să explice persoanelor vizate motivele pentru care consideră că interesul lor prevalează asupra interesului, drepturilor și libertăților fundamentale ale persoanei vizate.

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

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

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL AVIZ:

I. Introducere

Prezentul aviz analizează criteriile enunțate la articolul 7 din Directiva 95/46/CE[1] (denumită în continuare „directiva") privind legitimitatea prelucrării datelor. Acesta se concentrează, în special, asupra interesului legitim al operatorului, în conformitate cu articolul 7 litera (f).

Criteriile enumerate la articolul 7 sunt legate de principiul mai larg al „legalității", prevăzut la articolul 6 alineatul (1) litera (a), care stipulează că datele cu caracter personal trebuie să fie prelucrate „în mod corect și legal".

Articolul 7 prevede că datele cu caracter personal pot fi prelucrate numai în cazul în care se aplică cel puțin unul dintre cele șase temeiuri juridice enumerate la articolul respectiv. În special, datele cu caracter personal se prelucrează numai (a) pe baza consimțământului neechivoc al persoanei vizate[2]; sau în cazul în care – pe scurt[3] – prelucrarea este necesară pentru:

(b) executarea unui contract cu persoana vizată;
(c) îndeplinirea unei obligații legale impuse operatorului;
(d) protecția interesului vital al persoanei vizate;
(e) îndeplinirea unei sarcini efectuate în interes public; sau
(f) interesul legitim urmărit de operator, care face obiectul unui test comparativ suplimentar în raport cu interesul și drepturile persoanei vizate.

Acest ultim temei permite prelucrarea „necesară pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți cărora le sunt comunicate datele, cu condiția ca acest interes să nu prejudicieze interesul sau[4] drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecție în temeiul articolului 1 alineatul (1)". Cu alte cuvinte, articolul 7 litera (f) permite prelucrarea sub rezerva efectuării unui test comparativ, care pune

[1] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24.10.1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).
[2] A se vedea Avizul 15/2011 al grupului de lucru „articolul 29" pentru protecția datelor privind definiția consimțământului, adoptat la 13.7.2011 (WP187).
[3] Dispozițiile sunt discutate în detaliu într-o etapă ulterioară.
[4] Astfel cum se explică în secțiunea III. 3.2, versiunea în limba engleză a directivei pare să conțină o greșeală de tipar: textul ar trebui să aibă următorul conținut „interesul sau drepturile fundamentale" și nu „interesul pentru drepturile fundamentale".

în balanță interesul legitim al operatorului sau al terțului ori terților cărora le sunt comunicate datele – și interesul sau drepturile fundamentale ale persoanei vizate[5].

Necesitatea unei abordări mai coerente și mai armonizate în întreaga Europă

Studiile realizate de Comisie în contextul revizuirii directivei[6], precum și cooperarea și schimbul de opinii între autoritățile naționale pentru protecția datelor (denumite în continuare „APD") au indicat lipsa unei interpretări armonizate a articolului 7 litera (f) din directivă, care a condus la aplicări divergente în statele membre. În special, deși este necesară efectuarea unui test comparativ efectiv, în mai multe state membre articolul 7 litera (f) este perceput uneori în mod incorect ca o „ușă deschisă" pentru legitimarea oricărui tip de prelucrare a datelor care nu se încadrează în unul dintre celelalte temeiuri juridice.

Inexistența unei abordări coerente poate conduce la lipsă de securitate juridică și de previzibilitate, ar putea slăbi poziția persoanelor vizate și poate, de asemenea, să impună sarcini administrative inutile asupra întreprinderilor și asupra altor organizații care își desfășoară activitatea la nivel transfrontalier. Astfel de neconcordanțe au condus deja la litigii în fața Curții de Justiție a Uniunii Europene (denumită în continuare „CEJ")[7].

Prin urmare și întrucât activitatea de elaborare a unui nou regulament general privind protecția datelor continuă, este deosebit de oportun ca al șaselea temei pentru prelucrare (care se referă la „interesul legitim") și relația acestuia cu celelalte temeiuri pentru prelucrare să fie mai bine înțelese. În special, având în vedere faptul că drepturile fundamentale ale persoanelor vizate sunt în joc, aplicarea tuturor celor șase temeiuri ar trebui să țină cont – în mod corespunzător și echitabil – de respectarea drepturilor respective. Articolul 7 litera (f) nu ar trebui să devină o soluție facilă pentru a eluda respectarea legislației privind protecția datelor.

Din acest motiv, grupul de lucru „articolul 29" pentru protecția datelor („grupul de lucru"), ca parte a programului său de lucru pentru 2012-2013, a decis să analizeze cu atenție acest subiect și – pentru a-și executa programul de lucru[8] – s-a angajat să elaboreze prezentul aviz.

[5] Trimiterea la articolul 1 alineatul (1) nu ar trebui să fie interpretată ca limitând sfera intereselor și a drepturilor și libertăților fundamentale ale persoanei vizate. Mai degrabă, rolul trimiterii este de a sublinia obiectivul general al legislației privind protecția datelor și al directivei ca atare. Într-adevăr, articolul 1 alineatul (1) nu se referă numai la protecția vieții private, ci și la protecția tuturor celorlalte „drepturi și libertăți ale persoanelor fizice", viața privată fiind doar unul dintre acestea.

[6] La 25 ianuarie 2012, Comisia Europeană a adoptat un pachet de măsuri pentru reformarea cadrului european pentru protecția datelor. Pachetul include (i) o comunicare (COM(2012)9 final), (ii) o propunere de regulament general privind protecția datelor (denumită în continuare „propunerea de regulament") (COM(2012)11 final) și (iii) o propunere de directivă privind protecția datelor în domeniul aplicării legii penale (COM(2012)10 final). Evaluarea impactului care o însoțește și care conține 10 anexe este inclusă într-un document de lucru al Comisiei [SEC(2012)72 final]. A se vedea, în special, studiul intitulat „Evaluarea punerii în aplicare a Directivei privind protecția datelor", care constituie anexa 2 la evaluarea impactului care însoțește pachetul de reformare a protecției datelor al Comisiei Europene.

[7] A se vedea pagina 7, în capitolul „II.1 Scurt istoric", *„Punerea în aplicare a directivei; hotărârea în cauzele ASNEF și FECEMD".*

[8] A se vedea programul de lucru pentru perioada 2012-2013 al grupului de lucru „articolul 29" pentru protecția datelor, adoptat la 1 februarie 2012 (WP190).

Punerea în aplicare a cadrului juridic actual și pregătirea pentru viitor

Programul de lucru specifică în mod clar două obiective: „asigurarea aplicării corecte a cadrului juridic actual", precum și „pregătirea pentru viitor".

Prin urmare, primul obiectiv al prezentului aviz este asigurarea unei înțelegeri comune a cadrului juridic existent. Acest obiectiv vine în continuarea avizelor anterioare privind alte dispoziții esențiale ale directivei[9]. În al doilea rând, pe baza analizei, avizul va formula, de asemenea, recomandări de politică pentru a fi luate în considerare la revizuirea cadrului juridic privind protecția datelor.

Structura avizului

După o scurtă trecere în revistă a istoricului și rolului intereselor legitime și a altor temeiuri pentru prelucrare în capitolul II, capitolul III examinează și interpretează dispozițiile relevante ale directivei, luând în considerare o bază comună pentru punerea în aplicare la nivel național. Analiza este ilustrată cu exemple practice pe baza experienței naționale acumulate. Analiza stă la baza recomandărilor formulate în capitolul IV atât în ceea ce privește aplicarea cadrului de reglementare actual, cât și în contextul revizuirii directivei.

II. Observații generale și aspecte de politică

II.1. Scurt istoric

Această prezentare se concentrează asupra modului în care au fost dezvoltate conceptele de legalitate și temei juridic pentru prelucrare, inclusiv interesul legitim. Aceasta explică, în special, faptul că necesitatea unui temei juridic a fost utilizată pentru prima dată ca o cerință în contextul derogărilor de la drepturile privind viață privată și, ulterior, a devenit o cerință separată în contextul protecției datelor.

Convenția Europeană a Drepturilor Omului („CEDO")

Articolul 8 din Convenția europeană a drepturilor omului (CEDO), adoptată în 1950, consacră dreptul la viață privată, și anume respectarea vieții private și de familie, a domiciliului și a corespondenței. Acesta interzice orice încălcare a dreptului la viață privată, cu excepția cazului în care acest lucru este „prevăzut de lege" și „necesar într-o societate democratică" pentru a satisface anumite tipuri de interese publice imperioase, enumerate în mod explicit.

Articolul 8 din Convenția europeană a drepturilor omului se concentrează asupra protecției vieții private și prevede necesitatea unei justificări pentru orice încălcare a dreptului la viață privată. Această abordare se bazează pe o interdicție generală a încălcării dreptului la viață privată și permite excepții numai în condiții strict definite. În cazurile în care există „încălcări ale dreptului la viață privată" este necesar un temei juridic, precum și specificarea unui scop legitim ca o precondiție pentru a evalua necesitatea încălcării. Această abordare explică faptul

[9] Cum ar fi Avizul nr. 3/2013 privind limitarea scopului, adoptat la 3.4.2013 (WP203), Avizul nr. 15/2011 privind definiția consimțământului (citat la nota de subsol 2), Avizul nr. 8/2010 privind legislația aplicabilă, adoptat la 16.12.2010 (WP179) și Avizul nr. 1/2010 privind conceptele de „operator" și „persoana împuternicită de către operator", adoptat la 16.2.2010 (WP169).

că CEDO nu prevede o listă a posibilelor temeiuri juridice, ci se axează pe necesitatea unui temei juridic, precum și pe condițiile pe care un astfel de temei juridic ar trebui să le îndeplinească.

Convenția nr. 108

Convenția 108 a Consiliului Europei[10], deschisă spre semnare în 1981, introduce protecția datelor cu caracter personal ca noțiune de sine stătătoare. Ideea de bază la momentul respectiv nu era aceea că prelucrarea datelor cu caracter personal ar trebui să fie întotdeauna considerată ca reprezentând „o *încălcare* a dreptului la viața privată", ci mai degrabă că, pentru a *proteja* drepturile și libertățile fundamentale ale tuturor persoanelor, în special dreptul acestora la viață privată, prelucrarea datelor cu caracter personal trebuie să îndeplinească anumite condiții. Astfel, articolul 5 stabilește principiile fundamentale ale legislației privind protecția datelor, inclusiv cerința conform căreia „datele cu caracter personal care fac obiectul unei prelucrări automatizate, sunt: (a) obținute și prelucrate în mod corect și legal". Cu toate acestea, convenția nu a furnizat temeiuri detaliate pentru prelucrare[11].

Orientările OCDE[12]

Orientările OCDE, pregătite în paralel cu Convenția 108 și adoptate în 1980, împărtășesc idei similare privind „legalitatea", deși conceptul este exprimat într-un mod diferit. Orientările au fost actualizate în 2013, fără modificări de fond privind principiul legalității. În special, articolul 7 din Orientările OCDE prevede că „ar trebui să existe limite la colectarea datelor cu caracter personal și orice astfel de date ar trebui să fie obținute pe cale legală și onestă și, după caz, cu cunoștința sau consimțământul persoanei vizate". Aici temeiul juridic al consimțământului este menționat în mod explicit ca opțiune, de utilizat „după caz". Aceasta va necesita o apreciere a intereselor și drepturilor în cauză, precum și evaluarea măsurii în care prelucrarea este invazivă. În acest sens, abordarea OCDE prezintă unele similitudini cu criteriile – mult mai dezvoltate – prevăzute în Directiva 95/46/CE.

Directiva 95/46/CE

La momentul adoptării sale în 1995, directiva a fost construită pe baza primelor instrumente de protecție a datelor, inclusiv Convenția 108 și Orientările OCDE. De asemenea, au fost luate în considerare primele experiențe în materie de protecția datelor într-o serie de state membre.

Pe lângă o cerință mai amplă prevăzută la articolul 6 alineatul (1) litera (a) conform căreia datele cu caracter personal trebuie să fie prelucrate „în mod corect și legal", directiva a adăugat un set specific de cerințe suplimentare, care până atunci nu existaseră ca atare în

[10] Convenția nr. 108 pentru protecția persoanelor în ceea ce privește prelucrarea automată a datelor cu caracter personal.

[11] Proiectul de text al convenției actualizate adoptate de plenara T-PD din noiembrie 2012 prevede că prelucrarea datelor poate fi efectuată pe baza consimțământului persoanei vizate sau în temeiul „unui motiv legitim prevăzut de lege", în mod similar Cartei drepturilor fundamentale a Uniunii Europene, menționată mai jos, la pagina 8.

[12] Orientările OCDE privind protecția vieții private și a fluxurilor transfrontaliere de date cu caracter personal, din 11 iulie 2013.

Convenția 108, nici în Orientările OCDE: prelucrarea datelor cu caracter personal trebuie să se bazeze pe unul dintre cele șase temeiuri juridice menționate la articolul 7.

Punerea în aplicare a directivei; hotărârea în cauzele ASNEF și FECEMD[13]

Raportul Comisiei intitulat „Evaluarea punerii în aplicare a Directivei privind protecția datelor”[14] subliniază faptul că punerea în aplicare a dispozițiilor directivei în legislația națională a fost uneori nesatisfăcătoare. În analiza tehnică a transpunerii directivei în statele membre[15], Comisia oferă detalii suplimentare cu privire la punerea în aplicare a articolului 7. Analiza arată că, în timp ce în majoritatea statelor membre legislația a stabilit șase temeiuri juridice în termeni relativ similari celor utilizați în directivă, flexibilitatea acestor principii, în fapt, a condus la aplicări divergente.

În acest context, este deosebit de relevant că, în hotărârea sa din 24 noiembrie 2011 în cauzele *ASNEF și FECEMD*, CEJ a constatat că Spania nu a transpus corect articolul 7 litera (f) din directivă atunci când a prevăzut că – în lipsa consimțământului persoanei vizate – orice date relevante utilizate ar trebui să apară în surse publice. De asemenea, hotărârea a stabilit că articolul 7 litera (f) are efect direct. Hotărârea limitează marja de apreciere pe care statele membre o au în punerea în aplicare a articolului 7 litera (f). În special, acestea nu trebuie să depășească granița delicată între clarificare, pe de o parte, și stabilirea de cerințe suplimentare, care ar modifica domeniul de aplicare a articolului 7 litera (f), pe de altă parte.

Hotărârea CEJ, care precizează faptul că nu se permite statelor membre să impună restricții și cerințe unilaterale suplimentare privind temeiurile juridice pentru prelucrarea legală a datelor în legislația lor națională, are consecințe importante. Instanțele naționale și alte organisme relevante trebuie să interpreteze dispozițiile naționale având în vedere hotărârea respectivă și, dacă este necesar, să elimine normele și practicile naționale contradictorii.

Având în vedere hotărârea CEJ, este cu atât mai important ca autoritățile naționale pentru protecția datelor (APD) și/sau organele legislative europene să ajungă la o înțelegere clară și comună privind aplicabilitatea articolului 7 litera (f). Acest lucru ar trebui realizat într-un mod echilibrat, fără a restricționa în mod nejustificat sau a extinde în mod nejustificat domeniul de aplicare a dispoziției în cauză.

Carta drepturilor fundamentale a Uniunii Europene

Întrucât Tratatul de la Lisabona a intrat în vigoare la 1 decembrie 2009, Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”), are „aceeași valoare juridică cu cea a tratatelor”[16]. Carta consacră protecția datelor cu caracter personal ca drept fundamental în temeiul articolului 8, care este distinct de respectarea vieții private și de familie în temeiul articolului 7. Articolul 8 conține cerința existenței unei baze legitime pentru prelucrare. În special, acesta prevede că datele cu caracter personal trebuie să fie prelucrate „pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut

[13] Hotărârea Curții de Justiție din 24.11.2011 în cauzele C-468/10 și C-469/10 (*ASNEF și FECEMD*).
[14] A se vedea anexa 2 din evaluarea impactului pentru pachetul de reformă al Comisiei privind protecția datelor, citată la nota de subsol 6 de mai sus.
[15] Analiza și studiul de impact privind punerea în aplicare a Directivei 95/46/CE în statele membre. A se vedea http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.
[16] A se vedea articolul 6 alineatul (1) din TUE.

de lege”[17]. Aceste dispoziții consolidează atât importanța principiului legalității, cât și necesitatea unui temei juridic adecvat pentru prelucrarea datelor cu caracter personal.

Propunerea de regulament privind protecția datelor

În contextul procesului de revizuire a normelor în materie de protecție a datelor, domeniul de aplicare a temeiurilor de legalitate în conformitate cu articolul 7, în special domeniul de aplicare a articolului 7 litera (f), face în prezent obiectul discuțiilor.

Articolul 6 din propunerea de regulament enumeră temeiurile pentru prelucrarea legală a datelor cu caracter personal. Cu câteva excepții (astfel cum se va arăta în continuare), cele șase temeiuri disponibile în prezent rămân în mare măsură neschimbate față de cele prevăzute la articolul 7 din directivă. Cu toate acestea, Comisia a propus să ofere orientări suplimentare sub formă de acte delegate.

Este interesant de observat că, în contextul activității comisiei relevante a Parlamentului European[18], s-a urmărit să se clarifice conceptul de interes legitim în propunerea de regulament ca atare. S-a elaborat o listă de cazuri în care interesul legitim al operatorului, ca regulă generală, ar prevala asupra interesului legitim și asupra drepturilor și libertăților fundamentale ale persoanei vizate, precum și o a doua listă de cazuri pentru situația inversă. Listele – prevăzute fie în cadrul dispozițiilor regulamentului, fie în considerente – oferă o contribuție relevantă pentru evaluarea echilibrului dintre interesul și drepturile operatorului și cele ale persoanei vizate și sunt luate în considerare în prezentul aviz[19].

II.2. Rolul conceptului

Interesul legitim al operatorului: testul comparativ ca ultimă soluție?

Articolul 7 litera (f) este prevăzut ca ultimă opțiune între cele șase temeiuri care permit prelucrarea legală a datelor cu caracter personal. Acesta solicită un test comparativ: ceea ce este necesar în interesul legitim al operatorului (sau al unor terți) trebuie să fie pus în balanță cu interesul sau drepturile și libertățile fundamentale ale persoanei vizate. Rezultatul testului comparativ determină dacă articolul 7 litera (f) poate fi invocat ca temei juridic pentru prelucrare.

Caracterul deschis al acestei dispoziții ridică numeroase întrebări importante cu privire la domeniul de aplicare exact și aplicarea acesteia, care vor fi analizate, pe rând, în prezentul aviz. Cu toate acestea, astfel cum se va explica mai jos, aceasta nu înseamnă în mod necesar că dispoziția în cauză ar trebui să fie privită ca o opțiune care poate fi utilizată în mod excepțional pentru a umple lacunele pentru situații neprevăzute și ca soluție de „ultimă

[17] A se vedea articolul 8 alineatul (2) din Cartă.

[18] Proiect de raport al Comisiei pentru libertăți civile, justiție și afaceri interne (LIBE) referitor la propunerea de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)”, [COM(2012) 0011 — C7-0025/2012-2012/0011 (COD)], din 16.1.2013 („Proiect de raport al Comisiei LIBE”). A se vedea, în special, amendamentele 101 și 102. De asemenea, a se vedea amendamentele adoptate de comisie la 21.10.2013 în raportul său final („Raportul final al Comisiei LIBE”).

[19] A se vedea secțiunea III.3.1, în special punctele de la paginile 24-25, care cuprind o listă neexhaustivă cu unele dintre cele mai comune situații în care poate surveni chestiunea interesului legitim în conformitate cu articolul 7 litera (f).

instanță” sau ca o ultimă șansă în cazul în care nu se aplică alte temeiuri. În același timp, aceasta nu ar trebui să fie considerată o opțiune preferată, iar utilizarea sa să fie prelungită în mod nejustificat deoarece ar fi considerată mai puțin constrângătoare decât celelalte temeiuri.

Dimpotrivă, există posibilitatea ca articolul 7 litera (f) să aibă propriul domeniu natural de relevanță și să poată juca un rol foarte util ca temei pentru prelucrarea legală, sub rezerva îndeplinirii unei serii de condiții esențiale.

Utilizarea corespunzătoare a articolului 7 litera (f), în condițiile potrivite și sub rezerva unor garanții adecvate, poate contribui, de asemenea, la prevenirea utilizării abuzive și a bazării excesive pe alte temeiuri juridice.

Primele cinci temeiuri de la articolul 7 se bazează pe consimțământ, înțelegerea contractuală, obligația legală a persoanei vizate sau alte justificări identificate în mod specific ca temei pentru legitimitate. În cazul în care prelucrarea se bazează pe unul dintre aceste cinci temeiuri, aceasta se consideră ca fiind legitimă *a priori*, prin urmare, aceasta face obiectul numai al respectării altor dispoziții aplicabile prin lege. Cu alte cuvinte, există o prezumție că echilibrul dintre diferitele drepturi și interese în discuție – inclusiv cele ale operatorului și ale persoanei vizate – este realizat – presupunând, desigur, că sunt respectate toate celelalte dispoziții ale legislației în materie de protecție a datelor. Spre deosebire de acestea, articolul 7 litera (f) impune un test *specific*, pentru cazurile care nu se încadrează în scenariile predefinite în cadrul temeiurilor (a)-(e). Acesta asigură faptul că, în afara scenariilor respective, orice prelucrare trebuie să îndeplinească cerința unui test comparativ, ținând seama în mod corespunzător de interesul și drepturile fundamentale ale persoanei vizate.

Testul comparativ poate conduce la concluzia, în anumite cazuri, că echilibrul înclină în favoarea intereselor și drepturilor fundamentale ale persoanelor vizate și că, prin urmare, activitatea de prelucrare nu poate avea loc. Pe de altă parte, o evaluare corespunzătoare a echilibrului în temeiul articolului 7 litera (f), adesea cu posibilitatea de excludere voluntară de la prelucrare, poate, în alte cazuri, să constituie o alternativă viabilă la utilizarea necorespunzătoare, de exemplu, a temeiului privind „consimțământul” sau „necesitatea pentru executarea unui contract”. Astfel privit, articolul 7 litera (f) prezintă garanții complementare – care necesită măsuri corespunzătoare – în comparație cu celelalte criterii prestabilite. Prin urmare, acesta nu ar trebui considerat drept „cea mai slabă verigă” sau o ușă deschisă pentru a legitima toate activitățile de prelucrare a datelor care nu intră sub incidența niciunuia dintre celelalte temeiuri juridice.

Grupul de lucru reiterează faptul că, în interpretarea domeniului de aplicare a articolului 7 litera (f), acesta urmărește să adopte o abordare echilibrată, care să asigure flexibilitatea necesară operatorilor de date pentru situațiile în care nu există niciun impact asupra persoanelor vizate, oferind, în același timp, persoanelor vizate un grad suficient de certitudine juridică și garanții că această dispoziție cu caracter deschis nu va fi utilizată în mod abuziv.

II.3. Concepte conexe

Relația temeiului de la articolul 7 litera (f) cu alte temeiuri pentru legalitate

Articolul 7 începe cu temeiul privind consimțământul și prezintă în continuare o listă cu celelalte temeiuri pentru legalitate, inclusiv contractele și obligațiile legale, realizând o tranziție treptată până la testul interesului legitim, care figurează ca ultimul dintre cele șase temeiuri disponibile. Ordinea în care sunt enumerate temeiurile juridice în conformitate cu articolul 7 a fost uneori interpretată ca o indicație a importanței fiecăruia dintre ele. Cu toate acestea, astfel cum s-a evidențiat deja în avizul grupului de lucru privind noțiunea de consimțământ[20], textul directivei nu face o distincție juridică între cele șase temeiuri și nu sugerează că există o ierarhie între acestea. Nu există niciun indiciu că articolul 7 litera (f) ar trebui să se aplice doar în cazuri excepționale și, de asemenea, textul nu sugerează că ordinea specifică a celor șase temeiuri juridice ar avea vreun efect relevant din punct de vedere juridic. În același timp, sensul exact al articolului 7 litera (f) și relația sa cu alte temeiuri pentru legalitate au fost mult timp destul de neclare.

În acest context și având în vedere diversitatea istorică și culturală și formularea cu caracter deschis a directivei, s-au dezvoltat abordări diferite: unele state membre au avut tendința de a vedea articolul 7 litera (f) drept temeiul cel mai puțin preferat, care este destinat să umple lacunele doar în unele cazuri excepționale, când niciunul dintre celelalte cinci temeiuri nu ar putea să se aplice sau nu s-ar aplica[21]. Dimpotrivă, alte state membre consideră acest temei drept una dintre cele șase posibilități, reprezentând o opțiune care nu este mai mult sau mai puțin importantă decât celelalte opțiuni și care se poate aplica unui număr mare și într-o mare varietate de situații, sub rezerva îndeplinirii condițiilor necesare.

Având în vedere această diversitate și, de asemenea, luând în considerare hotărârea în cauzele ASNEF și FECEMD, este important să se clarifice relația dintre temeiul „interesului legitim” și celelalte temeiuri de legalitate – de exemplu, privind consimțământul, contractele, sarcinile de interes public – și, de asemenea, în ceea ce privește dreptul de opoziție al persoanei vizate. Acest lucru poate contribui la o mai bună definire a rolului și a funcției temeiului interesului legitim și, prin urmare, poate spori securitatea juridică.

De asemenea, ar trebui remarcat că temeiul interesului legitim, la fel precum celelalte temeiuri în afară de consimțământ, impune o examinare a „necesității”. Acest lucru limitează contextul în care poate fi aplicat fiecare dintre temeiuri. Curtea Europeană de Justiție a considerat că

[20] A se vedea nota de subsol 2 de mai sus.

[21] De asemenea, trebuie remarcat faptul că proiectul de raport al Comisiei LIBE a propus în amendamentul 100 separarea articolului 7 litera (f) de restul temeiurilor juridice și a propus, de asemenea, cerințe suplimentare pentru cazul în care este utilizat temeiul juridic respectiv, inclusiv o mai mare transparență și o responsabilitate mai pronunțată, astfel cum se va explica în continuare.

„necesitatea” este un concept care are propriul său înțeles independent în legislația Uniunii[22]. Curtea Europeană a Drepturilor Omului a oferit, de asemenea, orientări utile în acest sens[23].

De asemenea, existența unui temei juridic corespunzător nu scutește operatorul de date de obligațiile care îi revin în temeiul articolului 6 în ceea ce privește echitatea, legalitatea, necesitatea și proporționalitatea, precum și calitatea datelor. De exemplu, inclusiv în cazul în care prelucrarea datelor cu caracter personal se bazează pe temeiul interesului legitim sau pe executarea unui contract, aceasta nu ar permite o colectare a datelor care este excesivă în raport cu scopul specificat.

Interesul legitim și alte temeiuri menționate la articolul 7 sunt temeiuri alternative și, prin urmare, este suficient dacă se aplică numai unul dintre acestea. Cu toate acestea, temeiurile sunt cumulative nu numai cu cerințele de la articolul 6, ci și cu toate celelalte principii și cerințe de protecție a datelor care pot fi aplicabile.

Alte teste comparative

Articolul 7 litera (f) nu prevede singurul test comparativ stipulat în directivă. De exemplu, articolul 9 solicită asigurarea unui echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare. Articolul permite statelor membre să prevadă exonerările și derogările necesare pentru prelucrarea datelor cu caracter personal „efectuată numai în scopuri jurnalistice, artistice sau literare” dacă acestea sunt „necesare pentru a pune dreptul la viață privată în acord cu normele care reglementează libertatea de exprimare”.

De asemenea, numeroase alte dispoziții ale directivei necesită, la rândul lor, o analiză de la caz la caz pentru a se asigura un echilibru între drepturile și interesele în discuție, precum și flexibilitatea evaluării în raport cu mai mulți factori. Printre acestea se numără dispoziții privind necesitatea, proporționalitatea și limitarea scopului, excepții de la articolul 13 și cercetarea științifică, pentru a indica doar câteva.

Într-adevăr, se pare că directiva a fost concepută astfel încât să lase loc pentru interpretarea și compararea intereselor. Aceasta a vizat, bineînțeles, cel puțin în parte, lăsarea unui spațiu mai mare de manevră pentru statele membre în vederea punerii în aplicare în dreptul intern. În plus, necesitatea păstrării unei anumite flexibilități provine, de asemenea, din natura însăși a dreptului la protecția datelor cu caracter personal și a dreptului la viață privată. Într-adevăr, cele două drepturi, împreună cu majoritatea celorlalte drepturi fundamentale (dar nu toate), sunt considerate drepturi ale omului relative sau calificate[24]. Astfel de drepturi trebuie

[22] Hotărârea Curții Europene de Justiție din 16 decembrie 2008 în cauza C-524/06 (Heinz Huber/Bundesrepublik Deutschland), punctul 52: „Prin urmare, având în vedere obiectivul de a asigura un nivel de protecție echivalent în toate statele membre, noțiunea de necesitate prevăzută la articolul 7 litera (e) din Directiva 95/46/CE, al cărui scop este acela de a delimita exact una dintre situațiile în care prelucrarea datelor cu caracter personal este legală, nu poate avea un sens care variază între statele membre. De aici rezultă că ceea ce este în discuție este un concept care are înțelesul său propriu, independent, în legislația comunitară și care trebuie să fie interpretat într-un mod care să reflecte pe deplin obiectivul acestei directive, astfel cum se prevede la articolul 1 alineatul (1)”.

[23] Hotărârea Curții Europene a Drepturilor Omului în cauza Silver & Others/Regatul Unit din 25 martie 1983, punctul 97, care analizează sintagma „necesar într-o societate democratică”: „adjectivul «necesar» nu este sinonim cu «indispensabil», nici nu are flexibilitatea unor expresii precum «admisibil», «obișnuit», «util», «rezonabil» sau «de dorit». [...]”

[24] Există doar câteva drepturi ale omului care nu pot fi puse în balanță cu drepturile altora sau cu interesul comunității mai largi. Acestea sunt cunoscute ca drepturi absolute. Astfel de drepturi nu pot fi niciodată limitate

întotdeauna să fie interpretate în context. Sub rezerva unor garanții adecvate, acestea pot fi puse în balanță cu drepturile altora. În anumite situații – și, de asemenea, sub rezerva unor garanții adecvate – acestea pot, de asemenea, să fie restricționate din motive de interes public.

II.4. Contextul și consecințele strategice

Asigurarea legitimității, dar și a flexibilității: mijloace de specificare a articolului 7 litera (f)

Textul actual al articolului 7 litera (f) din directivă are un caracter deschis. Aceasta înseamnă că dispoziția în cauză poate fi invocată într-o gamă largă de situații, atât timp cât sunt îndeplinite cerințele sale, inclusiv testul comparativ. Cu toate acestea, o astfel de flexibilitate poate avea, de asemenea, implicații negative. Pentru a o împiedica să conducă la aplicarea inconsecventă la nivel național sau la o lipsă de certitudine juridică, orientările suplimentare ar juca un rol important.

Comisia prevede astfel de orientări în propunerea de regulament, sub formă de acte delegate. Alte opțiuni includ furnizarea de clarificări și dispoziții detaliate în chiar textul propunerii de regulament[25] și/sau încredințarea misiunii de a furniza orientări suplimentare în domeniu Comitetului european pentru protecția datelor.

Fiecare dintre aceste opțiuni are, la rândul său, avantaje și dezavantaje. Dacă evaluarea s-ar efectua de la caz la caz în lipsa unor orientări suplimentare, s-ar risca aplicarea inconsecventă și lipsa de previzibilitate, astfel cum a fost cazul în trecut.

Dimpotrivă, furnizarea, în textul propunerii de regulament ca atare, de liste detaliate și exhaustive care să reflecte situațiile în care interesul legitim ale operatorului, ca regulă generală, prevalează asupra interesului și drepturilor fundamentale ale persoanei vizate sau invers ar risca să inducă în eroare sau să fie inutil de prescriptivă sau ambele.

Cu toate acestea, astfel de abordări ar putea inspira o soluție echilibrată, prin furnizarea de mai multe detalii în propunerea de regulament, precum și de orientări suplimentare în acte delegate sau în orientările Comitetului european pentru protecția datelor[26].

Analiza din capitolul III urmărește să pună bazele pentru identificarea unei astfel de abordări, care să nu fie nici prea generală pentru a fi lipsită de sens, nici prea specifică pentru a fi prea rigidă.

---

sau restricționate, indiferent de împrejurări – chiar în stare de război sau într-o situație de urgență. Un exemplu este dreptul de a nu fi torturat sau tratat într-un mod inuman sau degradant. Niciodată nu este permis ca o persoană să fie torturată sau să fie tratată într-un mod inuman sau degradant, indiferent de împrejurări. Exemple de drepturi ale omului non-absolute includ dreptul la respectarea vieții private și de familie, dreptul la libertatea de exprimare și dreptul la libertatea de gândire, de conștiință și de religie.

[25] A se vedea secțiunea II.1 Scurt istoric, la *„Propunerea de regulament privind protecția datelor”,* paginile 8-9.

[26] În ceea ce privește actele delegate și orientările Comitetului european pentru protecția datelor, Avizul nr. 08/2012 al grupului de lucru, care oferă informații suplimentare cu privire la discuțiile privind reforma protecției datelor, adoptat la 5.10.2012 (WP199) a exprimat o preferință clară pentru acestea din urmă (a se vedea p. 13-14).

III. Analiza dispozițiilor

III.1. Prezentare generală a articolului 7

Articolul 7 prevede că datele cu caracter personal pot fi prelucrate numai în cazul în care se aplică cel puțin unul dintre cele șase temeiuri juridice enumerate la articolul respectiv. Înainte de a analiza fiecare dintre temeiuri, prezenta secțiune III.1 oferă o prezentare generală a articolului 7 și a relației sale cu articolul 8 privind categoriile speciale de date.

III.1.1. Consimțământul sau „necesară pentru..."

Se poate face o distincție între cazul în care datele cu caracter personal sunt prelucrate pe baza consimțământului neechivoc al persoanei vizate [articolul 7 litera (a)] și celelalte cinci cazuri [articolul 7 litera (b)-(f)]. Cele cinci cazuri – pe scurt – prezintă scenarii în care prelucrarea poate fi necesară într-un context specific, cum ar fi executarea unui contract cu persoana vizată, respectarea unei obligații legale impuse operatorului etc.

În primul caz, în conformitate cu articolul 7 litera (a), persoanele vizate sunt cele care autorizează prelucrarea datelor lor cu caracter personal. Rămâne la latitudinea acestora să decidă dacă permit prelucrarea propriilor date. În același timp, consimțământul nu elimină necesitatea de a respecta principiile prevăzute la articolul 6[27]. În plus, consimțământul trebuie să îndeplinească anumite condiții esențiale pentru a fi legitim, astfel cum este explicat în Avizul nr. 15/2011 al grupului de lucru[28]. Întrucât prelucrarea datelor utilizatorului este, în ultimă instanță, la discreția sa, accentul se plasează pe validitatea și domeniul de aplicare a consimțământului persoanei vizate.

Cu alte cuvinte, primul temei, articolul 7 litera (a), se axează pe dreptul la autodeterminare al persoanei vizate ca temei de legitimitate. În schimb, toate celelalte temeiuri permit prelucrarea – sub rezerva unor garanții și măsuri – în situații în care, indiferent de acordarea consimțământului, este oportun și necesar să se prelucreze datele într-un anumit context pentru realizarea unui anumit interes legitim.

Fiecare dintre literele (b), (c), (d) și (e) specifică un criteriu privind legitimitatea prelucrării:

(b) executarea unui contract la care persoana vizată este parte;
(c) îndeplinirea unei obligații legale care îi revine operatorului;
(d) protejarea interesului vital al persoanei vizate;
(e) îndeplinirea unei sarcini de interes public.

[27] Hotărârea Curții Supreme a Țărilor de Jos din 9 septembrie 2011 în cauza: ECLI:NL:HR:2011:BQ8097, punctul 3.3 litera (e) cu privire la principiul proporționalității. A se vedea, de asemenea, pagina 7 din Avizul grupului de lucru 15/2011, citat la nota de subsol 2: „... obținerea consimțământului nu neagă obligațiile operatorului în temeiul articolului 6 cu privire la corectitudinea, necesitatea și proporționalitatea, precum și calitatea datelor. De exemplu, chiar și în cazul în care prelucrarea datelor cu caracter personal se bazează pe consimțământul utilizatorului, acest lucru nu ar justifica culegerea de date care este excesivă în raport cu un anumit scop".

[28] A se vedea paginile 11-25 din Avizul nr. 15/2011, citat la nota de subsol 2 de mai sus.

Litera (f) este mai puțin specifică și se referă, într-un mod general, la interesul legitim (de orice tip) urmărit de operator (în orice situație). Totuși, această dispoziție cu caracter general este condiționată de un test comparativ suplimentar, care urmărește să protejeze interesul și drepturile persoanelor vizate, astfel cum se va arăta în secțiunea III.2.

Evaluarea respectării criteriilor stabilite la articolul 7 literele (a)-(f) este realizată inițial, în toate cazurile, de către operatorul de date, sub rezerva dispozițiilor aplicabile și a orientărilor cu privire la modul în care ar trebui să se aplice legea. În a doua instanță, legitimitatea prelucrării poate fi supusă unei evaluări suplimentare și ar putea fi contestată de persoanele vizate, de alte părți interesate, de autoritățile în materie de protecție a datelor și, în cele din urmă, hotărâtă de instanțe.

Pentru a completa această scurtă prezentare, trebuie menționat că, după cum se va arăta în secțiunea III.3.6, cel puțin în cazurile menționate la literele (e) și (f), persoana vizată își poate exercita dreptul de opoziție, astfel cum se prevede la articolul 14[29]. Acest fapt va declanșa o nouă evaluare a intereselor în discuție sau, în cazul activităților de marketing direct [articolul 14 litera (b)], va necesita ca operatorul să înceteze prelucrarea datelor cu caracter personal, fără o evaluare suplimentară.

III.1.2. Relația cu articolul 8

Articolul 8 din directivă reglementează, de asemenea, prelucrarea anumitor categorii de date cu caracter personal. Acesta se referă în mod specific la datele „care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența sindicală, precum și prelucrarea datelor privind sănătatea sau viața sexuală” [articolul 8 alineatul (1)] și la datele „referitoare la infracțiuni sau condamnări penale” [articolul 8 alineatul (5)].

Prelucrarea unor astfel de date este în principiu interzisă, sub rezerva anumitor excepții. Articolul 8 alineatul (2) prevede o serie de excepții de la interdicție, în conformitate cu literele (a)-(e). Articolul 8 alineatele (3) și (4) prevede excepții suplimentare. Unele dintre dispoziții sunt similare – dar nu identice – cu dispozițiile prevăzute la articolul 7 literele (a)-(f).

Condițiile specifice de la articolul 8, precum și faptul că unele dintre temeiurile enumerate la articolul 7 se aseamănă cu condițiile stabilite la articolul 8, a ridicat problema relației dintre cele două dispoziții.

În cazul în care articolul 8 este conceput ca o *lex specialis*, ar trebui să se analizeze dacă aceasta exclude aplicabilitatea articolului 7 în totalitate. În caz afirmativ, aceasta ar însemna că, dacă se aplică una dintre excepțiile de la articolul 8, categoriile speciale de date cu caracter personal pot fi prelucrate fără a respecta articolul 7. Cu toate acestea, este posibil, de asemenea, ca relația să fie mai complexă și să fie necesară aplicarea cumulativă a articolelor 7 și 8[30].

[29] În conformitate cu articolul 14 litera (a), acest drept se aplică „cu excepția cazului în care se prevede altfel în legislația națională”. De exemplu, în Suedia, legislația națională nu permite posibilitatea de opoziție la o prelucrare în baza articolului 7 litera (e).

[30] Întrucât articolul 8 este creat ca o *interdicție cu excepții*, excepțiile pot fi considerate cerințe, care doar limitează domeniul de aplicare a interdicției, dar nu oferă ele însele un temei juridic suficient pentru prelucrare. În această lectură, aplicabilitatea excepțiilor de la articolul 8 nu exclude aplicabilitatea cerințelor de la articolul 7 și, dacă este cazul, ambele trebuie să fie aplicate cumulativ.

În orice caz, este clar că obiectivul de politică este de a oferi protecție suplimentară pentru categoriile speciale de date. Prin urmare, rezultatul final al analizei ar trebui să fie la fel de clar: aplicarea articolului 8, ca atare sau în mod cumulativ cu articolul 7, urmărește să ofere un nivel mai ridicat de protecție pentru categorii speciale de date.

În practică, deși în unele cazuri articolul 8 introduce cerințe mai stricte, cum ar fi consimțământul „explicit" la articolul 8 alineatul (2) litera (a) în comparație cu „consimțământul neechivoc" de la articolul 7 – acest lucru nu este valabil pentru toate dispozițiile. Unele excepții prevăzute la articolul 8 nu par echivalente sau mai stricte decât temeiurile enumerate la articolul 7. Ar fi inadecvat să se ajungă, de exemplu, la concluzia că faptul că o persoană a făcut publice în mod manifest categorii speciale de date în temeiul articolului 8 alineatul (2) litera (e) ar fi – întotdeauna și ca atare – o condiție suficientă pentru a permite orice tip de prelucrare a datelor respective, fără o evaluare a echilibrului între interesele și drepturile în cauză, astfel cum se prevede la articolul 7 litera (f)[31].

În unele situații, faptul că operatorul de date este un partid politic ar ridica, de asemenea, interdicția privind prelucrarea categoriilor speciale de date în conformitate cu articolul 8 alineatul (2) litera (d). Aceasta nu înseamnă însă că orice prelucrare în domeniul de aplicare a acestei dispoziții este în mod necesar legală. Situația trebuie să fie evaluată separat și operatorul poate fi obligat să demonstreze, de exemplu, că prelucrarea datelor cu caracter personal este necesară pentru executarea unui contract [articolul 7 litera (b)] sau că interesul său legitim prevalează, în conformitate cu articolul 7 litera (f). În cel din urmă caz, testul comparativ în temeiul articolului 7 litera (f) trebuie să fie efectuat după ce s-a stabilit că operatorul respectă cerințele de la articolul 8.

În mod similar, simplul fapt că „prelucrarea datelor este necesară în scopuri legate de medicina preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente ori de gestionarea serviciilor de sănătate", iar datele sunt prelucrate conform unei obligații de confidențialitate – toate astfel cum sunt menționate la articolul 8 alineatul (3) – implică faptul că o astfel de prelucrare a datelor sensibile este *exceptată de la interdicția* prevăzută la articolul 8 alineatul (1). Cu toate acestea, acest aspect nu este neapărat suficient pentru a asigura legalitatea în conformitate cu articolul 7 și va necesita un temei juridic, cum ar fi un contract cu pacientul în temeiul articolului 7 litera (b), o obligație legală în temeiul articolului 7 litera (c), îndeplinirea unei sarcini de interes public, în conformitate cu articolul 7 litera (e) sau un test comparativ în temeiul articolului 7 litera (f).

În concluzie, grupul de lucru consideră că trebuie să se efectueze o analiză de la caz la caz pentru a verifica dacă articolul 8 în sine prevede condiții mai stricte și suficiente[32] sau dacă este necesară o aplicare cumulativă atât a articolului 8, cât și a articolului 7 pentru a asigura

[31] În afară de aceasta, articolul 8 alineatul (2) litera (e) nu ar trebui interpretat în sens contrar, în sensul că, atunci când datele făcute publice de către persoana vizată nu sunt sensibile, acestea pot fi prelucrate fără nicio condiție suplimentară. Datele accesibile publicului sunt în continuare date cu caracter personal supuse cerințelor de protecție a datelor, inclusiv în ce privește respectarea articolului 7, indiferent dacă acestea sunt sau nu date sensibile.

[32] A se vedea analiza efectuată în avizul privind WADA al grupului de lucru, punctul 3.3, care ia în considerare atât articolul 7, cât și articolul 8 din directivă: Al doilea aviz nr. 4/2009 referitor la Standardul internațional privind protecția vieții private și a informațiilor cu caracter personal al Agenției Mondiale Antidoping (WADA), la dispozițiile relevante ale Codului WADA și la alte aspecte din domeniul vieții private, în contextul combaterii dopajului în sport de către WADA și organizațiile (naționale) antidoping, adoptat la 6.4.2009 (WP162).

protecția deplină a persoanelor vizate. Rezultatul examinării nu trebuie să conducă în niciun caz la o protecție mai scăzută pentru categoriile speciale de date[33].

Acest lucru înseamnă, de asemenea, că un operator care prelucrează categorii speciale de date nu poate invoca niciodată *numai* un temei juridic prevăzut la articolul 7 pentru a legitima o activitate de prelucrare a datelor. După caz, articolul 7 nu va *prevala,* ci se aplică întotdeauna în mod *cumulativ* cu articolul 8 pentru a se asigura că toate garanțiile și măsurile relevante sunt respectate. Acest lucru va fi cu atât mai relevant în cazul în care statele membre decid să adauge derogări suplimentare celor prevăzute la articolul 8, astfel cum se prevede la articolul 8 alineatul (4).

III.2. Articolul 7 literele (a)-(e)

Prezenta secțiune III.2 oferă o scurtă descriere a fiecăruia dintre temeiurile juridice de la articolul 7 literele (a)-(e) din directivă, înainte ca avizul să se concentreze, în secțiunea III.3, asupra articolului 7 litera (f). Analiza va sublinia, de asemenea, câteva dintre cele mai frecvente interfețe dintre aceste temeiuri juridice care se referă, de exemplu, la „contract", „obligație legală" și „interes legitim", în funcție de contextul respectiv și elementele de fapt în speță.

III.2.1. Consimțământul

Consimțământul ca temei juridic a fost analizat în Avizul nr. 15/2011 al grupului de lucru privind definiția consimțământului. Principala concluzie a avizului respectiv este că acordarea consimțământului constituie unul dintre temeiurile juridice pentru prelucrarea datelor cu caracter personal, mai degrabă decât temeiul principal. Acesta joacă un rol important, însă nu exclude posibilitatea, în funcție de context, ca alte argumente juridice să fie mai adecvate, fie din perspectiva operatorului, fie din perspectiva persoanei vizate. Dacă este utilizat în mod corespunzător, consimțământul reprezintă un instrument care acordă persoanei vizate control asupra prelucrării datelor sale. În cazul în care este utilizat incorect, controlul persoanei vizate devine iluzoriu și consimțământul constituie o bază inadecvată pentru prelucrare.

Printre recomandările sale, grupul de lucru a insistat asupra necesității de a clarifica ce înseamnă „consimțământul neechivoc": „Clarificarea trebuie să se facă în sensul sublinierii faptului că acordarea consimțământului neechivoc necesită utilizarea unor mecanisme care nu lasă loc de îndoieli cu privire la intenția persoanei vizate de a acorda consimțământul. În același timp, trebuie să se specifice faptul că utilizarea opțiunilor prestabilite pe care persoana vizată trebuie să le modifice pentru a refuza prelucrarea (consimțământul bazat pe tăcere) nu constituie ca atare consimțământ neechivoc. Acest lucru este în special valabil în mediul online"[34]. De asemenea, avizul a solicitat operatorilor de date să pună în aplicare mecanisme pentru a demonstra consimțământul (în cadrul unei obligații de răspundere generală) și a solicitat legiuitorului să adauge o obligație explicită privind calitatea și accesibilitatea informațiilor care constituie baza pentru consimțământ.

[33] Este de la sine înțeles că în cazul aplicării articolului 8 trebuie, de asemenea, să se asigure respectarea celorlalte dispoziții ale directivei, inclusiv articolul 6.

[34] A se vedea pagina 36 din Avizul nr. 15/2011 al grupului de lucru privind definiția consimțământului.

III.2.2. Contractul

Articolul 7 litera (b) oferă un temei juridic în situațiile în care „prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau în vederea luării unor măsuri, la cererea acesteia, înainte de încheierea contractului”. Acesta reglementează două scenarii diferite.

i) În primul rând, dispoziția se referă la situațiile în care prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte. Aceasta poate include, de exemplu, prelucrarea adresei persoanei vizate astfel încât bunurile cumpărate online să poată fi livrate sau prelucrarea detaliilor privind cardurile de credit pentru a efectua plata. În contextul ocupării forței de muncă, acest temei poate permite, de exemplu, prelucrarea informațiilor referitoare la salarii și a detaliilor privind conturile bancare astfel încât să se poată plăti salariile.

Dispoziția în cauză trebuie să fie interpretată în mod strict și nu acoperă situațiile în care prelucrarea nu este cu adevărat *necesară* pentru executarea unui contract, ci este mai degrabă impusă în mod unilateral asupra persoanei vizate de către operator. De asemenea, faptul că o anumită prelucrare a datelor face obiectul unui contract nu înseamnă în mod automat că prelucrarea este necesară pentru executarea acestuia. De exemplu, articolul 7 litera (b) nu este un temei juridic adecvat pentru crearea unui profil al gusturilor și al stilului de viață al utilizatorului în funcție de activitatea sa pe o pagină de internet și de articolele cumpărate, întrucât operatorul de date nu a fost contractat pentru a realiza crearea de profiluri, ci mai degrabă pentru a furniza, de exemplu, anumite bunuri și servicii. Chiar dacă astfel de activități de prelucrare sunt menționate în mod specific în textul tipărit cu caractere de dimensiuni mici al contractului, acest fapt în sine nu le face să fie „necesare” pentru executarea contractului.

Există o legătură clară între evaluarea necesității și respectarea principiului limitării scopului. Este important să se stabilească cu exactitate *motivele* încheierii contractului, și anume conținutul său și obiectivul fundamental, întrucât acesta este contextul în care se va verifica dacă prelucrarea datelor este necesară pentru executarea acestuia.

În unele situații limită poate fi discutabil sau poate fi necesară mai multă muncă de informare specifică pentru a se determina dacă prelucrarea este necesară pentru executarea contractului. De exemplu, stabilirea unei baze interne de date de contact ale angajaților, care conține numele, adresa comercială, numărul de telefon și adresa de e-mail ale tuturor angajaților, pentru a permite angajaților să ia legătura cu colegii lor, poate fi considerată necesară, în anumite situații, pentru executarea unui contract în temeiul articolului 7 litera (b), dar ar putea, de asemenea, să fie legală în temeiul articolului 7 litera (f), în cazul în care interesul superior al operatorului este demonstrat și sunt luate toate măsurile adecvate, inclusiv, de exemplu, consultarea adecvată a reprezentanților angajaților.

Alte cazuri, de exemplu, monitorizarea electronică a utilizării internetului, a emailului sau a telefonului de către angajați sau supravegherea video a angajaților constituie în mod mai clar o prelucrare care este probabil să depășească ceea ce este necesar pentru executarea unui contract de muncă, chiar dacă într-un astfel de caz, de asemenea, aceasta poate să depindă de natura locului de muncă. Prevenirea fraudei – care poate

include, printre altele, monitorizarea și crearea de profiluri ale consumatorilor – este un alt domeniu specific, care ar putea fi considerat ca depășind ceea ce este necesar pentru executarea unui contract. O astfel de prelucrare ar putea totuși legitimă în conformitate cu un alt temei de la articolul 7, de exemplu, consimțământul, după caz, o obligație legală sau interesul legitim al operatorului [articolul 7 literele (a), (c) sau (f)][35]. În cel din urmă caz, prelucrarea ar trebui să facă obiectul unor garanții și măsuri suplimentare pentru a proteja în mod adecvat interesele sau drepturile și libertățile persoanelor vizate.

Articolul 7 litera (b) se aplică numai la ceea ce este necesar pentru *executarea* unui contract. Acesta nu se aplică tuturor celorlalte acțiuni viitoare declanșate de nerespectare sau oricăror altor incidente în executarea unui contract. Atât timp cât prelucrarea vizează executarea normală a unui contract, aceasta ar putea intra sub incidența articolului 7 litera (b). Dacă există un incident în executare, care dă naștere unui conflict, prelucrarea datelor poate lua o altă direcție. Prelucrarea informațiilor de bază ale persoanei vizate, cum ar fi numele, adresa și trimiterea la obligațiile contractuale restante, comunicarea de notificări oficiale ar trebui să fie considerată ca încadrându-se în prelucrarea datelor necesară pentru executarea unui contract. În ceea ce privește prelucrarea mai elaborată a datelor, care poate sau nu să implice terți, cum ar fi colectarea datoriei externe sau aducerea în instanță a unui client care nu a plătit pentru un serviciu, s-ar putea argumenta că o astfel de prelucrare nu mai are loc în cadrul executării „normale" a contractului și, prin urmare, nu intră sub incidența articolului 7 litera (b). Cu toate acestea, acest lucru nu ar face prelucrarea nelegitimă ca atare: operatorul are un interes legitim să identifice soluții pentru a se asigura că sunt respectate drepturile sale contractuale. S-ar putea invoca alte temeiuri legale, cum ar fi articolul 7 litera (f), sub rezerva unor garanții și măsuri adecvate și a satisfacerii testului comparativ[36].

ii) În al doilea rând, articolul 7 litera (b) reglementează, de asemenea, prelucrarea care are loc *înainte* de încheierea unui contract. Aceasta include relațiile precontractuale, cu condiția să se ia măsuri la cererea persoanei vizate, mai degrabă decât la inițiativa operatorului sau a oricărui terț. De exemplu, dacă o persoană solicită unui comerciant cu amănuntul să îi transmită o ofertă pentru un produs, prelucrarea în aceste scopuri, cum ar fi păstrarea detaliilor privind adresa și a informațiilor cu privire la ceea ce s-a solicitat, pentru o perioadă limitată de timp, va fi oportună în conformitate cu acest temei juridic. În mod similar, în cazul în care o persoană solicită o cotație din partea unui asigurător pentru autovehiculul său, asigurătorul poate prelucra datele necesare, de exemplu, marca și vârsta mașinii și alte date relevante și proporționale, în scopul de a pregăti cotația.

---

[35] Un alt exemplu de temeiuri juridice multiple se regăsește în Avizul nr. 15/2011 al grupului de lucru privind definiția consimțământului (citat la nota de subsol 2). Pentru achiziționarea unui automobil, operatorul de date poate avea dreptul să prelucreze datele cu caracter personal în conformitate cu diferitele scopuri și pe baza unor criterii diferite:
- datele necesare pentru a cumpăra mașina: articolul 7 alineatul (b),
- prelucrarea documentelor mașinii: articolul 7 alineatul (c),
- pentru servicii de gestionare a clienților (de exemplu, pentru a beneficia de întreținere pentru mașină în diferite societăți afiliate din UE): articolul 7 alineatul (f),
- transferarea datelor către terți pentru propriile activități de marketing: articolul 7 alineatul (a).

[36] Cu privire la categoriile speciale de date, ar putea fi necesar să se ia în considerare, de asemenea, articolul 8 alineatul (1) litera (e) – „necesare pentru constatarea, exercitarea sau apărarea unui drept în justiție".

Cu toate acestea, verificarea antecedentelor, de exemplu, prelucrarea datelor legate de vizitele medicale înainte ca o societate de asigurări să ofere unui solicitant o asigurare de sănătate sau o asigurare de viață, nu ar fi considerate măsuri necesare efectuate la cererea persoanei vizate. De asemenea, controalele informațiilor privind creditele înainte de acordarea unui împrumut nu sunt efectuate *la cererea* persoanei vizate, în conformitate cu articolul 7 litera (b), ci mai degrabă în conformitate cu articolul 7 litera (f) sau în conformitate cu articolul 7 litera (c) în temeiul unei obligații legale a băncilor de a consulta o listă oficială a debitorilor înregistrați.

Marketingul direct la inițiativa comerciantului cu amănuntul/operatorului nu va fi posibil în acest temei. În unele cazuri, articolul 7 litera (f) ar putea constitui un temei juridic adecvat în locul articolului 7 litera (b), sub rezerva unor garanții și măsuri adecvate și a satisfacerii testului comparativ. În alte cazuri, inclusiv cele care implică o activitate extensivă de creare de profiluri, punerea în comun a datelor, marketingul direct online sau publicitatea comportamentală, ar trebui să se ia în considerare consimțământul în temeiul articolului 7 litera (a), astfel cum rezultă din analiza de mai jos[37].

III.2.3. Obligația juridică

Articolul 7 litera (c) prevede un temei juridic în situațiile în care „prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului”. Acest lucru ar putea fi valabil, de exemplu, în cazul în care angajatorii trebuie să raporteze date privind salariile angajaților lor către autoritățile financiare sau de securitate socială sau atunci când instituțiile financiare sunt obligate să raporteze anumite tranzacții suspecte autorităților competente, în temeiul normelor privind combaterea spălării banilor. De asemenea, aceasta ar putea fi o obligație la care este supusă o autoritate publică, întrucât nimic nu limitează aplicarea articolului 7 litera (c) la sectorul public sau privat. Acest lucru se aplică, de exemplu, colectării de date de către o autoritate locală în scopul gestionării amenzilor pentru parcarea în locuri nepermise.

Articolul 7 litera (c) prezintă similitudini cu articolul 7 litera (e), întrucât o sarcină de interes public se bazează adesea pe o dispoziție legală sau este derivată din aceasta. Cu toate acestea, domeniul de aplicare a articolului 7 litera (c) este strict delimitat.

Pentru a se aplica articolul 7 litera (c), obligația trebuie să fie impusă prin lege (și nu, de exemplu, printr-un acord contractual). Legea trebuie să îndeplinească toate condițiile relevante pentru ca obligația să fie valabilă și obligatorie și trebuie să respecte, de asemenea, legislația în materie de protecție a datelor, inclusiv cerința necesității, proporționalității[38] și limitării scopului.

De asemenea, este important să se sublinieze faptul că articolul 7 litera (c) se referă la legislația Uniunii Europene sau a unui stat membru. Obligațiile în conformitate cu legislația din țările terțe (cum ar fi, de exemplu, obligația de a institui sisteme de denunțare, în

[37] A se vedea secțiunea III.3.6 (b), capitolul „Ilustrare: evoluția abordării marketingul direct”, paginile 45-46.
[38] A se vedea, de asemenea, Avizul nr. 1/2014 al grupului de lucru privind aplicarea conceptelor de necesitate și proporționalitate și protecția datelor în domeniul aplicării legii, adoptat la 27.2.2014 (WP211).

conformitate cu legea Sarbanes-Oxley adoptată în Statele Unite în 2002) nu sunt acoperite de acest temei. Pentru a fi valabilă, o obligație legală dintr-o țară terță ar trebui să fie recunoscută în mod oficial și integrată în ordinea juridică a statului membru în cauză, de exemplu sub forma unui acord internațional[39]. Cu toate acestea, necesitatea de a se conforma unei obligații legale străine poate reprezenta un interes legitim al operatorului, dar numai sub rezerva testului comparativ menționat la articolul 7 litera (f) și cu condiția instituirii unor garanții adecvate, de tipul celor aprobate de autoritatea pentru protecția datelor.

Operatorul nu trebuie să aibă posibilitatea de a alege dacă să îndeplinească sau nu obligația. Prin urmare, angajamentele unilaterale voluntare și parteneriatele public-private de prelucrare a datelor, dincolo de ceea ce este prevăzut de lege, nu fac obiectul articolului 7 litera (c). De exemplu, în cazul în care – fără o obligație juridică clar și specifică în acest sens – un furnizor de servicii de internet decide să își monitorizeze utilizatorii într-un efort de a combate descărcarea ilegală, articolul 7 litera (c) nu va constitui un temei juridic adecvat în acest scop.

De asemenea, obligația legală în sine trebuie să fie suficient de clară în ceea ce privește prelucrarea datelor cu caracter personal pe care o impune. Prin urmare, articolul 7 litera (c) se aplică pe baza unor dispoziții legislative care se referă în mod explicit la natura și obiectul prelucrării. Operatorul nu ar trebui să aibă o putere discreționară nejustificată cu privire la modul de îndeplinire a obligației legale.

În unele cazuri, legislația poate stabili doar un obiectiv general, în timp ce obligațiile mai specifice sunt impuse la un nivel diferit, de exemplu, fie în legislația secundară, fie printr-o decizie cu caracter obligatoriu a unei autorități publice într-un caz concret. Acest lucru poate conduce, de asemenea, la obligații juridice în conformitate cu articolul 7 litera (c), cu condiția ca natura și obiectul prelucrării să fie bine definite și să facă obiectul unui temei juridic adecvat.

Cu toate acestea, situația este diferită în cazul în care o autoritate de reglementare nu face decât să furnizeze orientări generale de politică și condiții în care ar putea lua în considerare utilizarea competențelor sale executive (de exemplu, orientări în materie de reglementare ale instituțiilor financiare privind anumite standarde de precauție). În astfel de cazuri, activitățile de prelucrare ar trebui să fie evaluate în conformitate cu articolul 7 litera (f) și să fie considerate legitime numai sub rezerva testului comparativ suplimentar[40].

Ca o observație generală, trebuie remarcat faptul că unele activități de prelucrare pot părea aproape de domeniul de aplicare a articolului 7 litera (c) sau a articolului 7 litera (b), fără a îndeplini în totalitate criteriile pentru aplicarea temeiurilor respective. Aceasta nu înseamnă că o astfel de prelucrare este întotdeauna în mod necesar ilegală: uneori aceasta poate fi legitimă, dar mai degrabă în conformitate cu articolul 7 litera (f), cu condiția satisfacerii testului comparativ suplimentar.

[39] A se vedea în această privință secțiunea 4.2.2 din Avizul nr. 10/2006 al grupului de lucru privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT), adoptat la 20.11.2006 (WP128) și Avizul nr. 1/2006 al grupului de lucru privind aplicarea normelor UE de protecție a datelor în cazul sistemelor de informare în domeniul contabilității, controalelor contabile interne, auditării, combaterii corupției și infracționalității bancare și financiare, adoptat la 1.2.2006 (WP117).

[40] Orientările emise de către o autoritate de reglementare pot să joace un rol în evaluarea interesului legitim al operatorului [a se vedea secțiunea III.3.4 litera (a), în special pagina 36].

III.2.4. Interesul vital

Articolul 7 litera (d) prevede un temei juridic în situațiile în care „prelucrarea este necesară în scopul protejării interesului vital al persoanei vizate”. Formularea este diferită de limbajul utilizat la articolul 8 alineatul (2) litera (c), care este mai specific și se referă la situații în care „prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane, atunci când persoana vizată se află în incapacitatea fizică sau juridică să-și dea consimțământul”.

Cu toate acestea, ambele dispoziții par să sugereze că acest temei juridic ar trebui să aibă o aplicare limitată. În primul rând, expresia „interes vital” pare să limiteze aplicarea temeiului la chestiuni de viață și de moarte sau, cel puțin, la amenințări care prezintă un risc de vătămare sau de producere a vreunui alt prejudiciu adus sănătății persoanei vizate [sau, în cazul articolului 8 alineatul (2) litera (c), de asemenea, a altei persoane].

Considerentul 31 confirmă faptul că obiectivul acestui temei juridic este de a „proteja un interes care este esențial pentru viața persoanei vizate”. Cu toate acestea, directiva nu precizează dacă amenințarea trebuie să fie imediată. Aceasta are implicații asupra domeniului de aplicare a colectării de date, de exemplu ca măsură preventivă sau pe scară largă, cum ar fi culegerea de date ale pasagerilor companiilor aeriene în cazul în care a fost identificat un risc de boală epidemiologică sau un incident de securitate.

Grupul de lucru consideră că trebuie să se acorde o interpretare restrictivă dispoziției în cauză, în concordanță cu spiritul articolului 8. Deși articolul 7 litera (d) nu limitează în mod specific utilizarea acestui temei la situații în care consimțământul nu poate fi utilizat ca temei juridic, din motivele prevăzute la articolul 8 alineatul (2) litera (c), este rezonabil să se presupună că, în situațiile în care există posibilitatea și necesitatea de a solicita un consimțământ valabil, ori de câte ori este posibil, ar trebui efectiv să se solicite consimțământul. Aceasta ar limita, de asemenea, aplicarea dispoziției respective la o analiză de la caz la caz și nu poate fi utilizată în mod normal pentru a legitima orice colectare sau prelucrare masivă a datelor cu caracter personal. În cazul în care acest lucru ar fi necesar, articolul 7 literele (c) sau (e) ar reprezenta temeiuri mai adecvate pentru prelucrare.

III.2.5. Sarcina publică

Articolul 7 litera (e) prevede un temei juridic în situațiile în care „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”.

Este important de remarcat că, asemenea articolului 7 litera (c), articolul 7 litera (e) se referă la interesul public al Uniunii Europene sau al unui stat membru. În mod similar, „autoritatea publică” se referă la o autoritate acordată de Uniunea Europeană sau un stat membru. Cu alte cuvinte, sarcinile realizate în interesul public al unei țări terțe sau care rezultă din exercitarea autorității publice cu care o entitate este învestită în temeiul legislației străine nu intră în domeniul de aplicare a dispoziției[41].

[41] A se vedea secțiunea 2.4 din documentul de lucru al grupului de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995, adoptat la 25 noiembrie 2005

Articolul 7 litera (e) se referă la două situații și este relevant atât pentru sectorul public, cât și pentru sectorul privat. În primul rând, aceasta se referă la situațiile în care operatorul însuși are o sarcină de autoritate publică sau o sarcină de interes public (dar nu neapărat și o obligație legală de a prelucra datele) și prelucrarea este necesară pentru exercitarea autorității sau desfășurarea activității respective. De exemplu, o autoritate fiscală poate colecta și prelucra declarația fiscală a unei persoane în vederea stabilirii și a verificării cuantumului impozitului care trebuie plătit. De asemenea, o asociație profesională, cum ar fi un barou sau o asociație a profesioniștilor din domeniul medical, învestită cu o autoritate publică în acest sens, poate efectua proceduri disciplinare împotriva unora dintre membrii săi. Un alt exemplu ar putea fi un organism public local, cum ar fi o autoritate municipală, însărcinat cu gestionarea unui serviciu de bibliotecă, a unei școli sau a unei piscine locale.

În al doilea rând, articolul 7 litera (e) vizează, de asemenea, situațiile în care operatorul nu are o autoritate oficială, dar este solicitat de un terț care are autoritatea să divulge date. De exemplu, un funcționar al unei autorități publice competente pentru investigarea criminalității poate solicita operatorului să coopereze în cadrul unei anchete în curs, mai degrabă decât să impună operatorului să respecte o cerere specifică de a coopera. Articolul 7 litera (e) se poate referi, de asemenea, la situațiile în care operatorul divulgă în mod proactiv datele către un terț care are o astfel de autoritate publică. Acesta poate fi cazul, de exemplu, atunci când un operator constată că a fost săvârșită o infracțiune și furnizează informații autorităților competente de aplicare a legii din proprie inițiativă.

Spre deosebire de cazul articolului 7 litera (c), nu există nicio cerință ca operatorul să acționeze în conformitate cu o obligație legală. Utilizând exemplul de mai sus, un operator care observă din întâmplare că s-a săvârșit un furt sau o fraudă este posibil să nu aibă obligația legală de a sesiza acest lucru poliției, dar poate, cu toate acestea, în cazurile corespunzătoare, să facă aceasta în mod voluntar în conformitate cu articolul 7 litera (e).

Cu toate acestea, prelucrarea trebuie să fie „necesară pentru aducerea la îndeplinire a unei sarcini de interes public”. În mod alternativ, fie operatorul, fie terțul căruia operatorul îi divulgă datele trebuie să fie învestit cu o autoritate oficială și prelucrarea datelor trebuie să fie necesară pentru a exercita autoritatea respectivă[42]. De asemenea, este important să se sublinieze că o astfel de autoritate oficială sau sarcină publică trebuie, de regulă, să fi fost atribuită prin acte cu putere de lege sau alte norme juridice. În cazul în care prelucrarea implică o încălcare a vieții private sau dacă acest lucru este necesar în temeiul dreptului național pentru a asigura protecția persoanelor în cauză, temeiul juridic ar trebui să fie suficient de specific și de precis în ceea ce privește tipul de prelucrare a datelor care poate fi permis.

Astfel de situații sunt din ce în ce mai frecvente, de asemenea, în afara sectorului public, având în vedere tendința de externalizare a atribuțiilor guvernamentale către entități din sectorul privat. Acesta poate fi cazul, de exemplu, în contextul unor activități de prelucrare de date în sectorul transportului sau al sănătății (de exemplu, studii epidemiologice, cercetare).

(WP114), pentru o interpretare similară a noțiunii de „temeiuri importante de interes public” de la articolul 26 alineatul (1) litera (d).

[42] Cu alte cuvinte, în astfel de cazuri, relevanța publică a sarcinilor și responsabilitatea corespunzătoare va continua să existe chiar și în cazul în care executarea sarcinii a fost transferată către alte entități, inclusiv cele private.

De asemenea, acest temei ar putea fi invocat într-un context de aplicare a legii, astfel cum s-a sugerat deja în exemplele de mai sus. Cu toate acestea, măsura în care o întreprindere privată ar putea fi autorizată să coopereze cu autoritățile de aplicare a legii, de exemplu în lupta împotriva fraudei sau a conținutului ilegal de pe internet, necesită analizarea nu numai în temeiul articolului 7, ci și în temeiul articolului 6, având în vedere cerințele privind limitarea scopului, legalitatea și corectitudinea[43].

Articolul 7 litera (e) are în mod potențial un domeniu de aplicare foarte extins, ceea ce face necesară o interpretare strictă și o identificare clară, de la caz la caz, a interesului public aflat în discuție și a autorității oficiale care justifică prelucrarea. Domeniul de aplicare extins reprezintă, de asemenea, motivul pentru care, la fel precum în cazul articolului 7 litera (f), la articolul 14 a fost prevăzut un drept de opoziție atunci când prelucrarea se bazează pe articolul 7 litera (e)[44]. Astfel, în ambele cazuri, se pot aplica garanții și măsuri suplimentare similare [45].

În acest sens, articolul 7 litera (e) prezintă similitudini cu articolul 7 litera (f) și, în anumite contexte, în special în ceea ce privește autoritățile publice, articolul 7 litera (e) poate înlocui articolul 7 litera (f).

Atunci când se analizează domeniul de aplicare a dispozițiilor în cauză la organele din sectorul public, în special având în vedere modificările propuse ale cadrului juridic privind protecția datelor, este util să se remarce faptul că actualul text al Regulamentului (CE) nr. 45/2001[46], care conține normele de protecție a datelor aplicabile instituțiilor și organismelor Uniunii Europene, nu include nicio dispoziție comparabilă cu articolul 7 litera (f).

Cu toate acestea, considerentul 27 din regulamentul respectiv prevede că „prelucrarea de date cu caracter personal în scopul îndeplinirii unor misiuni de interes public de către instituțiile și organe comunitare include prelucrarea datelor cu caracter personal necesare administrării și funcționării acestor instituții și organe”. Prin urmare, această dispoziție permite prelucrarea datelor în baza unui temei de „misiune publică” interpretată în sens larg într-un număr mare de cazuri, care altfel ar fi putut fi acoperite de o dispoziție similară celei de la articolul 7 litera (f). Supravegherea video a spațiilor în scopuri de securitate, monitorizarea electronică a traficului de mesaje electronice sau evaluările personalului sunt doar câteva exemple de acțiuni care se pot încadra în această dispoziție interpretată în sens larg privind îndeplinirea „unor misiuni de interes public”.

Privind în perspectivă, este important, de asemenea, să se ia în considerare că propunerea de regulament prevede în mod expres la articolul 6 alineatul (1) litera (f) că temeiul interesului

[43] A se vedea, în acest sens, Avizul grupului de lucru privind SWIFT (citat la nota de subsol 39 de mai sus), Avizul nr. 4/2003 al grupului de lucru privind nivelul de protecție asigurat în Statele Unite pentru transferul de date ale pasagerilor”, adoptat la 13.6.2003 (WP78) și documentul de lucru privind aspectele de protecție a datelor legate de drepturile de proprietate intelectuală, adoptat la 18.1.2005 (WP104).

[44] Astfel cum s-a menționat mai sus, posibilitatea de opoziție nu există în unele state membre (de exemplu, Suedia) în ceea ce privește prelucrarea datelor în temeiul articolului 7 litera (e).

[45] Astfel cum se va arăta în continuare, proiectul de raport al Comisiei LIBE propune garanții suplimentare – în special, creșterea transparenței – în cazul în care se aplică articolul 7 litera (f).

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

legitim „nu se aplică în cazul prelucrării efectuate de către autoritățile publice în îndeplinirea sarcinilor care le revin”. În cazul în care această dispoziție este adoptată și va fi interpretată în sens larg astfel încât să excludă în totalitate utilizarea de către autoritățile publice a interesului legitim ca temei juridic, atunci temeiurile privind „interesul general” și „autoritatea publică” prevăzute la articolul 7 litera (e) trebuie să fie interpretate într-un mod care să permită autorităților publice un anumit grad de flexibilitate, cel puțin pentru a asigura gestionarea și funcționarea corespunzătoare a acestora, la fel cum este interpretat Regulamentul (CE) nr. 45/2001 în prezent.

În mod alternativ, ultima teză menționată de la articolul 6 alineatul (1) litera (f) din propunerea de regulament ar putea fi interpretată într-un mod care să nu excludă complet posibilitatea ca autoritățile publice să utilizeze interesul legitim ca temei juridic. În acest caz, formularea „prelucrarea efectuată de către autoritățile publice în îndeplinirea sarcinilor care le revin” de la articolul 6 alineatul (1) litera (f), astfel cum s-a propus, ar trebui să fie interpretată în mod restrictiv. Interpretarea restrictivă ar însemna că prelucrarea de către autoritățile publice pentru o bună gestionare și funcționare a acestora nu se încadrează în domeniul de aplicare a „prelucrării efectuate de către autoritățile publice în îndeplinirea sarcinilor care le revin”. Prin urmare, prelucrarea de către autoritățile publice pentru o bună gestionare și funcționare a acestora ar putea fi posibilă în continuare în baza temeiului interesului legitim.

III.3. Articolul 7 litera (f): interesul legitim

Articolul 7 litera (f)[47] impune un test comparativ: interesul legitim al operatorului (sau al terților) trebuie să fie pusă în balanță cu interesul sau drepturile și libertățile fundamentale ale persoanei vizate. Rezultatul testului comparativ stabilește în mare măsură dacă articolul 7 litera (f) poate fi invocat ca temei juridic pentru prelucrare.

Trebuie menționat deja în această etapă că nu este vorba despre un test comparativ facil, care ar consta pur și simplu în cântărirea a două „ponderi” ușor cuantificabile și ușor comparabile una cu cealaltă. Mai degrabă, astfel cum se va descrie în detaliu în cele ce urmează, efectuarea testului comparativ poate necesita o evaluare complexă, care ia în considerare o serie de factori. Pentru a facilita structurarea și simplificarea evaluării, am defalcat procesul în mai multe etape pentru a contribui la asigurarea faptului că testul comparativ poate fi efectuat în mod eficace.

Secțiunea III.3.1 examinează mai întâi o parte a comparației: ce anume constituie „interesul legitim urmărit de operator sau de terțul căruia îi sunt comunicate datele”. În secțiunea III.3.2, se examinează cealaltă parte a comparației, alcătuită din „interesul sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecție în temeiul articolului 1 alineatul (1)”.

În secțiunile III.3.3 și III.3.4, se furnizează orientări cu privire la modul de desfășurare a testului comparativ. Secțiunea III.3.3 oferă o introducere generală utilizând trei scenarii diferite. După această introducere, secțiunea III.3.4 prezintă cele mai importante aspecte care trebuie luate în considerare la efectuarea testului comparativ, inclusiv garanțiile și măsurile prevăzute de operatorul de date.

[47] Pentru textul integral al articolului 7 litera (f), a se vedea pagina 4 de mai sus.

La final, în secțiunile III.3.5 și III.3.6 vom examina, de asemenea, anumite mecanisme specifice, cum ar fi răspunderea, transparența și dreptul de opoziție, care pot contribui la asigurarea – și la susținerea în continuare – a unui echilibru între diferitele interese care ar putea fi implicate.

III.3.1. Interesul legitim al operatorului (sau al terților)

Conceptul de „interes”

Conceptul de „interes” este strâns legat, dar diferit de noțiunea de „scop” menționată la articolul 6 din directivă. În discursul privind protecția datelor, „scopul” este motivul specific pentru care datele sunt prelucrate: scopul sau intenția prelucrării datelor. Spre deosebire de acesta, un interes este cauza mai amplă pe care un operator o poate avea pentru prelucrare sau avantajul pe care operatorul îl obține – sau pe care societatea l-ar putea obține – în urma prelucrării.

De exemplu, o întreprindere poate avea un *interes* în asigurarea sănătății și securității personalului său care lucrează la centrala sa nucleară. În acest sens, întreprinderea poate avea ca *scop* punerea în aplicare a unor proceduri specifice de control al accesului care justifică prelucrarea anumitor date cu caracter personal specificate, în scopul de a garanta sănătatea și securitatea personalului.

Un interes trebuie să fie articulat suficient de clar pentru a permite efectuarea testului comparativ în raport cu interesul și drepturile fundamentale ale persoanei vizate. În plus, interesul în discuție trebuie, de asemenea, să fie „urmărit de operator”. Acest lucru necesită un interes real și actual, care corespunde activităților curente sau beneficiilor preconizate în viitorul foarte apropiat. Cu alte cuvinte, interesele care sunt prea vagi sau speculative nu vor fi suficiente.

Natura interesului poate varia. Unele interese pot fi imperioase și benefice pentru societate, în sens larg, cum ar fi interesul presei de a publica informații cu privire la corupția în cadrul guvernului sau interesul în efectuarea de cercetări științifice (sub rezerva unor garanții adecvate). Alte interese pot fi mai puțin stringente pentru societate în ansamblu sau, în orice caz, impactul urmăririi acestora asupra societății poate fi mai complex sau controversat. Aceasta se poate aplica, de exemplu, interesului economic al unei întreprinderi în a afla cât mai multe informații posibil cu privire la potențialii clienți, astfel încât să direcționeze mai bine publicitatea pentru produsele sau serviciile sale.

Ce determină caracterul „legitim” sau „nelegitim” al unui interes?

Obiectivul acestei întrebări constă în identificarea pragului a ceea ce constituie un interes legitim. În cazul în care interesul operatorului de date este nelegitim, testul comparativ nu va intra în discuție deoarece nu va fi fost atins pragul inițial pentru utilizarea articolului 7 litera (f).

În opinia grupului de lucru, conceptul de interes legitim ar putea include o gamă largă de interese, fie ele minore sau imperioase, clare sau mai controversate. Ulterior, într-o a doua etapă, atunci când vine vorba despre asigurarea unui echilibru între astfel de interese și

interesele și drepturile fundamentale ale persoanelor vizate, ar trebui să se adopte o abordare mai restrânsă și o analiză mai substanțială.

Următoarea este o listă neexhaustivă cu unele dintre cele mai comune situații în care poate surveni chestiunea interesului legitim în sensul articolului 7 litera (f). Aceasta este prezentată aici fără a aduce atingere faptului dacă interesul operatorului va prevala în cele din urmă față de interesul și drepturile persoanelor vizate atunci când se realizează testul comparativ:

- exercitarea dreptului la libertatea de exprimare și de informare, inclusiv în mass-media și artă;
- marketingul direct convențional și alte forme de marketing sau publicitate;
- mesajele necomerciale nesolicitate, inclusiv pentru campaniile politice sau strângerea de fonduri în scopuri caritabile;
- executarea drepturilor legale, inclusiv recuperarea datoriilor prin proceduri necontencioase;
- prevenirea fraudei, a utilizării abuzive a serviciilor sau a spălării de bani;
- monitorizarea angajaților în scopuri de siguranță sau de gestionare;
- sistemele de informare;
- securitatea fizică, securitatea informatică și a rețelelor;
- prelucrarea în scopuri istorice, științifice și statistice;
- prelucrarea în scopuri de cercetare (inclusiv studii de marketing).

În consecință, interesul poate fi considerat ca fiind legitim atât timp cât operatorul îl poate urmări într-un mod care este în conformitate cu legislația privind protecția datelor, precum și cu alte legi. Cu alte cuvinte, un interes legitim trebuie să fie „acceptabil în conformitate cu legea”[48].

Prin urmare, pentru a fi relevant în temeiul articolului 7 litera (f), un „interes legitim” trebuie:

- să fie legal (și anume, în conformitate cu dreptul UE și legislația națională aplicabilă);
- să fie suficient de clar articulat pentru a permite efectuarea testului comparativ în raport cu interesul și drepturile fundamentale ale persoanei vizate (și anume, suficient de specific);
- să reprezinte un interes real și actual (și anume, să nu fie speculativ).

[48] Observațiile cu privire la natura „legitimității” din secțiunea III.1.3 din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9 de mai sus) se aplică, de asemenea, în cazul de față *mutatis mutandis*. La fel precum în avizul respectiv, la paginile 19-20, „noțiunea de „lege” este utilizată în acest caz în sensul cel mai larg. Aceasta include alte legi aplicabile, cum ar fi dreptul muncii, dreptul contractual sau legislația în materie de protecție a consumatorilor. În plus, noțiunea de lege „include toate formele de drept scris și de drept comun, legislația primară și secundară, decretele municipale, precedentele judiciare, principiile constituționale, drepturile fundamentale, alte principii juridice, precum și jurisprudența, ca atare „legea” ar fi interpretată și luată în considerare de către instanțele competente. În limitele legii, alte elemente, cum ar fi vama, codurile de conduită, codurile de etică, dispozițiile contractuale, precum și contextul general și faptele cauzei, pot fi, de asemenea, luate în considerare atunci când se stabilește dacă un anumit scop este legitim. Aceasta va include natura relației de bază dintre operator și persoanele vizate, fie ea comercială sau de altă natură”. De asemenea, ceea ce poate fi considerat ca fiind un interes legitim „poate, de asemenea, varia în timp, în funcție de evoluțiile științifice și tehnologice și schimbările care au loc în societate și atitudinile culturale”.

Faptul că operatorul are un interes legitim în ceea ce privește prelucrarea anumitor date nu înseamnă că acesta se poate baza în mod necesar pe articolul 7 litera (f) ca temei juridic pentru prelucrare. Legitimitatea interesului operatorului de date este doar un punct de plecare, reprezentând unul dintre elementele care trebuie să fie analizate în temeiul articolului 7 litera (f). Posibilitatea ca articolul 7 litera (f) să constituie temeiul prelucrării va depinde de rezultatul testului comparativ care urmează.

Pentru ilustrare: operatorii pot avea un interes legitim să cunoască preferințele clienților lor, astfel încât să aibă posibilitatea să își personalizeze mai bine ofertele și, în cele din urmă, să ofere produse și servicii care să răspundă mai bine nevoilor și dorințelor consumatorilor. În acest context, articolul 7 litera (f) poate constitui un temei juridic adecvat pentru a fi utilizat pentru anumite tipuri de activități de marketing, online și offline, cu condiția instituirii de garanții adecvate [inclusiv, printre altele, un mecanism care să permită contestarea unei asemenea prelucrări în conformitate cu articolul 14 litera (b), astfel cum se va arăta în secțiunea III.3.6, *Dreptul de opoziție și dincolo de acesta*].

Cu toate acestea, acest lucru nu înseamnă că operatorii vor putea să se bazeze pe articolul 7 litera (f) pentru a monitoriza în mod nejustificat activitățile online sau offline ale clienților lor, să combine volume mari de date despre aceștia din diferite surse care au fost colectate inițial în alte contexte și în scopuri diferite și să creeze – precum și, de exemplu, prin intermediul brokerilor de date, să comercializeze – profiluri complexe ale personalităților și preferințelor clienților fără știrea acestora, în absența unui mecanism de opoziție viabil, ca să nu mai vorbim de lipsa consimțământului în cunoștință de cauză. O astfel de activitate de creare de profiluri este posibil să constituie o intruziune semnificativă în viața privată a clientului și, într-un astfel de caz, interesul și drepturile persoanei vizate prevalează asupra interesului operatorului[49].

Pentru a oferi un alt exemplu, în avizul său privind SWIFT[50], deși grupul de lucru a recunoscut interesul legitim al întreprinderii de a se conforma citațiilor emise în temeiul legislației Statelor Unite pentru a evita riscul de a fi sancționată de către autoritățile americane, acesta a concluzionat că articolul 7 litera (f) nu ar putea fi invocat. Grupul de lucru a considerat, în special, că, din cauza efectelor extinse ale prelucrării datelor asupra persoanelor într-o manieră „ascunsă, sistematică, masivă și pe termen lung”, „interesul sau drepturile și libertățile fundamentale ale numeroaselor persoane vizate prevalează asupra interesului SWIFT de a nu fi sancționat de SUA pentru eventuala nerespectare a citațiilor”.

Astfel cum se va explica în continuare, în cazul în care interesul urmărit de operator nu este imperios, interesul și drepturile persoanei vizate sunt mai susceptibile să prevaleze asupra interesului legitim – dar mai puțin semnificativ – al operatorului. În același timp, acest lucru nu înseamnă că interesele mai puțin imperioase ale operatorului nu pot uneori prevala asupra intereselor și drepturilor persoanelor vizate: de regulă, acest lucru se întâmplă atunci când impactul prelucrării asupra persoanelor vizate este, de asemenea, mai puțin semnificativ.

[49] Aspectul tehnologiilor de urmărire și rolul consimțământului în temeiul articolului 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic vor fi discutate separat. A se vedea secțiunea III.3.6(b) din capitolul „Ilustrare: evoluția abordării marketingului direct”.

[50] A se vedea secțiunea 4.2.3 din avizul deja citat la nota de subsol 39 de mai sus. Interesul legitim al operatorului în acest caz a fost, de asemenea, legat de interesul public al unui terț, care nu a putut fi luat în considerare în conformitate cu Directiva 95/46/CE.

Interesul legitim în sectorul public

Textul actual al directivei nu exclude în mod expres operatorii care sunt autorități publice de la prelucrarea datelor cu utilizarea articolului 7 litera (f) ca temei juridic pentru prelucrare[51].

Cu toate acestea, propunerea de regulament[52] exclude posibilitatea „prelucrării efectuate de către autoritățile publice în îndeplinirea misiunii lor".

Propunerea de modificare legislativă subliniază importanța principiului general conform căruia autoritățile publice, de regulă, ar trebui să prelucreze date în îndeplinirea sarcinilor lor dacă au o autorizație corespunzătoare prin lege să facă acest lucru. Aderarea la acest principiu este deosebit de importantă – și prevăzută în mod clar de jurisprudența Curții Europene a Drepturilor Omului – în cazul în care viața privată a persoanelor vizate este în joc și activitățile autorității publice ar afecta viața privată.

Prin urmare, este necesară o autorizație prin lege suficient de *detaliată și specifică* – de asemenea în conformitate cu directiva actuală – în cazul în care prelucrarea de către autoritățile publice interferează cu viața privată a persoanelor vizate. Aceasta poate lua forma unei obligații legale specifice de a prelucra datele, care poate îndeplini cerințele de la articolul 7 litera (c), sau a unei autorizații specifice (dar nu neapărat o obligație) de a prelucra date, care poate îndeplini cerințele de la articolul 7 literele (e) sau (f)[53].

Interesul legitim al terților

Textul actual al directivei nu se referă numai la „interesul legitim urmărit de operator", ci permite, de asemenea, utilizarea articolului 7 litera (f) atunci când interesul legitim este urmărit „de unul sau mai mulți terți cărora le sunt comunicate datele"[54]. Următoarele exemple ilustrează o serie de contexte în care se poate aplica această dispoziție.

Publicarea datelor în scopul transparenței și al răspunderii. Un context important în care articolul 7 litera (f) poate fi relevant este cazul publicării datelor în scopul transparenței și al răspunderii (de exemplu, remunerațiile personalului administrativ de conducere dintr-o întreprindere). În acest caz, se poate considera că divulgarea publică se realizează, în

[51] Inițial, prima propunere a Comisiei privind directiva reglementa separat prelucrarea datelor din sectorul privat și activitățile de prelucrare din sectorul public. Distincția formală dintre normele aplicabile sectorului public și sectorului privat a fost abandonată în propunerea modificată. Acest lucru ar fi putut conduce, de asemenea, la diferențe de interpretare și de punere în aplicare de către statele membre.

[52] A se vedea articolul 6 alineatul (1) litera (f) din propunerea de regulament.

[53] În acest sens, a se vedea, de asemenea, secțiunea III.2.5 de mai sus privind sarcinile publice (paginile 21-23), precum și discuțiile de mai jos din capitolul *Interesele legitime ale terților* (la paginile 27-28). A se vedea, de asemenea, reflecțiile privind limitele „executării private" a legislației la pagina 35, în capitolul „Interesele publice/interesele comunității mai largi". În toate aceste situații, este deosebit de important să se asigure că limitele articolului 7 litera (f), precum și ale articolului 7 litera (e) sunt pe deplin respectate.

[54] Propunerea de regulament vizează limitarea utilizării temeiului în cauză la „interesul legitim urmărit de operatorul de date". Nu reiese clar doar din textul propus dacă limbajul propus înseamnă doar o simplificare a textului sau dacă intenția este de a exclude situațiile în care un operator ar putea divulga date în interesul legitim al altora. Cu toate acestea, textul nu este definitiv. Interesul terților a fost reintrodus, de exemplu, în versiunea finală a raportului Comisiei LIBE cu ocazia votului privind amendamentele de compromis în Comisia LIBE a Parlamentului European la 21 octombrie 2013. A se vedea, în acest sens, amendamentul 100 la articolul 6. Reintroducerea terților în propunere este sprijinită de grupul de lucru pe motiv că utilizarea sa poate continua să fie adecvată în anumite situații, inclusiv cele descrise mai jos.

principal, nu în interesul operatorului care publică date, ci în interesul altor părți interesate, precum angajații sau jurnaliștii sau publicul larg, cărora le sunt divulgate datele.

Din perspectiva protecției datelor cu caracter personal și a vieții private și pentru a asigura certitudinea juridică în general, se recomandă ca datele cu caracter personal să fie făcute publice pe baza unei legi care permite și – atunci când este cazul – specifică în mod clar datele care urmează să fie publicate, scopul publicării și orice alte garanții necesare[55]. Aceasta înseamnă, de asemenea, că ar putea fi de preferat să se utilizeze ca temei juridic articolul 7 litera (c), mai degrabă decât articolul 7 litera (f) atunci când datele cu caracter personal sunt comunicate în scopul transparenței și al răspunderii[56].

Cu toate acestea, în absența unei permisiuni sau a unei obligații legale specifice de a publica date, ar fi totuși posibil să se divulge date cu caracter personal către părți interesate relevante. În cazurile adecvate, ar fi posibil, de asemenea, să se publice date cu caracter personal din motive de transparență și răspundere.

În ambele cazuri – și anume, indiferent dacă datele cu caracter personal sunt comunicate sau nu pe baza unei legi care permite acest lucru – divulgarea depinde în mod direct de rezultatul testului comparativ menționat la articolul 7 litera (f) și de punerea în aplicare a garanțiilor și a măsurilor corespunzătoare[57].

De asemenea, utilizarea ulterioară pentru o mai mare transparență a datelor cu caracter personal deja publicate [de exemplu, republicarea datelor de către presă sau difuzarea ulterioară a datelor publicate inițial într-un mod mai inovator sau mai ușor accesibil prin intermediul unei organizații neguvernamentale (ONG)], poate fi, de asemenea, de dorit. Posibilitatea unei astfel de republicări și reutilizări va depinde de rezultatul testului comparativ, care ar trebui să ia în considerare, printre altele, natura informațiilor și efectul republicării sau reutilizării asupra persoanelor vizate[58].

---

[55] Această recomandare de bună practică nu ar trebui să aducă atingere normelor juridice naționale privind transparența și accesul public la documente.

[56] Într-adevăr, în unele state membre trebuie să fie respectate norme diferite în ceea ce privește prelucrarea efectuată de participanții din sectoarele public și privat. De exemplu, conform Codului italian pentru protecția datelor, comunicarea datelor cu caracter personal de către un organism public este permisă numai în cazul în care aceasta este prevăzută de o lege sau o reglementare (secțiunea 19.3).

[57] Astfel cum s-a explicat în Avizul nr. 6/2013 al grupului de lucru privind datele deschise (a se vedea pagina 9 din aviz, citată la nota de subsol 88 de mai jos), „orice practică națională sau legislație națională privind transparența trebuie să respecte articolul 8 din Convenția europeană a drepturilor omului și articolele 7 și 8 din Carta drepturilor fundamentale a UE. Acest lucru implică, astfel cum a stabilit Curtea Europeană de Justiție în hotărârile în cauzele *Österreichischer Rundfunk* și *Schecke*, că trebuie să se verifice dacă divulgarea este necesară și proporțională cu obiectivul legitim urmărit de lege". A se vedea hotărârea Curții Europene de Justiție din 20 mai 2003, Rundfunk, cauzele conexate C-465/00, C-138/01 și C-139/01 și hotărârea Curții Europene de Justiție din 9 noiembrie 2010, Volker und Markus Schecke, cauzele conexate C-92/09 și C-93/09.

[58] Limitarea scopului este, de asemenea, un element important în acest context. La pagina 19 din Avizul nr. 6/2013 al grupului de lucru privind datele deschise (citat la nota de subsol 88 de mai jos), WP29 recomandă „ca orice legislație care solicită accesul public la date să specifice în mod clar scopul pentru dezvăluirea datelor cu caracter personal. Dacă acest lucru nu se întâmplă sau se efectuează numai în termeni generali și vagi, securitatea juridică și previzibilitatea vor avea de suferit. În special, în ceea ce privește orice solicitări de reutilizare, se dovedește a fi foarte dificil pentru organismul din sectorul public și potențialii reutilizatori în cauză să stabilească care a fost scopul inițial al publicării și, ulterior, ce alte scopuri ar fi compatibile cu aceste scopuri. Așa cum s-a menționat deja, chiar și în cazul în care datele cu caracter personal sunt publicate pe internet, nu trebuie să se presupună că acestea pot fi prelucrate în orice scopuri".

Cercetarea istorică sau alte tipuri de cercetare științifică. Un alt context important în care divulgarea pentru realizarea interesului legitim al terților ar putea fi relevantă este cercetarea istorică sau alte tipuri de cercetare științifică, în special în cazul în care se solicită accesul la anumite baze de date. Directiva prevede recunoașterea specifică a unor astfel de activități, sub rezerva unor garanții și măsuri adecvate[59], însă trebuie ținut cont că temeiul legitim pentru activitățile respective va fi adesea o utilizare bine gândită a articolului 7 litera (f)[60].

Interesul publicului larg sau interesul unui terț. În fine, interesul legitim al terților poate, de asemenea, să fie relevant în mod diferit. Acesta este cazul atunci când un operator – uneori încurajat de autoritățile publice – urmărește un interes care corespunde unui interes public general sau unui interes al unui terț. Aceasta poate include situațiile în care un operator depășește obligațiile legale specifice stabilite în legi și reglementări în scopul de a sprijini aplicarea legii pentru a asista organele de aplicare a legii sau părți interesate private în eforturile lor de combatere a activităților ilegale, cum ar fi spălarea de bani, ademenirea copiilor în scopuri sexuale sau partajarea ilegală de fișiere online. Cu toate acestea, în astfel de situații, este deosebit de important să se asigure că limitele articolului 7 litera (f) sunt pe deplin respectate[61].

Prelucrarea trebuie să fie necesară pentru scopul (scopurile) preconizat(e)

În sfârșit, prelucrarea datelor cu caracter personal trebuie, de asemenea, să fie „necesară pentru realizarea interesului legitim" urmărit fie de operator, fie – în cazul divulgării – de către terț. Această condiție completează cerința necesității în temeiul articolului 6 și impune o legătură între prelucrare și interesele urmărite. Cerința „necesității" se aplică în toate situațiile menționate la articolul 7 literele (b)-(f), dar este relevantă în special în cazul prevăzut la litera (f) pentru a se asigura că prelucrarea datelor în temeiul interesului legitim nu va conduce la o interpretare nejustificat de largă a necesității de a prelucra date. La fel precum în alte cazuri, acest lucru înseamnă că ar trebui să se analizeze dacă sunt disponibile alte mijloace mai puțin invazive pentru a servi aceluiași scop.

III.3.2. Interesul sau drepturile persoanei vizate

Interesul <u>sau</u> drepturile (și nu interesul <u>pentru</u> drepturile)

Articolul 7 litera (f) din directivă se referă la „interesul <u>pentru</u> drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecție în temeiul articolului 1 alineatul (1)".

[59] A se vedea, de exemplu, articolul 6 alineatul (1) literele (b) și (e).

[60] Astfel cum s-a explicat în Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9 de mai sus), utilizarea ulterioară a datelor în scopuri secundare ar trebui să facă obiectul unui test dublu. În primul rând, ar trebui să se garanteze faptul că datele vor fi utilizate în scopuri compatibile. În al doilea rând, ar trebui să se asigure că va exista un temei juridic corespunzător pentru prelucrarea datelor în temeiul articolului 7.

[61] A se vedea în acest sens, de exemplu, documentul de lucru privind aspectele de protecție a datelor legate de drepturile de proprietate intelectuală, adoptat în 18.1.2005 (WP104).

Cu toate acestea, grupul de lucru a remarcat, atunci când a comparat diferitele versiuni lingvistice ale directivei, că expresia „interesul pentru” a fost tradusă ca „interesul sau” în alte limbi-cheie care au fost utilizate la momentul negocierii textului[62].

Analiza suplimentară sugerează că formularea în limba engleză a directivei este pur și simplu rezultatul unei greșeli de tipar: „or” (sau) a fost scris în mod eronat „for” (pentru)[63]. Prin urmare, textul corect ar trebui să aibă forma „interesul sau drepturile și libertățile fundamentale”.

„Interesul” și „drepturile” ar trebui să beneficieze de o interpretare în sens larg

Trimiterea la „interesul sau drepturile și libertățile fundamentale” are un impact direct asupra domeniului de aplicare a dispoziției. Aceasta oferă un grad mai mare de protecție pentru persoana vizată, impunând luarea în considerare, de asemenea, a „interesului” persoanelor vizate, nu numai a drepturilor și libertăților fundamentale ale acestora. Cu toate acestea, nu există niciun motiv să se presupună că limitarea din articolul 7 litera (f) la drepturile fundamentale „care necesită protecție în temeiul articolului 1 alineatul (1)” – și, prin urmare, referirea explicită la obiectul directivei[64] – nu se aplică, de asemenea, noțiunii de „interes”. Cu toate acestea, reiese în mod clar că ar trebui să fie luate în considerare toate interesele relevante ale persoanei vizate.

Această interpretare a textului este justificată nu numai din punct de vedere gramatical, ci și atunci când se ține seama de interpretarea în sens larg a noțiunii de „interes legitim” al operatorului. În cazul în care operatorul – sau terțul, în cazul divulgării – poate urmări orice interes, cu condiția ca acesta să nu fie nelegitim, persoana vizată ar trebui, de asemenea, să aibă dreptul ca toate categoriile de interese să fie luate în considerare și să fie comparate cu cele ale operatorului, în măsura în care acestea sunt relevante în cadrul domeniului de aplicare a directivei.

Într-o perioadă de creștere a dezechilibrului în ceea ce privește „puterea informațională”, când atât guvernele, cât și organizațiile de afaceri obțin cantități de date fără precedent până în prezent referitoare la persoane și sunt din ce în ce mai în măsură să elaboreze profiluri detaliate care să le anticipeze comportamentul (consolidând dezechilibrul informațional și reducând autonomia acestora), este din ce în ce mai important să se asigure protecția interesului persoanelor de a-și păstra viața privată și autonomia.

---

[62] De exemplu, „l'intérêt ou les droits et libertés fondamentaux de la personne concernée” în limba franceză, „l'interesse o i diritti e le libertà fondamentali della persona interessata” în limba italiană; „das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person” în limba germană.

[63] Grupul de lucru constată că versiunea în limba engleză corectă punct de vedere gramatical ar fi trebuit să aibă forma „interesul în” mai degrabă decât „interesul pentru”, dacă acesta este sensul intenționat. În plus, expresia „interesul pentru” sau „interesul în” pare a fi inutilă, în primul rând, deoarece referirea la „drepturile și libertățile fundamentale, în mod normal, ar fi fost suficientă, dacă acesta era sensul intenționat. Interpretarea conform căreia a existat o greșeală de tehnoredactare este confirmată, de asemenea, de faptul că Poziția comună (CE) nr. 1/95 adoptată de Consiliu la 20 februarie 1995 se referă, de asemenea, la „interesul sau drepturile și libertățile fundamentale”. În cele din urmă, grupul de lucru observă, de asemenea, intenția Comisiei de a corecta greșeală de tehnoredactare în propunerea de regulament: articolul 6 alineatul (1) litera (f) se referă la „interesul sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal” și nu „interesul pentru” astfel de drepturi.

[64] A se vedea articolul 1 alineatul (1): „Statele membre asigură, în conformitate cu prezenta directivă, protejarea drepturilor și libertăților fundamentale ale persoanei și în special a dreptului la viața privată în ceea ce privește prelucrarea datelor cu caracter personal”.

În cele din urmă, este important de remarcat faptul că, spre deosebire de cazul interesului operatorului, adjectivul „legitim” nu este utilizat aici pentru a determina termenul „interes” al persoanei vizate. Acest lucru implică un domeniu de aplicare mai larg pentru protecția intereselor și drepturilor persoanelor vizate. Inclusiv persoanele angajate în activități ilegale nu ar trebui să facă obiectul unui amestec disproporționat în drepturile și interesele lor[65]. De exemplu, interesul unei persoane care este posibil să fi comis de furt într-un supermarket ar putea încă să prevaleze asupra publicării fotografiei sale și a adresei private pe pereții supermarket-ului și/sau pe internet de către proprietarul magazinului.

III.3.3. Introducere la aplicarea testului comparativ

Este util să ne imaginăm atât interesele legitime ale operatorului, cât și impactul asupra intereselor și drepturilor persoanei vizate, sub forma unui spectru. Interesele legitime pot varia de la interese nesemnificative la interese relativ importante până la interese imperioase. De asemenea, impactul asupra intereselor și drepturilor persoanelor vizate poate fi mai mult sau mai puțin semnificativ și poate varia de la minor la foarte grav.

Interesele legitime ale operatorului, atunci când sunt minore și nu foarte imperioase, pot, în general, să prevaleze asupra intereselor și drepturilor persoanelor vizate numai atunci când impactul lor asupra respectivelor drepturi și interese este chiar mai nesemnificativ. Dimpotrivă, interesele legitime imperioase și importante pot justifica, în unele cazuri și sub rezerva unor garanții și măsuri, o intruziune chiar semnificativă în viața privată sau un alt impact semnificativ asupra intereselor sau drepturilor persoanelor vizate[66].

În acest context, este important de subliniat rolul special pe care îl pot juca garanțiile[67] în reducerea impactului nejustificat asupra persoanelor vizate, modificând astfel echilibrul dintre drepturi și interese în măsura în care acestea nu vor prevala asupra intereselor legitime ale operatorului de date. Utilizarea garanțiilor nu este suficientă în sine pentru a justifica orice tip de prelucrare în toate contextele. De asemenea, garanțiile respective trebuie să fie adecvate și suficiente și trebuie să reducă fără îndoială și în mod semnificativ impactul asupra persoanelor vizate.

---

[65] Desigur, una dintre consecințele criminalității ar putea fi colectarea și posibila publicare a datelor cu caracter personal cu privire la infractori și persoanele suspectate. Cu toate acestea, astfel de acțiuni trebuie să facă obiectul unor condiții și garanții stricte.

[66] Ca o exemplificare, a se vedea raționamentul grupului de lucru în mai multe avize și documente de lucru:
- Avizul nr. 4/2006 privind comunicarea referitoare la o propunere de reglementare de către Departamentul Sănătății și Serviciilor Sociale privind controlul bolilor transmisibile și colectarea de informații privind pasagerii din 20 noiembrie 2005 (Controlul bolilor transmisibile propus în temeiul CFR 42 Partea 70 și Partea 71), adoptat la 14.6.2006 (WP 121), unde sunt în joc amenințări grave specifice la adresa sănătății publice.
- Avizul nr. 1/2006 privind sistemele de informare (citat la nota de subsol 39), în cazul în care gravitatea presupusei infracțiuni este unul dintre elementele testului comparativ.
- Documentul de lucru privind supravegherea comunicațiilor electronice la locul de muncă, adoptat la 29.5.2002 (WP 55), care realizează un echilibru între dreptul angajatorului de a-și desfășura activitatea în mod eficient și demnitatea umană a lucrătorului, precum și secretul corespondenței.

[67] Garanțiile pot include, printre altele, limite stricte cu privire la măsura în care datele sunt colectate, ștergerea imediată a datelor după utilizare, măsuri tehnice și organizatorice menite să asigure separarea funcțională, utilizarea adecvată a tehnicilor de anonimizare, agregarea datelor și tehnologiile menite să sporească protecția vieții private, dar și sporirea transparenței, a responsabilității și posibilitatea excluderii voluntare („opt-out”) de la prelucrare. A se vedea, de asemenea, secțiunea III.3.4 litera (d) și în continuare.

Scenarii introductive

Înainte de a trece la furnizarea de orientări privind modul de efectuare a testului comparativ, următoarele trei scenarii introductive pot oferi o primă ilustrare a modului în care se poate realiza asigurarea unui echilibru între interese și drepturi în viața reală. Toate cele trei exemple se bazează pe un scenariu simplu și inofensiv care începe cu o ofertă specială pentru livrarea de produse alimentare italiene. Exemplele introduc treptat noi elemente care arată modul în care echilibrul este afectat pe măsură ce crește impactul asupra persoanelor vizate.

Scenariul 1: Ofertă specială a unui lanț de pizzerii

Claudia comandă o pizza cu ajutorul unei aplicații mobile de pe telefonul ei inteligent, dar nu bifează opțiunea de excludere de la comercializarea pe internet. Detaliile privind adresa și cardul său de credit sunt stocate pentru livrare. Câteva zile mai târziu, Claudia primește cupoane de reducere pentru produse similare provenind de la lanțul de pizzerii în cutia sa poștală de la domiciliu.

Analiză succintă: Lanțul de pizzerii are un interes legitim, dar nu deosebit de imperios, în a încerca să vândă clienților săi o mai mare cantitate din produsele sale. Pe de altă parte, nu pare să existe nicio intruziune importantă în viața privată a Claudiei sau orice alt impact nejustificat asupra drepturilor și intereselor sale. Datele și contextul sunt relativ inofensive (consumul de pizza). Lanțul de pizzerii a stabilit anumite garanții: se utilizează doar o serie relativ mică de informații (datele de contact) și cupoanele sunt trimise prin poșta tradițională. De asemenea, se oferă o opțiune ușor de utilizat de excludere voluntară de la comercializarea pe internet.

În concluzie și având în vedere, de asemenea, garanțiile și măsurile existente (inclusiv un instrument de excludere voluntară ușor de utilizat), interesul și drepturile persoanei vizate nu par să prevaleze asupra interesului legitim al lanțului de pizzerii de a efectua o astfel de prelucrare a unui număr minim de date.

Scenariul 2: Publicitate selectivă pentru aceeași ofertă specială

Contextul este același, însă de această dată lanțul de pizzerii stochează nu numai adresa și detaliile cardului de credit al Claudiei, ci și istoricul recent al comenzilor sale (din ultimii trei ani). De asemenea, istoricul achizițiilor este combinat cu datele de la supermarket-ul unde Claudia își face cumpărăturile online, care este administrat de aceeași întreprindere ca și cea care administrează lanțul de pizzerii. Claudia primește de la lanțul de pizzerii oferte speciale de pizza și publicitate selectivă pe baza istoricului ei de comenzi pentru cele două servicii diferite. Aceasta primește reclame și oferte speciale atât online, cât și offline, prin poșta obișnuită, e-mail și plasarea pe site-ul web al întreprinderii, precum și pe site-urile web ale unei anumit număr de parteneri (atunci când accesează site-urile respective pe calculator sau pe telefonul mobil). De asemenea, istoricul său de navigare este monitorizat (click-stream). Datele privind locul în care se află sunt, de asemenea, urmărite prin intermediul telefonului mobil. Datele sunt introduse într-un software de analiză, care prevede preferințele Claudiei, precum și momentele și locațiile când aceasta este cel mai probabil să facă o achiziție mai mare, este dispusă să plătească un preț mai mare, este susceptibilă a fi influențată de o anumită reducere a prețurilor sau când îi este poftă cel mai mult de deserturile sau preparatele preferate[68]. Claudia este foarte iritată de anunțurile publicitare persistente, care apar pe telefonul mobil atunci când verifică orarul autobuzelor în drum spre casă și care fac publicitate celor mai recente oferte de alimente la pachet, de la care încearcă să se abțină. Claudia nu putut găsi informații ușor de folosit sau un mod simplu de a opri anunțurile, deși întreprinderea susține că există un sistem de excludere voluntară în funcțiune. De asemenea, aceasta a fost surprinsă să constate că, atunci când s-a mutat într-o zonă mai puțin prosperă, nu a mai primit ofertele speciale. Acest lucru a avut ca rezultat o creștere cu aproximativ 10 % a cheltuielilor lunare pentru alimente. Un prieten mai priceput în domeniul informaticii i-a arătat o serie de speculații de pe un blog online conform cărora supermarket-ul taxa mai mult comenzile din cartierele sărace din cauza riscurilor mai ridicate, din punct de vedere statistic, de fraudă legată de cardurile de credit în astfel de cazuri. Întreprinderea nu a comentat și a argumentat că are drepturi exclusive asupra politicii privind reducerile și asupra algoritmului pe care îl utilizează pentru a stabili prețurile, acestea neputând fi dezvăluite.

Analiză succintă: Datele și contextul rămân relativ inofensive. Cu toate acestea, amploarea colectării datelor și a tehnicilor utilizate pentru a o influența pe Claudia (inclusiv diverse tehnici de monitorizare, care oferă predicții privind momentele și locațiile poftelor alimentare și faptul că în momentele respective Claudia este cel mai vulnerabilă să cedeze tentației) sunt factori care trebuie luați în considerare atunci când se evaluează impactul prelucrării datelor. Lipsa de transparență în ceea ce privește logica prelucrării datelor de către întreprindere, care ar fi condus *de facto* la prețuri discriminatorii pe baza locului din care este transmisă o comandă, precum și potențialul impact financiar semnificativ asupra clienților înclină balanța în cele din urmă, chiar și în contextul inofensiv al alimentelor la pachet și al achizițiilor de produse alimentare. În locul oferirii unei simple posibilități de a renunța la acest tip de creare de profiluri și publicitate selectivă, ar fi necesar un consimțământ în cunoștință de cauză, în conformitate cu articolul 7 litera (a), dar și în conformitate cu articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic. În consecință, articolul 7 litera (f) nu ar trebui să fie invocat ca temei juridic pentru prelucrare.

[68] A se vedea, de exemplu, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *Cercetările recente sugerează că voința este o resursă finită care poate fi diminuată sau refăcută*

Scenariul 3: Utilizarea comenzilor de produse alimentare pentru a adapta primele de asigurare de sănătate

Datele despre obiceiurile Claudiei în ceea ce privește consumul de pizza, inclusiv momentul și natura produselor alimentare comandate, sunt vândute de lanțul de pizzerii unei societăți de asigurări, care le utilizează pentru a-și adapta primele de asigurare de sănătate.

Analiză succintă: Societatea de asigurări de sănătate poate avea un interes legitim – în măsura în care legislația aplicabilă permite acest lucru – de a evalua riscurile de sănătate ale clienților săi și de a percepe prime diferențiate în funcție de riscuri diferite. Cu toate acestea, modul în care datele sunt colectate și amploarea colectării de date în sine sunt excesive. Este puțin probabil ca o persoană rezonabilă aflată în situația Claudiei să se aștepte că informațiile despre consumul său de pizza ar putea fi folosite pentru a i se calcula primele de asigurare de sănătate.

Pe lângă caracterul excesiv al creării de profiluri și posibilele deducții incorecte (pizza ar putea fi comandată pentru altcineva), deducerea unor date sensibile (date medicale) din date aparent inofensive (comenzi de alimente la pachet) contribuie la înclinarea balanței în favoarea interesului și drepturilor persoanei vizate. În sfârșit, prelucrarea are, de asemenea, un impact financiar semnificativ asupra persoanei vizate.

În concluzie, în acest caz specific, interesul și drepturile persoanei vizate prevalează asupra intereselor legitime ale societății de asigurări de sănătate. În consecință, articolul 7 litera (f) nu ar trebui să fie invocat ca temei juridic pentru prelucrare. De asemenea, este discutabil dacă articolul 7 litera (a) ar putea fi utilizat ca temei juridic, având în vedere amploarea excesivă a colectării de date și, de asemenea, eventual, din cauza unor restricții specifice în temeiul legislației naționale.

Scenariile de mai sus și posibila introducere a unor variații cu alte elemente subliniază necesitatea stabilirii unui număr limitat de factori-cheie care pot contribui la concentrarea evaluării, precum și necesitatea unei abordări pragmatice care să permită utilizarea unor ipoteze practice („reguli generale”), în primul rând pe baza a ceea ce o persoană rezonabilă ar considera acceptabil în circumstanțele date („așteptări rezonabile”) și pe baza consecințelor activității de prelucrare a datelor asupra persoanelor vizate („impact”).

III.3.4. Factorii-cheie care trebuie luați în considerare atunci când se aplică testul comparativ

Statele membre au stabilit o serie de factori utili care trebuie luați în considerare atunci când se efectuează testul comparativ. Factorii sunt discutați în prezenta secțiune în cadrul următoarelor patru capitole principale: (a) evaluarea interesul legitim al operatorului, (b)

în timp [10]. Să ne imaginăm că preocupările cu privire la obezitate determină un consumator să încerce să se abțină de la produsele alimentare nesănătoase preferate. Se dovedește că există momente și locuri în care nu poate să facă acest lucru. Big data (volumele mari de date) ajută comercianții să înțeleagă exact modul și momentul în care să abordeze consumatorul respectiv atunci când este cel mai vulnerabil – în special într-o lume a expunerii constante la ecrane, în care chiar și aparatele noastre sunt capabile să îndemne la cumpărături.”

impactul asupra persoanelor vizate, (c) echilibrul provizoriu și (d) garanțiile suplimentare aplicate de operator pentru a preveni orice impact nejustificat asupra persoanelor vizate[69].

Pentru a efectua testul comparativ, în primul rând, este important să se ia în considerare natura și sursa intereselor legitime, pe de o parte, și impactul asupra persoanelor vizate, pe de altă parte. Această evaluare ar trebui să ia deja în considerare măsurile pe care operatorul intenționează să le adopte pentru a se conforma directivei (de exemplu, pentru a asigura limitarea scopului și proporționalitatea în conformitate cu articolul 6 sau pentru a furniza informații persoanelor vizate în temeiul articolelor 10 și 11).

După analizarea și cântărirea comparativă a celor două părți, se poate stabili un „echilibru" provizoriu. În cazul în care rezultatul evaluării lasă în continuare loc de îndoieli, următorul pas va consta în a evalua dacă garanțiile suplimentare, care oferă o protecție sporită persoanei vizate, pot înclina balanța astfel încât să fie justificată prelucrarea.

(a) Evaluarea interesului legitim al operatorului

Întrucât noțiunea de interes legitim este destul de largă, astfel cum s-a explicat în secțiunea III.3.1 de mai sus, natura acesteia joacă un rol crucial în ceea ce privește punerea în balanță a interesului operatorului în raport cu interesul și drepturile persoanelor vizate. Deși este imposibil să se exprime judecăți de valoare cu privire la toate interesele legitime posibile, pot fi oferite anumite orientări. Astfel cum s-a menționat mai sus, astfel de interese pot varia de la interese minore la interese imperioase și pot fi clare sau mai controversat.

i) Exercitarea unui drept fundamental

Dintre drepturile și libertățile fundamentale consacrate de Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta")[70] și Convenția Europeană a Drepturilor Omului (denumită în continuare „CEDO"), unele pot intra în conflict cu dreptul la viață privată și dreptul la protecția datelor cu caracter personal, cum ar fi libertatea de exprimare și de informare[71], libertatea artelor și științelor[72], dreptul de acces la documente[73], precum și, de exemplu, dreptul la libertate și la siguranță[74], libertatea de gândire, de conștiință și de religie[75], libertatea de a desfășura o activitate comercială[76], dreptul de proprietate[77], dreptul la o cale de atac eficientă și la un proces echitabil[78] sau prezumția de nevinovăție și dreptul la apărare[79].

[69] Datorită importanței acestora, anumite aspecte specifice legate de garanții vor fi discutate în detaliu în sub-secțiuni separate din secțiunile III.3.5 și III.3.6.
[70] Dispozițiile Cartei se adresează instituțiilor și organismelor Uniunii Europene, cu respectarea principiului subsidiarității, precum și autorităților naționale numai în cazul în care acestea pun în aplicare dreptul Uniunii.
[71] Articolul 11 din Cartă și articolul 10 din CEDO.
[72] Articolul 13 din Cartă și articolele 9 și 10 din CEDO.
[73] Articolul 42 din Cartă. „Orice cetățean al Uniunii și orice persoană fizică sau juridică care are reședința sau sediul social într-un stat membru are dreptul de acces la documentele Parlamentului European, Consiliului și Comisiei." Drepturi similare de acces există în mai multe state membre în ceea ce privește documentele deținute de organisme publice din statele membre în cauză.
[74] Articolul 6 din Cartă și articolul 5 din CEDO.
[75] Articolul 10 din Cartă și articolul 9 din CEDO.
[76] Articolul 16 din Cartă.
[77] Articolul 17 din Cartă și articolul 1 din Protocolul nr. 1 la CEDO.
[78] Articolul 47 din Cartă și articolul 6 din CEDO.
[79] Articolul 48 din Cartă și articolele 6 și 13 din CEDO.

Pentru ca interesul legitim al operatorului să prevaleze, prelucrarea datelor trebuie să fie „necesară” și „proporțională” în vederea exercitării dreptului fundamental în cauză.

Pentru ilustrare, în funcție de faptele în speță, ar putea fi necesar și proporțional pentru un ziar să publice anumite informații incriminante despre comportamentul de consumator al unui funcționar de nivel înalt implicat într-un presupus scandal de corupție. Pe de altă parte, nu ar trebui să existe nicio autorizație generală pentru mass-media de publicare a oricăror și tuturor detaliilor irelevante privind viața privată a persoanelor publice. Acestea și alte cazuri similare ridică, de regulă, probleme complexe de evaluare și, pentru a contribui la orientarea evaluării, legislația specifică, jurisprudența, orientările, precum și codurile de conduită și alte standarde formale sau mai puțin formale pot toate să joace, de asemenea, un rol important[80].

După caz, în acest context de asemenea, garanțiile suplimentare pot juca un rol important și pot contribui la stabilirea direcției în care balanța echilibrului – uneori fragil – se va înclina.

ii) Interesul public/interesul comunității mai largi

În unele cazuri, operatorul ar putea să invoce interesul public sau interesul comunității mai largi (indiferent dacă acest lucru este prevăzut sau nu în legile sau reglementările naționale). De exemplu, o organizație caritabilă poate prelucra date cu caracter personal în scopuri de cercetare medicală sau o organizație fără scop lucrativ poate prelucra date în vederea sensibilizării cu privire la corupția în cadrul guvernului.

De asemenea, aceasta poate include cazul în care interesul economic privat al unei întreprinderi coincide cu un interes public, într-o anumită măsură. Acest lucru se poate întâmpla, de exemplu, în ceea ce privește combaterea fraudei financiare sau a altor utilizări frauduloase a unor servicii[81]. Un prestator de servicii poate avea un interes economic legitim în a se asigura că proprii clienți nu vor abuza de serviciu (sau nu vor putea să obțină servicii fără plată) și, în același timp, clienții întreprinderii, contribuabilii, precum și publicul larg au, de asemenea, un interes legitim în a se asigura că activitățile frauduloase sunt descurajate și detectate atunci când se produc.

În general, faptul că un operator acționează nu numai în propriul interes legitim (de exemplu, de afaceri), ci și în interesul comunității mai largi poate oferi mai multă „greutate” interesului respectiv. Cu cât interesul public sau interesul comunității mai largi este mai imperios și cu cât este mai clar recunoscut și așteptat în comunitate și de către persoanele vizate ca operatorul să poată lua măsuri și prelucra datele în vederea realizării interesului respectiv, cu atât mai mult cântărește un astfel de interes legitim.

[80] În ceea ce privește criteriile care trebuie aplicate în cazurile care implică libertatea de exprimare, jurisprudența Curții Europene a Drepturilor Omului oferă, de asemenea, orientări utile. A se vedea, de exemplu, hotărârea CEDO în cauza von Hannover/Germania (nr. 2) din 7 februarie 2012, în special punctele 95-126. De asemenea, trebuie să ia în considerare că articolul 9 din directivă (sub titlul *Prelucrarea datelor cu caracter personal și libertatea de exprimare*) permite statelor membre să „prevadă exonerări și derogări de la [anumite dispoziții din directivă] pentru prelucrarea datelor cu caracter personal efectuată numai în scopuri jurnalistice, artistice sau literare” cu condiția ca acestea să fie „necesare pentru a pune dreptul la viață privată în acord cu normele care reglementează libertatea de exprimare”.

[81] A se vedea, de pildă, „Exemplul 21: Date privind contorizarea inteligentă extrase pentru a detecta utilizarea frauduloasă a energiei” de la pagina 67 din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9).

Cu toate acestea, „aplicarea privată” a legii nu ar trebui să fie utilizată pentru a legitima practici intruzive care, dacă ar fi efectuate de o organizație guvernamentală, ar fi interzise în conformitate cu jurisprudența Curții Europene a Drepturilor Omului pe motiv că activitățile autorității publice ar aduce atingere vieții private a persoanelor vizate, fără a îndeplini condițiile stricte prevăzute la articolul 8 alineatul (2) din CEDO.

iii) Alte interese legitime

În unele cazuri, astfel cum s-a discutat în secțiunea III.2, contextul în care apare un interes legitim se poate apropia de unul dintre contextele în care se pot aplica unele dintre celelalte temeiuri juridice, în special, temeiurile juridice prevăzute la articolul 7 litera (b) (contractul), articolul 7 litera (c) (obligația legală) sau articolul 7 litera (e) (sarcina de interes public). De exemplu, o activitate de prelucrare a datelor ar putea să nu fie neapărat necesară, dar poate fi relevantă pentru executarea unui contract – sau o lege poate doar permite, dar nu impune prelucrarea anumitor date. După cum am văzut, nu este întotdeauna ușor să se stabilească o distincție clară între diferitele temeiuri, dar acest lucru face ca analiza testului comparativ, prevăzut la articolul 7 litera (f), să fie cu atât mai importantă.

Și în acest caz, precum în toate celelalte cazuri posibile care nu au fost menționate până acum, cu cât interesul operatorului este mai imperios și cu cât este mai clar recunoscut și așteptat în comunitatea mai largă ca operatorul să poată lua măsuri și prelucra datele în vederea realizării interesului respectiv, cu atât mai mult cântărește un astfel de interes legitim[82]. Aceasta ne conduce la următorul punct, cu un caracter general.

iv) Recunoașterea juridică și culturală/societală a legitimității interesului

În toate contextele de mai sus, este cu siguranță relevant, de asemenea, dacă dreptul UE sau legislația unui stat membru autorizează în mod specific (chiar dacă nu impune) ca operatorii să ia măsuri în vederea realizării interesului public sau privat în cauză. Existența oricăror orientări neobligatorii, adoptate în mod corespunzător, emise de autoritățile de reglementare, de exemplu, agenții de reglementare, care încurajează operatorii să prelucreze datele în vederea realizării interesului în cauză este, de asemenea, relevantă.

Respectarea oricăror orientări neobligatorii furnizate de autoritățile de protecție a datelor sau de alte organe relevante cu privire la modalitățile de prelucrare a datelor va fi, de asemenea, de natură să contribuie la o evaluare echilibrului în favoarea operatorului. Așteptările culturale și societale, inclusiv atunci când nu sunt reflectate în mod direct în instrumentele legislative sau de reglementare, pot juca, de asemenea, un rol și pot înclina balanța în ambele sensuri.

Cu cât este recunoscut mai explicit în lege, în alte instrumente de reglementare – fie că sunt obligatorii sau nu pentru operator – sau chiar în cultura comunității în general, fără niciun temei juridic specific, că operatorii pot lua măsuri și pot prelucra date în vederea realizării unui interes anume, cu atât mai mult cântărește interesul legitim în cauză[83].

[82] Desigur, evaluarea trebuie să includă, de asemenea, un proces de reflecție asupra posibilelor prejudicii suferite de operator, de terți sau de comunitatea mai largă dacă nu are loc prelucrarea datelor.

[83] Cu toate acestea, un astfel de interes nu poate fi utilizat pentru a legitima practici care violează viața privată, care altfel nu îndeplinesc condițiile prevăzute la articolul 8 alineatul (2) din CEDO.

(b) Impactul asupra persoanelor vizate

De cealaltă parte a balanței, impactul prelucrării datelor asupra interesului sau asupra drepturilor și libertăților fundamentale ale persoanei vizate este un criteriu esențial. Prima subsecțiune de mai jos analizează în termeni generali modul de evaluare a impactului asupra persoanei vizate.

Mai multe elemente pot fi utile în acest sens și sunt analizate în subsecțiunile ulterioare, inclusiv natura datelor cu caracter personal, modul în care sunt prelucrate informațiile, așteptările rezonabile ale persoanelor vizate și statutul operatorului de date și al persoanei vizate. De asemenea, vom discuta pe scurt aspecte referitoare la potențialele surse de risc, care pot conduce la un impact asupra persoanelor în cauză, gravitatea oricăror impacturi asupra persoanelor în cauză și probabilitatea concretizării unor astfel de impacturi.

i) Evaluarea impactului

În evaluarea impactului[84] prelucrării, ar trebui să fie luate în considerare atât consecințele pozitive, cât și cele negative. Acestea pot include posibile viitoare decizii sau acțiuni ale terților și situații în care prelucrarea poate conduce la excluderea sau discriminarea persoanelor, la defăimare sau, în sens general, la situații în care există un risc de a prejudicia reputația, puterea de negociere sau autonomia persoanei vizate.

Pe lângă efectele negative care pot fi prevăzute în mod specific, trebuie să fie luat în considerare, de asemenea, impactul emoțional mai larg, inclusiv iritarea, frica și suferința psihică, care pot rezulta din pierderea controlului din partea unei persoane vizate asupra informațiilor sale cu caracter personal sau din realizarea faptului că acestea au fost sau pot fi utilizate necorespunzător sau periclitate – de exemplu, prin expunerea pe internet. De asemenea, trebuie să se ia în considerare în mod corespunzător efectul descurajator asupra comportamentului protejat, cum ar fi libertatea cercetării sau libertatea de exprimare, care ar putea să rezulte din monitorizarea/urmărirea continuă.

Grupul de lucru subliniază că este esențial să se înțeleagă faptul că un „impact” relevant reprezintă un concept mult mai larg decât prejudiciile sau daunele cauzate uneia sau mai multor persoane vizate. Noțiunea de „impact”, astfel cum este utilizată în prezentul aviz, are în vedere orice consecințe eventuale (potențiale sau efective) ale prelucrării datelor. Din motive de claritate, subliniem, de asemenea, că acest concept nu este legat de noțiunea de încălcare a securității datelor și este mult mai amplu decât efectele care ar putea rezulta din încălcarea securității datelor cu caracter personal. În schimb, noțiunea de impact, astfel cum este utilizată aici, cuprinde diferitele modalități în care o persoană poate fi afectată – în mod pozitiv sau negativ – de prelucrarea datelor sale cu caracter personal[85].

[84] Evaluarea impactului trebuie să fie înțeleasă în contextul articolului 7 litera (f). Cu alte cuvinte, aceasta nu se referă la o „analiză de risc” sau o „evaluare a impactului asupra protecției datelor” în sensul propunerii de regulament (articolele 33 și 34) și al diferitelor amendamente LIBE la acesta. Problema metodologiei care trebuie să fie urmată într-o „analiză de risc” sau o „evaluare a impactului asupra protecției datelor” depășește domeniul de aplicare a prezentului aviz. Pe de altă parte, trebuie să se ia în considerare faptul că – într-un mod sau altul – analiza impactului în conformitate cu articolul 7 litera (f) poate constitui o parte importantă a oricărei „evaluări a riscurilor” sau „evaluări a impactului asupra protecției datelor” și poate contribui, de asemenea, la identificarea situațiilor în care ar trebui să fie consultată autoritatea pentru protecția datelor.

[85] Întotdeauna trebuie să se ia în considerare riscul daunelor financiare, de exemplu, în cazul în care o încălcare a securității datelor divulgă informații financiare care trebuiau să fie într-un mediu sigur și acest lucru conduce la

De asemenea, este important să se înțeleagă faptul că, cel mai adesea, o serie de evenimente asociate și neasociate pot conduce în mod cumulativ la impactul negativ final asupra persoanei vizate și poate fi dificil să se identifice activitatea de prelucrare prin care operatorul a jucat un rol-cheie în impactul negativ.

Având în vedere că intentarea unei acțiuni în despăgubire pentru prejudiciul sau dauna suferită este adesea dificilă pentru persoanele vizate în acest context, chiar dacă efectul este foarte real, este cu atât mai important să ne concentrăm asupra prevenirii și asupra asigurării faptului că activitățile de prelucrare a datelor pot fi efectuate numai cu condiția să nu prezinte niciun risc sau să prezinte un risc foarte scăzut de impact negativ nedorit asupra intereselor sau asupra drepturilor și libertăților fundamentale ale persoanelor vizate.

În evaluarea impactului, terminologia și metodologia evaluării tradiționale a riscurilor pot fi utile, într-o anumită măsură, prin urmare, anumite elemente metodologice vor fi prezentate mai jos, pe scurt. Cu toate acestea, o metodologie globală de evaluare a impactului – în contextul articolului 7 litera (f) sau în sens mai larg – ar depăși domeniul de aplicare a prezentului aviz.

În acest și în orice alt context, este important să se identifice sursele unor potențiale impacturi asupra persoanelor vizate.

Probabilitatea de materializare a riscului este unul dintre elementele de luat în considerare. De exemplu, accesul la internet, schimburile de date cu site-uri din afara UE, interconexiunile cu alte sisteme, precum și un grad ridicat de eterogenitate sau variabilitate a sistemului pot reprezenta vulnerabilități pe care hackerii le-ar putea exploata. Această sursă de risc are o probabilitate relativ ridicată de materializare a riscului de compromitere a datelor. În schimb, un sistem omogen și stabil care nu are interconexiuni și nu este conectat la internet are o probabilitate mai mică de compromitere a datelor.

Un alt element al evaluării riscurilor este gravitatea consecințelor unui risc materializat. Gravitatea poate varia de la niveluri scăzute (precum necesitatea supărătoare de a introduce din nou datele de contact cu caracter personal pierdute de către operator) la niveluri foarte ridicate (cum ar fi pierderea vieții, în cazul în care modelele de localizare individuală a persoanelor protejate ajung pe mâinile infractorilor sau când alimentarea cu energie electrică este întreruptă de la distanță, prin dispozitive de contorizare inteligentă, în condiții meteorologice sau de sănătate personală critice).

Aceste două elemente-cheie – probabilitatea de materializare a riscului, pe de o parte, și gravitatea consecințelor, pe de altă parte – contribuie fiecare la evaluarea globală a impactului potențial.

În cele din urmă, în aplicarea metodologiei, ar trebui reamintit faptul că evaluarea impactului în temeiul articolului 7 litera (f) nu trebuie să conducă la un exercițiu mecanic și pur

furtul de identitate ori la alte forme de fraudă sau riscul de vătămare corporală, durere, suferința și pierderea facilităților care ar putea rezulta în cele din urmă, de exemplu, în urma modificării neautorizate a dosarelor medicale și, în consecință, a tratării necorespunzătoare a unui pacient, deși acestea nu sunt limitate la situațiile din domeniul de aplicare a articolului 7 litera (f). În același timp, astfel de riscuri nu sunt singurele care trebuie luate în considerare în momentul evaluării impactului în temeiul articolului 7 litera (f).

cantitativ. În scenariile tradiționale de evaluare a riscului, „gravitatea” poate lua în considerare numărul persoanelor care ar putea fi afectate. Cu toate acestea, ar trebui să se țină seama de faptul că prelucrarea datelor cu caracter personal care ar putea avea un impact asupra unui număr mic de persoane vizate – sau chiar și numai asupra unei singure persoane – necesită în continuare o analiză foarte atentă, în special în cazul în care impactul asupra fiecărei persoane vizate ar putea fi semnificativ.

ii) Natura datelor

În primul rând, ar fi important să se evalueze dacă prelucrarea implică date sensibile fie datorită faptului că acestea aparțin categoriilor speciale de date în conformitate cu articolul 8 din directivă, fie din alte motive, cum este cazul datelor biometrice, al informațiilor genetice, al datelor de comunicații, al datelor de localizare și al altor tipuri de informații cu caracter personal care necesită o protecție specială[86].

Pentru ilustrare, în opinia grupului de lucru, ca regulă generală, utilizarea datelor biometrice pentru cerințele generale de securitate a bunurilor și persoanelor este considerată ca fiind un interes legitim care ar prevala asupra interesului sau asupra drepturilor și libertăților fundamentale ale persoanei vizate. Astfel, datele biometrice precum amprentele digitale și/sau scanarea irisului ar putea fi utilizate pentru securitatea unei zone cu grad sporit de risc, cum ar fi un laborator care desfășoară activități de cercetare privind virusurile periculoase, cu condiția ca operatorul să fi furnizat dovezi concrete ale unui risc considerabil[87].

În general, cu cât informațiile în cauză sunt mai sensibile, cu atât pot exista mai multe consecințe pentru persoana vizată. Totuși, acest lucru nu înseamnă că datele care în sine ar putea să pară inofensive pot fi prelucrate liber în temeiul articolului 7 litera (f). În fapt, chiar și astfel de date, în funcție de modul în care sunt prelucrate, pot avea un impact semnificativ asupra persoanelor, astfel cum se va arăta la punctul (iii) de mai jos.

În această privință, faptul dacă datele au fost deja făcute publice de către persoana vizată sau de către terți poate fi relevant. În acest sens, în primul rând, este important să se sublinieze că datele cu caracter personal, inclusiv în cazul în care au fost puse la dispoziția publicului, continuă să fie considerate drept date cu caracter personal și, prin urmare, prelucrarea acestora necesită în continuare garanții adecvate[88]. Nu există o permisiune generală de a reutiliza și a prelucra în continuare datele cu caracter personal accesibile publicului în temeiul articolului 7 litera (f).

[86] Datele biometrice și informațiile genetice sunt considerate categorii speciale de date în propunerea Comisiei de regulament privind protecția datelor, citit împreună cu amendamentele propuse de Comisia LIBE. A se vedea amendamentul 103 la articolul 9 din versiunea finală a raportului Comisiei LIBE. Cu privire la relația dintre articolele 7 și 8 din Directiva 95/46/CE, a se vedea secțiunea II.1.2 de mai sus, paginile 14-15.

[87] A se vedea Avizul nr. 3/2012 al grupului de lucru „articolul 29” privind evoluția tehnologiilor biometrice (WP193). Ca un alt exemplu, în Avizul său nr. 4/2009 privind Agenția Mondială Antidoping (citat la nota de subsol 32), grupul de lucru a subliniat că articolul 7 litera (f) nu ar fi un temei valabil pentru a prelucra datele medicale și datele referitoare la infracțiuni în contextul investigațiilor antidoping, având în vedere „gravitatea încălcărilor vieții private”. Prelucrarea datelor ar trebui să fie prevăzută de lege și să îndeplinească cerințele de la articolul 8 alineatele (4) sau (5) din directivă.

[88] A se vedea Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9 de mai sus), precum și Avizul nr. 6/2013 al grupului de lucru privind datele deschise și reutilizarea informațiilor din sectorul public (ISP), adoptat la 5.6.2013 (WP207).

Având în vedere acestea, faptul că datele cu caracter personal sunt disponibile publicului poate fi considerat un factor în cadrul evaluării, în special în cazul în care publicarea a fost efectuată cu o așteptare rezonabilă de utilizare ulterioară a datelor în anumite scopuri (de exemplu, în scopuri de cercetare sau legate de transparență și răspundere).

iii) Modul în care sunt prelucrate datele

Într-un sens mai larg, evaluarea impactului poate implica analizarea faptului dacă datele sunt făcute publice sau altfel accesibile unui număr mare de persoane sau o cantitate mare de date cu caracter personal sunt prelucrate sau combinate cu alte date (de exemplu, în cazul creării de profiluri, pentru activități comerciale, de aplicare a legii sau în alte scopuri). Datele aparent inofensive, atunci când sunt prelucrate la scară largă și combinate cu alte date, pot conduce la concluzii cu privire la date mai sensibile, astfel cum s-a arătat mai sus în scenariul 3, care ilustrează relația dintre obiceiurile de consum de pizza și primele de asigurare de sănătate.

Pe lângă faptul că ar putea conduce la prelucrarea de date mai sensibile, o astfel de analiză ar putea genera, de asemenea, estimări ciudate, neașteptate și uneori, de asemenea, inexacte, de exemplu în ceea ce privește comportamentul sau personalitatea persoanelor vizate. În funcție de natura și impactul previziunilor, acest lucru poate fi deosebit de intruziv pentru viața privată a persoanelor[89].

Grupul de lucru a subliniat, de asemenea, într-un aviz precedent riscurile inerente ale anumitor soluții de securitate (inclusiv pentru soluțiile de tip firewall, antivirus și antispam), întrucât acestea pot conduce la implementarea pe scară largă a unui sistem de examinare în detaliu a pachetului de date, care poate avea o influență semnificativă asupra evaluării echilibrului drepturilor[90].

În general, cu cât mai negativ sau nesigur ar putea fi impactul prelucrării, cu atât este mai puțin probabil ca prelucrarea să fie considerată, în ansamblu, ca fiind legitimă. Disponibilitatea metodelor alternative pentru atingerea obiectivelor urmărite de operator, cu un impact mai puțin negativ pentru persoana vizată, ar trebui să fie, cu siguranță, un aspect relevant în acest context. Atunci când este necesar, evaluările impactului asupra protecției datelor și a vieții private pot fi utilizate pentru a stabili dacă acest lucru este posibil.

iv) Așteptările rezonabile ale persoanei vizate

Așteptările rezonabile ale persoanei vizate în ceea ce privește utilizarea și divulgarea datelor sunt, de asemenea, foarte relevante în acest sens. Astfel cum s-a subliniat, de asemenea, cu privire la analiza principiului limitării scopului[91], este „important să se analizeze dacă statutul operatorului de date[92], natura relației sau a serviciilor furnizate[93] sau obligațiile legale sau

[89] A se vedea secțiunea III.2.5 și anexa 2 („Volumele mari de date” și „Datele deschise”) din avizul privind limitarea scopului (citat la nota de subsol 9).
[90] A se vedea secțiunea 3.1 din Avizul nr. 1/2009 al grupului de lucru privind propunerile de modificare a Directivei 2002/58/CE asupra confidențialității și comunicațiilor electronice (Directiva privind confidențialitatea în mediul electronic) (WP159).
[91] A se vedea paginile 24-25 din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9).
[92] „Cum ar fi, de exemplu, un avocat sau un medic.”

contractuale aplicabile (sau alte promisiuni făcute la momentul colectării) ar putea da naştere unor aşteptări rezonabile de confidenţialitate mai strictă şi limitări mai stricte privind utilizarea ulterioară. În general, cu cât contextul colectării este mai specific şi mai restrictiv, cu atât este probabil să existe mai multe restricţii privind utilizarea. În acest caz de asemenea, este necesar să se ţină seama de contextul de fapt, mai degrabă decât să se invoce pur şi simplu clauzele contractuale tipărite cu caractere mici.

v) Statutul operatorului de date şi al persoanei vizate

Statutul persoanei vizate şi cel al operatorului de date sunt, de asemenea, relevante pentru a evalua impactul prelucrării datelor. În funcţie de faptul dacă operatorul de date este o persoană fizică sau o organizaţie mică, o întreprindere mare multinaţională sau un organism din sectorul public, precum şi de circumstanţele specifice, poziţia acestuia poate fi mai mult sau mai puţin dominantă în ceea ce priveşte persoana vizată. O întreprindere mare multinaţională poate, de exemplu, să dispună de mai multe resurse şi de o putere de negociere mai mare decât persoana vizată, prin urmare, aceasta ar putea fi mai în măsură să impună persoanei vizate ceea ce consideră că este în propriul „interes legitim". Acest aspect ar putea fi chiar mai pregnant în cazul în care întreprinderea deţine o poziţie dominantă pe piaţă. Dacă nu se iau măsuri, acest lucru se poate întâmpla în detrimentul persoanelor vizate. La fel cum legislaţia în materie de protecţie a consumatorilor şi în domeniul concurenţei contribuie la asigurarea faptului că o astfel de putere nu va fi utilizată în mod abuziv, legislaţia în materie de protecţie a datelor ar putea juca, de asemenea, un rol important în garantarea faptului că drepturile şi interesele persoanelor vizate nu vor fi afectate în mod nejustificat.

În acelaşi timp, statutul persoanei vizate este, de asemenea, relevant. În timp ce testul comparativ ar trebui, în principiu, să se efectueze în raport cu o persoană obişnuită, situaţiile specifice ar trebui să conducă la o abordare de la caz la caz: de exemplu, ar fi relevant să se stabilească dacă persoana vizată este un minor[94] sau aparţine unei categorii mai vulnerabile a populaţiei, care necesită o protecţie specială, cum ar fi, de exemplu, persoanele bolnave mintal, solicitanţi de azil sau persoanele în vârstă. De asemenea, cu siguranţă ar trebui să fie relevant dacă persoana vizată este un angajat, un student, un pacient al operatorului, sau dacă există un alt tip de dezechilibru în relaţia dintre poziţia persoanei vizate şi cea a operatorului. Este important să se evalueze efectul prelucrării efective a datelor asupra anumitor persoane.

În sfârşit, este important să se sublinieze faptul că nu toate impacturile negative asupra persoanelor vizate au aceeaşi „pondere" în cadrul echilibrului. Scopul exerciţiului de comparare în temeiul articolului 7 litera (f) nu este de a preveni orice impact negativ asupra persoanei vizate. Mai degrabă, scopul acestuia este de a preveni un impact disproporţionat. Aceasta este o diferenţă fundamentală. De exemplu, publicarea în ziar a unui articol bine documentat şi exact privind presupusa corupţie guvernamentală poate dăuna reputaţiei funcţionarilor guvernamentali implicaţi şi poate conduce la consecinţe semnificative, inclusiv

[93] „Cum ar fi, de exemplu, serviciile de cloud computing pentru gestionarea documentelor personale, serviciile de poştă electronică, agende, cititoarele electronice dotate cu caracteristici de luare de notiţe şi diverse aplicaţii tip jurnal („life-logging") care pot conţine informaţii foarte personale."

[94] A se vedea Avizul nr. 2/2009 al grupului de lucru privind protecţia datelor cu caracter personal ale copiilor, (Orientări generale şi cazul special al şcolilor), adoptat la 11.2.2009 (WP160). Avizul insistă asupra vulnerabilităţii specifice a copilului şi, în cazul în care copilul este reprezentat, asupra necesităţii de a se lua în considerare interesul superior al copilului, şi nu cel al reprezentantului acestuia.

pierderea reputației, pierderea alegerilor sau închisoare, însă ar putea, cu toate acestea, să aibă ca temei articolul 7 litera (f)[95].

(c) Echilibrul provizoriu

Atunci când sunt puse în balanță interesele și drepturile în cauză, astfel cum se descrie mai sus, măsurile adoptate de operator pentru a-și respecta obligațiile generale în temeiul directivei, inclusiv în ceea ce privește proporționalitatea și transparența, vor contribui în mod semnificativ la asigurarea faptului că prelucrarea datelor respectă cerințele prevăzute la articolul 7 litera (f). Conformitatea deplină ar trebui să însemne că impactul asupra persoanelor este redus, că interesele persoanelor vizate sau drepturile sau libertățile fundamentale sunt *mai puțin susceptibile* a fi afectate și că, prin urmare, este *mai probabil* ca operatorul de date să se poată baza pe articolul 7 litera (f). Acest lucru ar trebui să încurajeze operatorii să respecte toate dispozițiile orizontale ale directivei[96].

Acest lucru nu înseamnă, cu toate acestea, că respectarea cerințelor orizontale va fi întotdeauna suficientă, în sine, pentru a asigura un temei juridic în baza articolului 7 litera (f). Într-adevăr, dacă ar fi astfel, articolul 7 litera (f) ar fi de prisos sau ar deveni o lacună legislativă care ar lipsi de sens întregul articol 7, care prevede existența unui temei juridic specific adecvat pentru prelucrare.

Din acest motiv, este important să se efectueze o evaluare suplimentară în cadrul exercițiului de comparare în cazurile în care – pe baza unei analize preliminare – nu este clară direcția în care ar trebui să se atingă un echilibru. Operatorul poate lua în considerare posibilitatea de a introduce măsuri suplimentare, dincolo de respectarea dispozițiilor orizontale ale directivei, în scopul de a contribui la reducerea impactului nejustificat al prelucrării asupra persoanelor vizate.

Măsurile suplimentare pot include, de exemplu, oferirea unui mecanism ușor accesibil și funcțional pentru a asigura o posibilitate necondiționată de excludere voluntară de la prelucrare pentru persoanele vizate. Astfel de măsuri suplimentare pot, în unele cazuri (dar nu în toate) să încline balanța și să faciliteze garantarea faptului că prelucrarea se poate întemeia pe articolul 7 litera (f) și, în același timp, să asigure protecția drepturilor și a intereselor persoanelor vizate.

(d) Garanțiile suplimentare aplicate de către operator

Astfel cum s-a explicat mai sus, modul în care operatorul ar aplica măsuri adecvate ar putea, în anumite situații, să contribuie la „înclinarea balanței" echilibrului. Acceptabilitatea rezultatului va depinde de evaluarea în ansamblu. Cu cât este mai semnificativ impactul asupra persoanei vizate, cu atât ar trebui să se acorde mai multă atenție garanțiilor relevante.

Exemplele de măsuri pot include, printre altele, limitarea strictă cu privire la cantitatea de date colectate sau ștergerea imediată a datelor după utilizare. În timp ce unele dintre aceste măsuri

[95] Astfel cum s-a explicat mai sus, trebuie să se ia în considerare, de asemenea, orice derogări relevante pentru prelucrarea în scopuri jurnalistice în temeiul articolului 9 din directivă.
[96] În ceea ce privește rolul important al „conformității orizontale", a se vedea, de asemenea, pagina 54 din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului, citat la nota de subsol 9 de mai sus.

pot fi deja obligatorii în temeiul directivei, acestea sunt, adesea, scalabile și lasă operatorilor o marjă pentru a asigura o mai bună protecție a persoanelor vizate. De exemplu, operatorul poate să colecteze mai puține date sau să furnizeze informații suplimentare față de ceea ce este prevăzut în mod explicit la articolele 10 și 11 din directivă.

În alte cazuri, garanțiile nu sunt prevăzute în mod explicit în directivă, dar pot fi solicitate în viitor în cadrul propunerii de regulament sau sunt necesare numai în anumite situații precum:

- măsuri tehnice și organizatorice pentru a se asigura că datele nu pot fi utilizate pentru a lua decizii sau pentru a întreprinde alte acțiuni cu privire la persoane („separarea funcțională”, astfel cum se practică adesea într-un context de cercetare);
- utilizarea extinsă a tehnicilor de anonimizare;
- agregarea datelor;
- tehnologii menite să sporească protecția vieții private, protejarea vieții private din faza de concepție, evaluări ale impactului asupra protecției datelor și a vieții private;
- transparență sporită;
- dreptul general și necondiționat de excludere voluntară („opt-out”);
- portabilitatea datelor și măsurile conexe de sprijinire a persoanelor vizate;

Grupul de lucru observă că, în ceea ce privește unele aspecte-cheie, inclusiv separarea funcțională și tehnicile de anonimizare, au fost deja furnizate unele orientări în secțiunile relevante din avizele sale privind limitarea scopului, privind datele deschise și privind tehnicile de anonimizare[97].

În ceea ce privește pseudonimizarea și criptarea, grupul de lucru ar dori să sublinieze că, în cazul în care datele nu sunt direct identificabile ca atare, aceasta nu afectează aprecierea legitimității prelucrării: aceasta nu ar trebui interpretată ca transformarea unei prelucrări nelegitime într-o prelucrare legitimă[98].

În același timp, pseudonimizarea și criptarea, la fel ca toate celelalte măsuri tehnice și organizatorice introduse pentru a proteja datele cu caracter personal, vor juca un rol important în ceea ce privește evaluarea potențialului impact al prelucrării asupra persoanei vizate și, prin urmare, pot în unele cazuri să joace un rol în înclinarea balanței în favoarea operatorului. Utilizarea unor forme mai puțin riscante de prelucrare a datelor cu caracter personal (de exemplu, date cu caracter personal care sunt criptate atunci când sunt stocate sau în tranzit sau date cu caracter personal care sunt mai puțin directe și mai dificil de identificat) ar însemna, în general, că este redusă probabilitatea ca interesele sau drepturilor și libertăților fundamentale ale persoanelor vizate să fie afectate.

[97] A se vedea secțiunile III.2.3, III.2.5 din și anexa 2f la Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului, citat mai sus la nota de subsol 9, referitoare la prelucrarea ulterioară în scopuri istorice, statistice și științifice, precum și volumele mari de date și datele deschise; a se vedea, de asemenea, părțile relevante la Avizul nr. 6/2013 al grupului de lucru privind datele deschise (citat la nota de subsol 88 de mai sus) și Avizul nr. 5/2014 privind tehnicile de anonimizare.

[98] În acest sens, a se vedea amendamentele votate de Comisia LIBE în raportul final al Comisiei LIBE, în special amendamentul 15 privind considerentul 38 care corelează pseudonimizarea și așteptările legitime ale persoanei vizate.

În legătură cu astfel de garanții – și evaluarea globală a echilibrului – grupul de lucru dorește să sublinieze trei teme specifice care joacă adesea un rol esențial în contextul articolului 7 litera (f):

- relația dintre testul comparativ, transparență și principiul răspunderii;
- dreptul persoanei vizate de a se opune prelucrării datelor și, dincolo de opoziție, disponibilitatea opțiunii de excludere voluntară, fără a fi necesară o justificare, precum și
- sprijinirea persoanelor vizate: portabilitatea datelor, precum și disponibilitatea unor mecanisme viabile pentru ca persoana vizată să acceseze, să modifice, să șteargă, să transfere sau să prelucreze în continuare propriile date în alt mod (sau să permită unor terți să le prelucreze în continuare).

Datorită importanței lor, aceste subiecte vor fi discutate în secțiuni separate.

III.3.5. Răspundere și transparență

În primul rând, înainte de efectuarea unei operațiuni de prelucrare în temeiul articolului 7 litera (f), operatorul are responsabilitatea de a evalua dacă are un interes legitim, dacă prelucrarea este necesară pentru realizarea interesului legitim respectiv și dacă interesele și drepturile persoanelor vizate prevalează în cazul respectiv.

În acest sens, articolul 7 litera (f) se bazează pe principiul răspunderii. Operatorul trebuie să efectueze în prealabil un test atent și eficace, bazat pe elementele specifice ale cazului mai degrabă decât într-un mod abstract, luând în considerare, de asemenea, așteptările rezonabile ale persoanelor vizate. O bună practică ar fi ca, după caz, efectuarea testului să fie documentată suficient de detaliat și transparent, astfel încât aplicarea corectă și completă a testului să poată fi verificată – atunci când este necesar – de către părțile interesate relevante, inclusiv persoanele vizate și autoritățile de protecție a datelor și, în cele din urmă, de instanțele judecătorești.

Operatorul definește întâi interesul legitim și efectuează testul comparativ, dar acesta nu reprezintă neapărat evaluarea finală și definitivă: în cazul în care, în realitate, interesul urmărit nu este cel care a fost specificat de operator sau dacă operatorul a definit interesul insuficient de detaliat, echilibrul trebuie să fie reevaluat, pe baza interesului real, care trebuie să fie stabilit de autoritatea pentru protecția datelor sau de o instanță[99]. La fel precum în cazul altor aspecte importante ale protecției datelor cum ar fi identificarea operatorului de date sau specificarea scopului[100], ceea ce contează este realitatea din spatele oricărei afirmații făcute de către operator.

Noțiunea de răspundere este strâns legată de noțiunea de transparență. Pentru a permite persoanelor vizate să își exercite drepturile și pentru a permite examinarea publică de către părțile interesate la un nivel mai amplu, grupul de lucru recomandă ca operatorii să explice persoanelor vizate într-un mod clar și ușor de înțeles motivele pentru care aceștia consideră că interesul sau drepturile și libertățile fundamentale ale persoanei vizate nu prevalează asupra interesului operatorului și să explice, de asemenea, măsurile de protecție care au fost luate

[99] De exemplu, în urma unei plângeri sau a unei obiecții în temeiul articolului 14.
[100] A se vedea avizele citate în nota de subsol 9.

pentru a proteja datele cu caracter personal, inclusiv, dacă este cazul, dreptul de excludere voluntară de la prelucrare[101].

În această privință, grupul de lucru subliniază faptul că legislația în materie de protecție a consumatorului, în special legislația care protejează consumatorii împotriva practicilor comerciale neloiale, este, de asemenea, extrem de relevantă în acest context.

Dacă un operator ascunde informații importante referitoare la utilizarea ulterioară neașteptată a datelor în spatele terminologiei juridice utilizate în clauzele contractuale tipărite cu caractere mici, atunci acest lucru poate aduce atingere normelor de protecție a consumatorilor privind clauzele contractuale abuzive (inclusiv interzicerea „clauzelor surprinzătoare") și, de asemenea, nu îndeplinește cerințele prevăzute la articolul 7 litera (a) privind consimțământul valabil și în cunoștință de cauză sau cerințele de la articolul 7 litera (f) în ceea ce privește așteptările rezonabile ale persoanei vizate și un echilibru în general acceptabil al intereselor. Desigur, acest lucru ar ridica, de asemenea, întrebări legate de conformitatea cu articolul 6 în ceea ce privește necesitatea unei prelucrări corecte și legale a datelor cu caracter personal.

De exemplu, în numeroase cazuri, utilizatorii serviciilor online „gratuite" precum serviciile de căutare, poștă electronică, mijloace de comunicare sociale, stocarea de fișiere sau alte aplicații online sau mobile nu sunt pe deplin conștienți de măsura în care activitatea lor este înregistrată și analizată pentru a genera valoare pentru prestatorul de servicii și, prin urmare, rămân indiferenți la riscurile implicate.

Pentru a sprijini persoanele vizate în aceste situații, o primă condiție prealabilă[102] necesară – dar nu suficientă în sine – este clarificarea faptului că serviciile nu sunt gratuite și că, mai degrabă, consumatorii plătesc cu datele lor cu caracter personal. De asemenea, condițiile și garanțiile sub rezerva cărora pot fi utilizate datele trebuie să fie explicate foarte clar în fiecare caz pentru a asigura validitatea consimțământului prevăzut la articolul 7 litera (a) sau un echilibru favorabil în temeiul articolului 7 litera (f).

III.3.6. Dreptul de opoziție și dincolo de acesta

(a) Dreptul de opoziție prevăzut la articolul 14 din directivă

Articolul 7 literele (e) și (f) este special în sensul că, în timp ce articolul se bazează, în principal, pe o evaluare obiectivă a intereselor și drepturilor în cauză, acesta permite, de asemenea, luarea în considerare a autodeterminării persoanei vizate, care are drept de

[101] Conform explicațiilor de la pagina 46 din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat mai sus la nota de subsol 9), în cazul creării de profiluri cu automatizarea procesului decizional, „pentru a asigura transparența, persoanele vizate/consumatorii ar trebui să aibă acces la «profilurile» lor, precum și la logica procesului decizional (algoritmul) care a condus la elaborarea a profilului. Cu alte cuvinte: organizațiile ar trebui să își facă publice criteriile decizionale. Acest lucru este o garanție esențială și cu atât mai importantă într-o lume a marilor volume de date". Faptul dacă o organizație oferă sau nu această transparență reprezintă un factor foarte relevant care trebuie luat în considerare, de asemenea, în exercițiul de comparare.

[102] Pentru mai multe garanții posibile referitoare la situațiile din ce în ce mai comune în care consumatorii plătesc cu datele lor cu caracter personal, a se vedea secțiunea III.3.6, în special paginile 47-48 privind „Alternative favorabile protecției datelor la serviciile online «gratuite»" și „Portabilitatea datelor, «midata» și aspecte conexe".

opoziție[103]: cel puțin în cazul celor două temeiuri, articolul 14 litera (a) din directivă prevede că („exceptând cazul când dreptul intern prevede altfel") persoana vizată „poate să se opună, în orice moment, din considerente întemeiate și legitime legate de situația sa particulară, prelucrării datelor în cauză". Acesta adaugă dispoziția conform căreia, în cazul în care opoziția este justificată, prelucrarea datelor cu caracter personal în cauză trebuie să înceteze.

În principiu, în conformitate cu legislația actuală, persoana vizată trebuie să demonstreze existența unor „considerente întemeiate și legitime" pentru a împiedica prelucrarea datelor sale personale [articolul 14 litera (a)], cu excepția contextului activităților de marketing direct în care nu este necesar ca obiecția să fie justificată [articolul 14 litera (b)].

Acest lucru nu ar trebui să fie considerat ca fiind în contradicție cu testul comparativ prevăzut la articolul 7 litera (f), care este efectuat *a priori*: mai degrabă, acesta completează echilibrul, în sensul că, în cazul în care prelucrarea este permisă în urma unei evaluări obiective și rezonabile a diferitelor drepturi și interese aflate în discuție, persoana vizată are în continuare o posibilitate *suplimentară* de a se opune, pe considerente legate de situația sa personală. Acest fapt va trebui să conducă ulterior la o nouă evaluare, luând în considerare argumentele specifice prezentate de persoana vizată. Noua evaluare este, în principiu, supusă din nou verificării de către o autoritate responsabilă cu protecția datelor sau de instanțele judecătorești.

(b) Dincolo de opoziție: rolul excluderii voluntare ca garanție suplimentară

Grupul de lucru subliniază că, deși dreptul de opoziție prevăzut la articolul 14 litera (a) face obiectul justificării de către persoana vizată, nimic nu împiedică operatorul să ofere o opțiune de excludere voluntară care ar fi mai amplă și nu ar necesita nicio demonstrație suplimentară a interesului legitim (imperios sau nu) din partea persoanei vizate. Un astfel de drept necondiționat nu ar fi necesar să se bazeze pe situația specifică a persoanelor vizate.

Într-adevăr, mai ales în cazurile-limită, în care este dificil să se ajungă la un echilibru, un mecanism de excludere voluntară bine conceput și operativ, deși nu ar furniza neapărat persoanelor vizate toate elementele care ar îndeplini condițiile prin care un consimțământ este valabil în temeiul articolului 7 litera (a), ar putea juca un rol important în protejarea drepturilor și intereselor persoanelor vizate.

Pentru aceasta este necesară o abordare nuanțată, care să facă distincția între cazurile în care este necesar consimțământul de includere („opt-in") prevăzut la articolul 7 litera (a) și cazurile în care o posibilitate operativă de excludere voluntară („opt-out") de la prelucrare (combinată cu alte măsuri suplimentare posibile) poate contribui la protejarea persoanelor vizate de articolul 7 litera (f).

Cu cât mecanismul de excludere voluntară („opt-out") este mai larg aplicabil și mai ușor de utilizat, cu atât va contribui mai mult acesta la înclinarea balanței în favoarea identificării unui temei juridic pentru prelucrare în articolul 7 litera (f).

[103] Dreptul de opoziție nu ar trebui să fie confundat cu consimțământul în baza articolului 7 litera (a), conform căruia operatorul de date nu poate prelucra date înainte de a obține consimțământul. În contextul articolului 7 litera (f), operatorul poate prelucra datele, sub rezerva unor condiții și garanții, atât timp cât persoana vizată nu a ridicat obiecții. În acest sens, dreptul de opoziție poate fi considerat o formă specifică de excludere voluntară. A se vedea mai multe detalii în Avizul nr. 15/2011 al grupului de lucru privind definiția consimțământului (citat la nota de subsol 2).

Ilustrare: evoluția abordării marketingului direct

Pentru a ilustra modul în care se face o distincție între cazurile în care este necesar consimțământul prevăzut la articolul 7 litera (a) și cazurile în care se poate utiliza o excludere voluntară ca măsură de protecție în temeiul articolului 7 litera (f), este util să se utilizeze exemplul marketingului direct, pentru care a existat în mod tradițional o clauză specifică de excludere voluntară inclusă în articolul 14 litera (b) din directivă. Pentru a aborda noile evoluții tehnologice, dispoziția respectivă a fost completată ulterior prin dispoziții specifice ale Directivei privind confidențialitatea în mediul electronic[104].

În temeiul articolului 13 din Directiva privind confidențialitatea în mediul electronic, pentru anumite tipuri de activități – mai intruzive – de marketing direct (precum marketingul prin e-mail și roboți de apelare automată), consimțământul este norma. Ca o excepție, în relațiile existente cu clienții în care un operator face publicitate propriilor produse sau servicii „similare", este suficient să se ofere o posibilitate (necondiționată) de „excludere voluntară" fără justificare.

Tehnologiile au evoluat, făcând necesare soluții similare relativ simple care să urmeze o logică asemănătoare pentru noile practici de marketing.

În primul rând, a evoluat modul în care materialul promoțional este livrat: în loc de simple e-mailuri care ajung în căsuța de poștă electronică, în prezent, anunțurile specifice de publicitate comportamentală apar, de asemenea, pe ecranele telefoanelor inteligente și ale computerelor. În viitorul apropiat, reclamele vor putea fi integrate, de asemenea, în obiecte inteligente legate în cadrul internetului obiectelor.

În al doilea rând, reclamele devin din ce în ce mai specific direcționate: în loc să se bazeze pe simple profiluri ale clienților, activitățile consumatorilor sunt din ce în ce mai mult urmărite și stocate online și offline și analizate utilizând metode automate mai sofisticate[105].

Ca urmare a acestor evoluții, obiectul exercițiului de comparare s-a modificat: nu se mai pune problema dreptului la liberă exprimare comercială, ci, în primul rând, a intereselor economice ale organizațiilor patronale de a-și cunoaște clienții prin urmărirea și monitorizarea activităților lor online și offline, care ar trebui să fie puse în balanță cu drepturile (fundamentale) la viață privată și protecția datelor cu caracter personal a persoanelor vizate și interesul acestora de a nu fi monitorizate în mod nejustificat.

Schimbarea modelelor de afaceri prevalente, precum și creșterea valorii datelor cu caracter personal ca activ pentru organizațiile comerciale explică recenta cerință privind consimțământul în acest context, în conformitate cu articolul 5 alineatul (3) și articolul 13 din Directiva privind confidențialitatea în mediul electronic.

Prin urmare, există diferite norme specifice, în funcție de forma de comercializare, inclusiv:

[104] În ceea ce privește articolul 13 din Directiva privind confidențialitatea în mediul electronic, a se vedea, de asemenea, secțiunea III.2.4 din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9).

[105] A se vedea secțiunea III.2.5 și anexa 2 (privind volumele mari de date și datele deschise) din Avizul nr. 3/2013 al grupului de lucru privind limitarea scopului (citat la nota de subsol 9).

- dreptul necondiționat de a se opune marketingului direct (conceput pentru contextul trimiterii de comunicări prin poșta tradițională și pentru comercializarea unor produse similare) în temeiul articolului 14 litera (b) din directivă; articolul 7 litera (f) ar putea constitui temeiul juridic în acest caz;
- cerința privind consimțământul, în conformitate cu articolul 13 din Directiva privind confidențialitatea în mediul electronic pentru sistemele de apelare automată, fax, mesajele tip SMS și marketingul prin e-mail (sub rezerva anumitor excepții)[106] și aplicarea *de facto* a articolului 7 litera (a) din Directiva privind protecția datelor;
- cerința privind consimțământul, în conformitate cu articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic [și articolul 7 litera (a) din Directiva privind protecția datelor] în ceea ce privește publicitatea comportamentală pe baza unor tehnici de urmărire, cum ar fi cookie-urile care stochează informații în terminalul utilizatorului[107].

În timp ce temeiurile juridice aplicabile sunt clare în ceea ce privește articolul 5 alineatul (3) și articolul 13 din Directiva privind confidențialitatea în mediul electronic, nu toate formele de comercializare sunt reglementate și ar fi de dorit să existe orientări cu privire la situațiile care necesită consimțământul prevăzut la articolul 7 litera (a) și situațiile pentru care este obținut un echilibru în temeiul articolului 7 litera (f), inclusiv posibilitatea de excludere voluntară („opt-out”).

În acest sens, este util să se țină seama de avizul grupului de lucru privind limitarea scopului, în care se precizează că „în cazul în care o întreprindere dorește în mod specific să analizeze sau să anticipeze preferințele, comportamentul și atitudinile personale ale clienților individuali, care vor influența ulterior «măsurile sau deciziile» luate în ceea ce privește acești clienți ... aproape întotdeauna va fi necesar consimțământul «opt-in» neechivoc, informat, specific și liber, altfel utilizarea ulterioară nu poate fi considerată compatibilă. Important este faptul că un astfel de consimțământ ar fi necesar, de exemplu, pentru urmărirea și crearea de profiluri în scopuri de marketing direct, publicitate comportamentală, brokeraj de date, publicitate bazată pe localizare sau cercetarea pieței digitale pe baza urmăririi”[108].

Alternative favorabile protecției datelor la serviciile online „gratuite”

În contextul în care clienții care se înscriu la servicii online „gratuite”, de fapt „plătesc” pentru astfel de servicii permițând utilizarea datelor lor cu caracter personal, ar contribui, de asemenea, la evaluarea favorabilă a echilibrului – sau la constatarea faptului că, într-adevăr, consumatorul a dispus efectiv de libertate de alegere și, prin urmare, a acordat un consimțământ valabil în temeiul articolului 7 litera (a) – dacă operatorul ar oferi, de asemenea, o versiune alternativă a serviciilor sale în care „datele cu caracter personal” nu ar fi utilizate în scopuri de marketing.

[106] A se vedea, de asemenea, articolul 13 alineatul (3) din Directiva privind confidențialitatea în mediul electronic, care oferă statelor membre posibilitatea de a alege între includere („opt-in”) și excludere („opt-out”) pentru marketingul direct prin alte mijloace.
[107] Pentru aplicarea dispoziției respective, a se vedea Avizul nr. 2/2010 al grupului de lucru privind publicitatea comportamentală online (WP171).
[108] A se vedea anexa II (privind volumele mari de date și datele deschise) din aviz (citat la nota de subsol 9), pagina 45.

Atât timp cât astfel de servicii alternative nu sunt disponibile, este mai dificil să se susțină că s-a acordat un consimțământ (liber) valabil în temeiul articolului 7 litera (a) prin simpla utilizare a serviciilor gratuite sau că balanța echilibrului prevăzut la articolul 7 litera (f) ar trebui să se încline în favoarea operatorului.

Considerațiile de mai sus subliniază rolul important pe care garanțiile suplimentare, inclusiv un mecanism viabil de excludere voluntară de la prelucrare, îl pot juca în modificarea echilibrului provizoriu. În același timp, acestea sugerează, de asemenea, că în unele cazuri articolul 7 litera (f) nu poate fi invocat ca temei pentru prelucrare și operatorii trebuie să asigure un consimțământ valabil în temeiul articolului 7 litera (a) – sau să îndeplinească alte condiții din directivă – pentru ca prelucrarea să aibă loc.

Portabilitatea datelor, „midata" și aspecte conexe

Printre măsurile suplimentare de protecție care ar putea contribui la înclinarea balanței, o atenție deosebită ar trebui acordată portabilității datelor și măsurilor conexe, care pot fi din ce în ce mai relevante în mediul online. Grupul de lucru reamintește avizul său privind limitarea scopului, în care a subliniat că „în multe situații, garanții precum acordarea de acces direct persoanelor vizate/clienților la datele lor personale într-un format prelucrabil automat ușor de utilizat și portabil poate contribui la sprijinirea acestora și la remedierea dezechilibrului economic dintre marile corporații, pe de o parte, și persoanele vizate/consumatori, pe de altă parte. De asemenea, aceasta ar permite persoanelor «să împărtășească bogăția» creată de volumele mari de date și ar stimula dezvoltatorii să ofere mai multe caracteristici și aplicații utilizatorilor lor"[109].

Disponibilitatea unor mecanisme viabile prin care persoanele vizate să acceseze, să modifice, să șteargă, să transfere sau să prelucreze în continuare propriile date în alt mod (sau să permită unor terți să le prelucreze în continuare) va veni în sprijinul persoanelor vizate și le va permite acestora să beneficieze mai mult de pe urma serviciilor digitale. De asemenea, aceasta poate încuraja un mediu de piață mai competitiv, permițând clienților să schimbe furnizorii cu ușurință (de exemplu în contextul serviciilor bancare pe internet sau în cazul furnizorilor de energie într-un mediu de rețele inteligente). În cele din urmă, aceasta poate contribui, de asemenea, la dezvoltarea unor servicii cu valoare adăugată suplimentară de către terții care pot să acceseze datele clienților la cerere și pe baza consimțământului clienților. În această perspectivă, portabilitatea datelor este benefică, prin urmare, nu doar pentru protecția datelor, ci și pentru concurență și pentru protecția consumatorilor[110].

[109] „A se vedea inițiativele precum «midata» în Regatul Unit, care se bazează pe principiul fundamental conform căruia datele trebuie să fie returnate consumatorilor. Midata este un program voluntar, care, în timp, ar trebui să ofere consumatorilor acces sporit la datele lor personale într-un format electronic portabil. Ideea centrală este că și consumatorii ar trebui să beneficieze, de asemenea, de volumele mari de date prin acces la propriile informații pentru a le permite să facă alegeri mai bune. A se vedea, de asemenea, inițiativele «butonul verde» care permit consumatorilor să aibă acces la informațiile privind propriul consum de energie." Pentru mai multe informații despre inițiativele din Regatul Unit și din Franța, a se vedea http://www.midatalab.org.uk/ și http://mesinfos.fing.org/.

[110] În ceea ce privește dreptul la portabilitatea datelor, a se vedea articolul 18 din propunerea de regulament.

IV. Observații finale

În prezentul aviz, grupul de lucru a analizat criteriile definite în articolul 7 din directivă privind legitimitatea prelucrării datelor. Dincolo de orientări privind interpretarea și aplicarea practică a articolului 7 litera (f) conform cadrului juridic existent, avizul urmărește formularea de recomandări de politică pentru a sprijini factorii de decizie atunci când iau în considerare modificări ale actualului cadru juridic privind protecția datelor. Înainte de elaborarea de recomandări, principalele constatări privind interpretarea articolului 7 sunt rezumate în cele ce urmează.

IV.1. Concluzii

Prezentare generală a articolului 7

Articolul 7 prevede ca datele cu caracter personal să fie prelucrate numai dacă se aplică cel puțin unul dintre cele șase temeiuri juridice enumerate în articolul în cauză.

Primul temei, articolul 7 litera (a), se axează pe consimțământul persoanei vizate ca temei de legitimitate. În schimb, restul temeiurilor permit prelucrarea – sub rezerva unor garanții – în situații în care, indiferent de consimțământ, este oportun și necesar să se prelucreze datele, într-un anumit context, pentru realizarea unui anumit interes legitim.

Fiecare dintre literele (b), (c), (d) și (e) specifică un anumit context în care prelucrarea datelor cu caracter personal poate fi considerată legitimă. Condițiile care se aplică în fiecare dintre diferitele contexte necesită o atenție deosebită, întrucât acestea determină domeniul de aplicare a diferitelor temeiuri de legitimitate. Mai exact, criteriile „necesară pentru executarea unui contract”, „necesară în vederea îndeplinirii unei obligații legale”, „necesară în scopul protejării interesului vital al persoanei vizate” și „necesară pentru aducerea la îndeplinire a unei sarcini de interes public sau care rezultă din exercitarea autorității publice” conțin cerințe diferite, care au fost discutate în secțiunea III.2.

Litera (f) se referă, mai general, la interesul legitim (de orice tip) urmărit de operator (în orice situație). Această dispoziție cu caracter general este însă condiționată de un test comparativ suplimentar, care impune ca interesul legitim urmărit de operator – sau de unul sau mai mulți terți cărora le sunt comunicate datele – să fie evaluat în funcție de interesul sau drepturile fundamentale ale persoanei vizate.

Rolul articolului 7 litera (f)

Articolul 7 litera (f) nu ar trebui să fie considerat un temei juridic care poate fi utilizat doar în cazuri excepționale pentru a umple lacunele în situații rare și neprevăzute ca soluție „de ultimă instanță” sau ca o ultimă șansă, în cazul în care nu se pot aplica alte temeiuri. În același timp, acesta nu ar trebui să fie considerat o opțiune preferată, iar utilizarea sa să fie extinsă în mod nejustificat deoarece ar fi considerat mai puțin constrângător decât celelalte temeiuri. Mai degrabă, acesta este un mijloc la fel de viabil ca oricare altul dintre temeiurile de legitimare a prelucrării datelor cu caracter personal.

Utilizarea corespunzătoare a articolului 7 litera (f), în condițiile potrivite și sub rezerva unor garanții adecvate, poate contribui la prevenirea utilizării abuzive și a bazării excesive pe alte temeiuri juridice. O evaluare corespunzătoare a echilibrului, astfel cum este prevăzută la articolul 7 litera (f), adeseori cu posibilitatea de excludere voluntară de la prelucrare, ar putea constitui, în unele cazuri, o alternativă viabilă la utilizarea necorespunzătoare, de exemplu, a temeiului privind „consimțământul" sau „necesară pentru executarea unui contract". Examinat în acest mod, articolul 7 litera (f) prezintă garanții complementare în raport cu alte criterii prestabilite. Prin urmare, acesta nu ar trebui considerat drept „cea mai slabă verigă" sau o ușă deschisă pentru a legitima toate activitățile de prelucrare a datelor care nu intră sub incidența niciunuia dintre celelalte temeiuri juridice.

Interesul legitim al operatorului/interesul sau drepturile fundamentale ale persoanei vizate

Conceptul de „interes" este miza mai largă pe care un operator o poate avea în ceea ce privește prelucrarea sau beneficiile pe care le obține – sau pe care societatea le-ar putea obține – în urma prelucrării. Interesul poate fi imperios, clar sau mai controversat. Prin urmare, situațiile menționate la articolul 7 litera (f) pot varia de la exercitarea drepturilor fundamentale sau protecția unor interese personale sau sociale importante la contexte mai puțin evidente sau chiar problematice.

Pentru a fi considerat „legitim" și pentru a fi relevant în temeiul articolului 7 litera (f), interesul va trebui să fie legal, și anume, conform cu dreptul UE și cu legislația națională. De asemenea, acesta trebuie să fie suficient de clar definit și suficient de specific pentru a permite efectuarea testului comparativ în raport cu interesul și drepturile fundamentale ale persoanei vizate. De asemenea, acesta trebuie să fie un interes real și actual – și anume, interesul nu trebuie să fie ipotetic.

Dacă operatorul sau terțul căruia îi sunt comunicate datele are un interes legitim, aceasta nu înseamnă neapărat că se poate baza pe articolul 7 litera (f) ca temei juridic pentru prelucrare. Posibilitatea ca articolul 7 litera (f) să poată constitui temeiul prelucrării va depinde de rezultatul testului comparativ subsecvent. De asemenea, prelucrarea trebuie să fie „necesară pentru realizarea interesului legitim" urmărit de operator sau – în cazul divulgării – de terț. Prin urmare, ar trebui să se prefere întotdeauna mijloacele mai puțin invazive care servesc aceluiași scop.

Noțiunea de „interes" al persoanelor vizate este definită în sens chiar mai larg, întrucât aceasta nu necesită un „element" de legitimitate. În timp ce operatorul de date sau terțul pot urmări orice interese, cu condiția ca acestea să nu fie nelegitime, persoana vizată, la rândul său, are dreptul să solicite luarea în considerare a tuturor categoriilor de interese și compararea acestora cu cele ale operatorului sau ale terțului, în măsura în care sunt relevante în ceea ce privește domeniul de aplicare a directivei.

Aplicarea testului comparativ

La interpretarea domeniului de aplicare a articolului 7 litera (f), grupul de lucru urmărește o abordare echilibrată, care să asigure flexibilitatea necesară operatorilor de date pentru situațiile în care nu există niciun impact asupra persoanelor vizate, oferind, în același timp, un grad suficient de certitudine juridică și de garanții persoanelor vizate, astfel încât dispoziția deschisă în cauză să nu fie utilizată în mod abuziv.

Pentru efectuarea testului comparativ, este important, în primul rând, să se ia în considerare natura și sursa intereselor legitime și dacă prelucrarea este necesară pentru urmărirea intereselor respective, pe de o parte, și impactul asupra persoanelor vizate, pe de altă parte. Această evaluare inițială ar trebui să ia în considerare măsurile, cum ar fi transparența sau colectarea limitată a datelor, pe care operatorul intenționează să le adopte pentru a se conforma directivei.

După analizarea și cântărirea comparativă a celor două părți, se poate stabili un „echilibru" provizoriu: se poate ajunge la o concluzie preliminară privind determinarea faptului că interesele legitime ale operatorului prevalează sau nu asupra drepturilor și intereselor persoanelor vizate. Cu toate acestea, pot exista cazuri în care rezultatul testului comparativ să fie neclar și să existe îndoieli legate de faptul dacă prevalează interesul legitim al operatorului (sau al terțului) și dacă prelucrarea se poate baza pe articolul 7 litera (f).

Din acest motiv, este important să se efectueze o evaluare suplimentară în cadrul exercițiului de comparare. În această etapă, operatorul poate analiza dacă este în măsură să introducă măsuri suplimentare, dincolo de respectarea altor dispoziții orizontale din directivă, pentru a contribui la protejarea persoanelor vizate. Măsurile suplimentare pot include, de exemplu, oferirea unui mecanism ușor accesibil și funcțional pentru a asigura o posibilitate necondiționată de excludere voluntară de la prelucrare pentru persoanele vizate.

Factorii-cheie care trebuie luați în considerare atunci când se aplică testul comparativ

Având în vedere cele menționate anterior, factorii utili care trebuie luați în considerare atunci când se efectuează testul comparativ includ:

- natura și sursa interesului legitim, inclusiv:

  - dacă prelucrarea datelor este necesară pentru exercitarea unui drept fundamental sau
  - dacă prelucrarea servește în alt fel interesului public sau beneficiază de recunoaștere juridică/normativă, culturală sau socială în comunitatea în cauză;

- impactul asupra persoanelor vizate, inclusiv:

  - natura datelor, de exemplu eventualitatea ca prelucrarea să implice date care pot fi considerate sensibile sau care au fost obținute din surse aflate la dispoziția publicului;
  - modul în care sunt prelucrate datele, inclusiv dacă datele sunt făcute publice sau sunt accesibile într-un alt mod unui număr mare de persoane sau dacă o cantitate mare de date cu caracter personal sunt prelucrate sau combinate cu alte date (de exemplu, în cazul creării de profiluri, pentru activități comerciale, de aplicare a legii sau în alte scopuri);

- așteptările rezonabile ale persoanei vizate, în special în ceea ce privește utilizarea și divulgarea datelor în contextul specific;
- statutul operatorului de date și al persoanei vizate, inclusiv echilibrul de putere între persoana vizată și operatorul de date sau dacă persoana vizată este un minor sau aparține unei categorii mai vulnerabile a populației.

- garanții suplimentare pentru a împiedica impactul nejustificat asupra persoanelor vizate, inclusiv:

  - minimizarea datelor (de exemplu, limite stricte privind colectarea datelor sau ștergerea imediată a datelor după utilizare);
  - măsuri organizatorice și tehnice pentru a se asigura faptul că datele nu pot fi folosite pentru a lua decizii sau alte acțiuni cu privire la persoane („separarea funcțională”);
  - utilizarea extinsă a tehnicilor de anonimizare, agregarea datelor, tehnologiile menite să sporească protecția vieții private, protejarea vieții private din faza de concepție, evaluări ale impactului asupra protecției datelor și a vieții private;
  - creșterea transparenței, dreptul necondiționat și general de excludere voluntară, portabilitatea datelor și măsurile conexe în sprijinul persoanelor vizate.

Răspunderea, transparența, dreptul de opoziție și dincolo de acesta

În legătură cu măsurile de protecție – și evaluarea în ansamblu a echilibrului – trei aspecte joacă adesea un rol crucial în contextul articolului 7 litera (f) și, prin urmare, necesită o atenție specială:

- existența unor măsuri și eventuala necesitate a unor măsuri suplimentare pentru a spori transparența și răspunderea;
- dreptul persoanei vizate de a se opune prelucrării datelor și, dincolo de opoziție, existența posibilității de excludere voluntară, fără a fi necesară niciun fel de justificare;
- sprijinirea persoanelor vizate: portabilitatea datelor, precum și disponibilitatea unor mecanisme viabile pentru ca persoana vizată să acceseze, să modifice, să șteargă, să transfere sau să prelucreze propriile date în continuare în alt mod (sau să permită unor terți să le prelucreze în continuare).

IV. 2. Recomandări

Textul actual al articolului 7 litera (f) din directivă are un caracter deschis. Formularea flexibilă a acestuia lasă loc de interpretări și a condus uneori – după cum arată experiența – la o lipsă a predictibilității și a securității juridice. Cu toate acestea, în cazul în care este utilizat în contextul potrivit și cu aplicarea criteriilor adecvate, astfel cum se indică în prezentul aviz, articolul 7 litera (f) are de jucat un rol esențial ca temei juridic pentru prelucrarea legitimă a datelor.

Prin urmare, grupul de lucru sprijină abordarea actuală de la articolul 6 din propunerea de regulament, care menține echilibrul intereselor ca un temei juridic separat. Cu toate acestea, ar fi binevenite orientări suplimentare, pentru a garanta o aplicare adecvată a testului comparativ.

Domeniu de aplicare și mijloace de prevedere a unor specificații suplimentare

O cerință esențială ar fi ca dispoziția să rămână suficient de flexibilă și să reflecte atât perspectivele operatorului de date și ale persoanei vizate, cât și natura dinamică a contextelor relevante. Din acest motiv, grupul de lucru este de opinie că furnizarea – în textul propunerii de regulament sau în acte delegate – de liste detaliate și exhaustive cu situații în care interesul ar fi calificat *de facto* ca fiind legitim nu este recomandabilă. De asemenea, grupul de lucru ar fi împotriva definirii cazurilor în care interesul sau dreptul uneia dintre părți ar trebui, *ca principiu* sau *ca prezumție*, să primeze asupra interesului sau dreptului celeilalte părți doar din cauza naturii unui astfel de drept sau interes sau datorită faptului că au fost luate anumite măsuri de protecție, de exemplu datele au fost doar pseudonimizate. Acest lucru ar risca să inducă în eroare și să fie inutil de prescriptiv.

Mai degrabă decât să se adopte decizii definitive privind meritele diferitelor drepturi și interese, grupul de lucru insistă asupra *rolului crucial al testului comparativ* în evaluarea prevăzută la articolul 7 litera (f). Este necesar să se mențină flexibilitatea testului, dar modul în care acesta se realizează trebuie să devină mai eficace în practică și să permită o conformare mai eficace. Aceasta ar trebui să se traducă prin *consolidarea* obligației de *răspundere* pentru operatorii de date, în cazul în care operatorului îi revine responsabilitatea de a *demonstra* că interesul și drepturile persoanei vizate nu prevalează asupra propriului interes.

Orientări și răspundere

În acest scop, grupul de lucru recomandă furnizarea de orientări în propunerea de regulament, după cum urmează.

1) Ar fi util să se identifice și să se furnizeze într-un considerent o listă neexhaustivă a factorilor-cheie care trebuie luați în considerare atunci când se aplică testul comparativ, cum ar fi natura și sursa interesului legitim, impactul asupra persoanelor vizate, precum și măsurile suplimentare de protecție care pot fi aplicate de către operator pentru a preveni orice impact nejustificat al prelucrării asupra persoanelor vizate. Astfel de garanții pot include, printre altele:
   - separarea funcțională a datelor, utilizarea adecvată a tehnicilor de anonimizare, criptarea și alte măsuri tehnice și organizatorice pentru a limita eventualele riscuri pentru persoanele vizate;
   - precum și măsuri pentru a asigura un grad mai ridicat de transparență și de alegere pentru persoanele vizate, cum ar fi, după caz, existența unei posibilități necondiționate de excludere voluntară de la prelucrare, gratuită și care poate fi invocată într-un mod eficace și cu ușurință.

2) Grupul de lucru ar sprijini, de asemenea, clarificări suplimentare în propunerea de regulament privind modul în care operatorul poate *demonstra*[111] o răspundere sporită.

   Modificarea condițiilor pentru exercitarea de către persoanele vizate a dreptului de opoziție, astfel cum se prevede la articolul 19 din propunerea de regulament, este deja un

[111] Demonstrarea trebuie să rămână în limite rezonabile şi să se concentreze mai degrabă pe rezultate decât pe procesul administrativ.

element important al răspunderii. În cazul în care persoana vizată se opune prelucrării datelor sale în temeiul articolului 7 litera (f), în conformitate cu propunerea de regulament va reveni operatorului să demonstreze că interesul său prevalează. Această inversare a sarcinii probei este puternic susținută de grupul de lucru deoarece contribuie la intensificarea obligației privind răspunderea.

În cazul în care operatorul de date nu reușește să demonstreze persoanei vizate într-un caz concret că interesul acestuia prevalează, acest fapt ar putea avea, de asemenea, consecințe mai vaste asupra întregii activități de prelucrare, nu doar în ceea ce privește persoana vizată care a formulat obiecții. În consecință, operatorul poate pune în discuție sau poate decide să reorganizeze prelucrarea, atunci când este adecvat, nu numai pentru persoana vizată în cauză, ci și pentru toate celelalte persoane vizate care pot fi într-o situație similară[112].

Această cerință este necesară, dar nu și suficientă. Pentru a asigura de la început protecția și pentru a evita situația în care inversarea sarcinii probei este eludată[113], este important ca măsurile să fie luate *înainte* de începerea prelucrării, și nu doar în cadrul procedurilor de „opoziție" *ex post*.

Prin urmare, se propune ca, în prima etapă a oricărei activități de prelucrare, operatorul de date să întreprindă mai multe măsuri. Primele două măsuri ar putea să fie menționate într-un considerent din propunerea de regulament, iar a treia, într-o dispoziție specifică:

- efectuarea unei evaluări[114], care ar trebui să cuprindă diferitele etape ale analizei elaborate în prezentul aviz și rezumate în anexa 1. Operatorul ar trebui să identifice în

[112] Pe lângă inversarea sarcinii probei, grupul de lucru susține, de asemenea, faptul că propunerea de regulament nu va mai impune ca o obiecție să se bazeze pe „motive legitime și *imperioase* legate de situația particulară" [a persoanei vizate]. Mai degrabă, în conformitate cu propunerea de regulament, trimiterile la orice motive legitime (nu neapărat „imperioase") legate de situația particulară a persoanei vizate ar fi suficientă. Într-adevăr, o opțiune suplimentară, care a fost propusă în raportul final al Comisiei LIBE, este, de asemenea, să se elimine cerința conform căreia obiecția ar trebui să se refere la situația particulară a persoanei vizate. Grupul de lucru sprijină această abordare în sensul că recomandă ca persoanele vizate să fie în măsură să profite de oricare dintre oportunități sau de ambele, după caz, și anume să se opună fie pe baza propriei lor situații particulare, fie cu un scop general, iar în acest din urmă să nu fie obligate să furnizeze o justificare anume. A se vedea, în acest sens, amendamentul 114 la articolul 19 alineatul (1) din propunerea de regulament din raportul final al Comisiei LIBE.

[113] De exemplu, operatorii de date pot fi tentați să evite demonstrația de la caz la caz a faptului că interesul lor prevalează utilizând formularele de justificare standard sau procedează astfel încât exercitarea dreptului de opoziție să fie greoaie.

[114] Evaluarea, astfel cum s-a precizat anterior la nota de subsol 84, nu ar trebui să fie confundată cu o amplă evaluare a impactului asupra protecției vieții private și a datelor. În prezent, nu există nicio orientare cuprinzătoare privind evaluările impactului efectuate la nivel european, deși în anumite domenii, și anume în ceea ce privește RFID și aparatele de contorizare inteligentă, s-au depus o serie de eforturi salutare pentru a defini o metodologie/un cadru (și/sau un model) sectorial care ar putea fi aplicat în întreaga Uniune Europeană. A se vedea „Propunerea industriei pentru un cadru de evaluare a impactului asupra protecției datelor și a vieții private în cazul aplicațiilor RFID" și „Modelul de evaluare a impactului asupra protecției datelor pentru rețelele inteligente și sistemele de contorizare inteligentă", elaborat de grupul de experți 2 al grupului operativ al Comisiei pentru rețelele inteligente. Grupul de lucru a emis avize repetate cu privire la cele două metodologii.
De asemenea, au existat unele inițiative pentru a defini o metodologie generică de evaluare a impactului asupra protecției datelor, de care ar putea beneficia eforturile „specifice domeniului". A se vedea, de exemplu, proiectul PIAF (Un cadru de evaluare a impactului asupra vieții private pentru drepturile la protecția datelor și la viață privată): http://www.piafproject.eu/.
De asemenea, pentru orientări la nivel național, a se vedea, de exemplu, metodologia CNIL:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

mod explicit interesul (interesele) prevalent(e) în cauză, precum și motivul pentru care acestea prevalează asupra intereselor persoanelor vizate. Evaluarea prealabilă nu ar trebui să fie prea împovărătoare și ar trebui să rămână *scalabilă*: aceasta se poate limita la criterii esențiale în cazul în care impactul prelucrării asupra persoanelor vizate este, la prima vedere, nesemnificativ, dar, pe de altă parte, aceasta ar trebui să fie realizată mai detaliat dacă echilibrul a fost dificil de atins și ar necesita, de exemplu, adoptarea mai multor garanții suplimentare. Dacă este necesar – și anume, în cazul în care o operațiune de prelucrare prezintă riscuri specifice pentru drepturile și libertățile persoanelor vizate – ar trebui să fie efectuată o evaluare mai cuprinzătoare a impactului asupra protecției vieții private și a datelor (în conformitate cu articolul 33 din propunerea de regulament), în cadrul căreia evaluarea în temeiul articolului 7 litera (f) ar putea deveni o parte importantă.

- documentarea evaluării. Așa cum evaluarea este *scalabilă* în ceea ce privește detaliile necesare pentru efectuarea acesteia, tot astfel, și amploarea documentației ar trebui să fie scalabilă. Astfel, unele documente de bază ar trebui să fie disponibile în toate cazurile, în afară de cele mai banale, independent de aprecierea impactului prelucrării asupra persoanei vizate. Pe baza documentelor respective evaluarea operatorului poate fi verificată în continuare și, eventual, contestată;

- asigurarea transparenței și a vizibilității informațiilor privind evaluarea pentru persoanele vizate și alte părți interesate. Transparența ar trebui asigurată atât pentru persoanele vizate, cât și pentru autoritățile de protecție a datelor și, după caz, pentru publicul larg. În ceea ce privește persoanele vizate, grupul de lucru face referire la proiectul de raport al Comisiei LIBE[115], care a prevăzut că operatorul ar trebui să informeze persoana vizată cu privire la motivele pentru care consideră că interesul sau drepturile și libertățile fundamentale ale persoanei vizate nu prevalează asupra interesului său. În opinia grupului de lucru, astfel de informații ar trebui să fie furnizate persoanelor vizate, împreună cu informațiile pe care operatorul trebuie să le furnizeze în temeiul articolelor 10 și 11 din directivă (articolul 11 din propunerea de regulament). Aceasta va permite prezentarea de eventuale obiecții de către persoana vizată, într-o a doua fază, precum și prezentarea, de la caz la caz, de justificări suplimentare ale interesului prevalent din partea operatorului. De asemenea, la cerere, documentele pe care operatorul își întemeiază evaluarea ar trebui să fie puse la dispoziția autorităților pentru protecția datelor, pentru a permite eventuala verificare și aplicare, după caz.

Grupul de lucru ar susține includerea celor trei măsuri în mod explicit în propunerea de regulament în modurile prezentate mai sus. Astfel s-ar recunoaște rolul specific al temeiului juridic în evaluarea legitimității și s-ar clarifica importanța testului comparativ în contextul mai larg al măsurilor privind răspunderea și evaluările impactului în noul cadru legislativ propus.

Manualul de evaluare a impactului asupra vieții private al Biroul Comisarului pentru Informații (ICO) http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

[115] Proiect de raport referitor la propunerea de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor), [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)]

Grupul de lucru consideră că este recomandabil, de asemenea, să se încredințeze Comitetului european pentru protecția datelor misiunea de a oferi orientări suplimentare, acolo unde este necesar, pe baza acestui cadru. O astfel de abordare ar asigura atât o claritate suficientă în textul dispozițiilor, cât și o flexibilitate suficientă în ceea ce privește punerea în aplicare a acestora.

Anexa 1. Ghid succint privind modul de efectuare a testului comparativ prevăzut la articolul 7 litera (f)

Etapa 1: Stabilirea temeiului juridic care se poate aplica în mod potențial, în conformitate cu articolul 7 literele (a)-(f)

Prelucrarea datelor nu poate fi realizată decât în cazul în care se aplică unul sau mai multe dintre cele șase temeiuri – (a)-(f) – de la articolul 7 (temeiuri diferite pot fi invocate în etape diferite ale aceleiași activități de prelucrare). În cazul în care, la prima vedere, pare că articolul 7 litera (f) ar putea fi oportun ca temei juridic, se trece la etapa 2.

Orientări pe scurt:

- articolul 7 litera (a) se aplică numai dacă se acordă consimțământul liber, în cunoștință de cauză, specific și neechivoc; simplul fapt că persoana interesată nu a obiectat la o prelucrare în temeiul articolului 14 nu ar trebui să fie confundat cu consimțământul în baza articolului 7 litera (a) – cu toate acestea, un mecanism simplu de opoziție la o prelucrare poate fi considerat o măsură importantă de protecție în temeiul articolului 7 litera (f);
- articolul 7 litera (b) reglementează prelucrarea care este necesară pentru executarea contractului; simplul fapt că prelucrarea datelor este aferentă contractului sau este stipulată în termenii și condițiile contractului nu înseamnă în mod necesar că se aplică acest temei; după caz, se ia în considerare ca alternativă articolul 7 litera (f);
- articolul 7 litera (c) se referă numai la obligațiile legale clare și specifice în temeiul legislației UE sau a unui stat membru; în cazul unor orientări neobligatorii (de exemplu, cele emise de agenții de reglementare) sau al unei obligații legale străine, se ia în considerare articolul 7 litera (f) ca alternativă.

Etapa 2: Caracterizarea unui interes ca fiind „legitim” sau „nelegitim”

Pentru a fi considerat legitim, un interes trebuie să îndeplinească cumulativ următoarele condiții:

- să fie legal (și anume, în conformitate cu dreptul UE și cu legislația națională);
- să fie suficient de clar articulat pentru a permite efectuarea testului comparativ în raport cu interesul și drepturile fundamentale ale persoanei vizate (și anume, suficient de concret);
- să reprezinte un interes real și actual (și anume, să nu fie speculativ).

Etapa 3: Stabilirea necesității prelucrării pentru realizarea interesului urmărit

Pentru a îndeplini această cerință, analizați dacă există alte mijloace mai puțin invazive pentru a realiza scopul identificat al prelucrării și pentru a servi interesul legitim al operatorului de date.

Etapa 4: Stabilirea unui bilanț provizoriu prin evaluarea faptului dacă drepturile fundamentale sau interesele persoanelor vizate prevalează asupra interesului operatorului de date

- analizați natura interesului operatorului (drept fundamental, alt tip de interes, interes public);
- evaluați posibilele prejudicii suferite de către operator, de către terți sau de către comunitatea mai largă în cazul în care prelucrarea datelor nu are loc;
- luați în considerare natura datelor (sensibile într-un sens strict sau într-un sens mai larg?);

- analizați statutul persoanelor vizate (minor, salariat etc.) și al operatorului (de exemplu, dacă o societate comercială se află într-o poziție dominantă pe piață);
- examinați modul în care sunt prelucrate datele (la scară mare, extragerea de date, elaborarea de profiluri, divulgarea către un număr mare de persoane sau publicare);
- identificați interesul și/sau drepturile fundamentale ale persoanei vizate care ar putea fi afectate;
- analizați așteptările rezonabile ale persoanelor vizate;
- evaluați impactul asupra persoanei vizate și comparați cu beneficiul preconizat obținut din prelucrare de către operatorul de date.

Orientare succintă: Analizați efectul prelucrării concrete asupra persoanelor reale – nu priviți evaluarea ca pe un exercițiu pur ipotetic sau abstract.

Etapa 5: Stabilirea echilibrului final, luând în considerare garanțiile suplimentare

Identificați și puneți în aplicare garanții suplimentare care rezultă din obligația de prudență și diligență, precum:
- minimizarea datelor (de exemplu, limite stricte privind colectarea datelor sau ștergerea imediată a datelor după utilizare)
- măsuri tehnice și organizatorice pentru a se asigura că datele nu pot fi folosite pentru a lua decizii sau pentru a întreprinde alte acțiuni cu privire la persoane („separarea funcțională")
- utilizarea extinsă a tehnicilor de anonimizare, agregarea datelor, tehnologiile menite să sporească protecția vieții private, protejarea vieții private din faza de concepție, evaluări ale impactului asupra protecției datelor și a vieții private;
- creșterea transparenței, un drept general și necondiționat de opoziție (opt-out), portabilitatea datelor și măsurile conexe pentru sprijinirea persoanelor vizate.

Orientare succintă: Utilizarea abordărilor și a tehnologiilor menite să sporească protecția vieții private poate înclina balanța în favoarea operatorului de date și poate proteja, de asemenea, persoanele în cauză.

Etapa 6: Demonstrarea conformității și asigurarea transparenței

- elaborați un plan al etapelor 1-5 pentru a justifica prelucrarea înainte de inițierea acesteia;
- informați persoana vizată cu privire la motivele pentru care se consideră că echilibrul înclină în favoarea operatorului;
- păstrați documentația la dispoziția autorităților pentru protecția datelor.

Orientare succintă: Această etapă este *scalabilă*: detaliile evaluării și documentația ar trebui să fie adaptate la natura și contextul prelucrării. Măsurile vor fi mai ample în cazul în care se prelucrează o mare cantitate de informații despre numeroase persoane, într-o manieră care ar putea avea un impact semnificativ asupra acestora. O evaluare cuprinzătoare a impactului asupra protecției vieții private și a datelor (în conformitate cu articolul 33 din propunerea de regulament) va fi necesară numai în cazul în care o operațiune de prelucrare prezintă riscuri specifice pentru drepturile și libertățile persoanelor vizate. În astfel de cazuri, evaluarea în temeiul articolului 7 litera (f) ar putea deveni o parte esențială din evaluarea mai extinsă a impactului.

Etapa 7: Ce se întâmplă în cazul în care persoana vizată își exercită dreptul de opoziție?

- în cazul în care este disponibil numai un drept condiționat de excludere voluntară ca garanție [acest lucru este prevăzut în mod explicit în temeiul articolului 14 litera (a), ca o garanție minimă]: dacă persoana vizată se opune prelucrării, trebuie să se garanteze faptul că există un mecanism adecvat și ușor de utilizat care să reevalueze echilibrul pentru persoana în cauză și să se înceteze prelucrarea datelor sale în cazul în care reevaluarea arată că interesul său prevalează;
- în cazul în care se furnizează un drept necondiționat de excluderea voluntară ca garanție suplimentară [fie pentru că acest lucru este prevăzut în mod explicit în temeiul articolului 14 litera (b), fie deoarece aceasta este considerată a fi o garanție necesară sau utilă suplimentară]: dacă persoana vizată se opune prelucrării, trebuie să se garanteze faptul că opțiunea acesteia este respectată, fără necesitatea de a lua alte măsuri suplimentare sau de a efectua o evaluare.

Anexa 2. Exemple practice pentru a ilustra aplicarea testului comparativ prevăzut la articolul 7 litera (f)

Prezenta anexă oferă exemple cu privire la unele dintre cele mai comune situații în care poate surveni chestiunea interesului legitim în sensul articolului 7 litera (f). În majoritatea cazurilor, am grupat două sau mai multe exemple care merită să fie comparate într-o singură rubrică. O mare parte dintre exemple se bazează pe cazuri reale sau elemente ale unor cazuri reale soluționate de autoritățile pentru protecția datelor din diferite state membre. Cu toate acestea, uneori am modificat faptele într-o anumită măsură pentru a ilustra mai bine modul de efectuare a testului comparativ.

Exemplele sunt incluse pentru a ilustra *procesul logic* – metoda care urmează să fie utilizată la efectuarea testului comparativ utilizând mai mulți factori. Cu alte cuvinte, exemplele *nu* sunt menite să ofere o evaluare *definitivă* a cazurilor descrise. Într-adevăr, în multe cazuri, prin modificarea faptelor într-un anumit mod (de exemplu, dacă operatorul ar adopta măsuri suplimentare de protecție, cum ar fi o anonimizare mai completă, măsuri de securitate mai bune și mai multă transparență și opțiuni mai reale pentru persoanele vizate), rezultatul testului comparativ s-ar putea schimba[116].

Acest lucru ar trebui să încurajeze operatorii să respecte toate dispozițiile orizontale ale directivei și să ofere protecție suplimentară, acolo unde este cazul, pe baza protecției datelor și a vieții private din faza de concepție. Cu cât operatorii au mai mare grijă să protejeze datele cu caracter personal în general, cu atât este mai probabil ca aceștia să îndeplinească cerințele testului comparativ.

Exercitarea dreptului la libertatea de exprimare și de informare[117], inclusiv în mass-media și artă

Exemplul 1: Un ONG efectuează republicarea cheltuielilor membrilor Parlamentului

O autoritate publică – în temeiul unei obligații legale [articolul 7 litera (c)] – face publice cheltuielile membrilor Parlamentului; la rândul său, un ONG din domeniul transparenței analizează și efectuează republicarea datelor într-o versiune adnotată corectă, proporțională, dar cu o valoare informațională mai mare, contribuind la un nivel mai mare de transparență și de răspundere.

Presupunând că ONG-ul efectuează republicarea și adnotarea în mod exact și proporțional, adoptă măsuri adecvate de protecție și, la nivel general, respectă drepturile persoanelor vizate, ar trebui ca acesta să se poată baza pe articolul 7 litera (f) ca temei juridic pentru prelucrare. Factori precum natura interesului legitim (un drept fundamental la libertatea de exprimare și

[116] Aplicarea corectă a articolului 7 litera (f) poate ridica probleme complexe de evaluare, iar pentru a contribui la orientarea evaluării, o legislație specifică, jurisprudența, orientările, precum și codurile de conduită și alte standarde formale sau mai puțin formale pot toate să joace un rol important.

[117] În ceea ce privește libertatea de exprimare și de informare, a se vedea pagina 34 din prezentul aviz. Eventualele derogări relevante în temeiul legislației naționale în cazul prelucrării datelor în scopuri jurnalistice în baza articolului 9 din directivă trebuie să fie, de asemenea, luate în considerare atunci când se evaluează exemplele.

de informare), interesul publicului în ceea ce privește transparența și răspunderea, precum și faptul că datele au fost deja publicate și privesc date cu caracter personal (relativ mai puțin sensibile) referitoare la activități ale persoanelor care sunt relevante pentru exercitarea funcțiilor publice[118], toate cântăresc în favoarea legitimității prelucrării. Faptul că publicarea inițială a fost prevăzută de lege și că, prin urmare, persoanele ar trebui să se aștepte ca datele lor să fie publicate contribuie, de asemenea, la evaluarea favorabilă. Pe de altă parte, impactul asupra persoanei poate fi semnificativ, de exemplu, din cauza controlului public, integritatea personală a unor persoane poate fi pusă sub semnul întrebării, iar acest lucru poate conduce, de exemplu, la pierderea alegerilor sau, în unele cazuri, la o anchetă penală pentru activități frauduloase. Factorii de mai sus luați împreună arată, cu toate acestea, că pe ansamblu interesul operatorului (și interesul publicului căruia îi sunt comunicate datele) prevalează asupra interesului persoanelor vizate.

Exemplul 2: Un consilier local o numește pe fiica sa în funcția de asistent special

Un jurnalist publică într-un ziar online local un articol corect din punct de vedere factual și bine documentat despre un consilier local în care dezvăluie faptul că acesta a participat numai la una dintre ultimele unsprezece reuniuni ale consiliului și este puțin probabil să fie reales din cauza unui scandal recent cauzat de numirea fiicei sale în vârstă de șaptesprezece ani în funcția de asistent special.

O analiză similară celei din *exemplul 1* se aplică, de asemenea, în acest caz. Pe baza datelor, este în interesul legitim al ziarului în cauză să publice informațiile. Chiar dacă s-au dezvăluit date cu caracter personal referitoare la consilier, dreptul la viața privată al consilierului nu prevalează asupra dreptului fundamental la libertatea de exprimare prin publicarea știrii în ziar. Acest lucru se datorează faptului că drepturile la viață privată ale personalităților publice sunt relativ limitate în ceea ce privește activitățile lor publice, precum și importanței deosebite a libertății de exprimare – în special în ceea ce privește publicarea unei știri care este de interes public.

Exemplul 3: Primele rezultate ale căutării continuă să arate infracțiuni minore

Arhiva online a unui ziar conține un articol vechi despre o persoană, odinioară o celebritate pe plan local, căpitan al echipei de fotbal amator dintr-un oraș mic. Persoana este identificată cu numele complet și știrea se referă la implicarea sa într-o procedură penală relativ minoră (persoana respectivă se afla în stare de ebrietate și tulburase ordinea publică). Acum persoana în cauză nu mai are cazier judiciar, întrucât infracțiunea pentru care a ispășit o pedeapsă cu mai mulți ani în urmă a fost radiată. Ceea ce este cel mai îngrijorător pentru persoana în cauză este că, atunci când își caută numele pe motoarele de căutare online, printre primele rezultate care îl privesc apare link-ul către această știre veche. În pofida cererii sale, ziarul refuză să adopte măsuri tehnice care ar restrânge disponibilitatea mai largă a știrii referitoare la persoana vizată. De exemplu, ziarul refuză să adopte măsuri tehnice și organizatorice care ar avea ca scop – în măsura în care tehnologia permite – limitarea accesului la informații din

[118] Nu poate fi exclus că unele cheltuieli pot dezvălui date mai sensibile, cum ar fi date privind sănătatea. Într-un astfel de caz, acestea ar trebui să fie editate din setul de date înainte ca acesta să fie publicat inițial. Este o bună practică să se adopte o abordare „proactivă” și să se ofere persoanelor posibilitatea de a-și revizui datele înainte de publicarea lor, informându-le în mod clar despre posibilitățile și modalitățile de publicare.

motoarele de căutare externe atunci când se utilizează numele persoanei ca o categorie de căutare.

Acesta este un alt caz care ilustrează posibilul conflict dintre libertatea de exprimare și dreptul la viața privată. Exemplul arată, de asemenea, că, în unele cazuri, garanțiile suplimentare – cum ar fi asigurarea faptului că, cel puțin în cazul unei obiecții justificate în temeiul articolului 14 litera (a) din directivă, partea relevantă din arhivele ziarului nu va mai fi accesibilă prin motoarele de căutare externe sau formatul folosit pentru afișarea informațiilor nu va mai permite căutarea după nume – pot juca un rol esențial în stabilirea unui echilibru adecvat între cele două drepturi fundamentale în cauză, fără a aduce atingere oricăror alte măsuri care ar putea fi luate de către motoarele de căutare sau alte părți terțe[119].

Marketingul direct convențional și alte forme de marketing sau publicitate

Exemplul 4: Un magazin de computere face reclamă unor produse similare pentru clienți

Un magazin de computere obține și stochează de la clienții săi datele de contact ale acestora în contextul vânzării unui produs și folosește datele de contact respective pentru promovarea prin poștă obișnuită a propriilor produse similare. De asemenea, magazinul comercializează produse online și trimite email-uri promoționale atunci când o nouă serie de produse intră în stoc. Clienții sunt informați clar cu privire la posibilitatea de opoziție, în mod gratuit și cu ușurință, atunci când le sunt colectate datele de contact, precum și de fiecare dată când este trimis un mesaj, în cazul în care clientul nu a obiectat inițial.

Transparența prelucrării, faptul că un consumator se poate aștepta în mod rezonabil să primească oferte pentru produse similare în calitate de client al magazinului și faptul că acesta are dreptul de opoziție contribuie la consolidarea legitimității prelucrării și la protejarea drepturilor persoanelor. Pe de altă parte, nu pare să existe niciun impact disproporționat asupra dreptului persoanei la viață privată [în acest exemplu, se presupune că nu există profiluri informatice complexe create de magazin pentru clienții săi, de exemplu, utilizând analiza detaliată a datelor din istoricul de navigare („click-stream")].

Exemplul 5: O farmacie online desfășoară ample acțiuni de creare de profiluri

O farmacie online desfășoară activități de marketing pe baza medicamentelor și a altor produse achiziționate de clienți, inclusiv produsele obținute pe bază de rețetă medicală. Aceasta analizează informațiile respective – combinate cu informații demografice despre clienți – de exemplu, vârstă și sex – pentru a crea un profil privind „sănătatea și bunăstarea" fiecărui client. De asemenea, sunt utilizate datele din istoricul de navigare, care sunt colectate nu numai pentru produsele cumpărate de clienți, ci și pentru alte produse și informații pe care aceștia le-au căutat pe site-ul de internet. Profilurile clienților includ informații sau predicții care sugerează că o anumită clientă este însărcinată, suferă de o anumită boală cronică sau ar fi interesată să achiziționeze suplimente alimentare, loțiune de bronzat sau alte produse de îngrijire a pielii în anumite perioade ale anului. Analiștii farmaciei online utilizează astfel de informații pentru a oferi medicamente care nu necesită rețetă, suplimente de sănătate și alte

[119] A se vedea, de asemenea, cauza C-131/12 Google Spania/ Agencia Española de Proteccion de Datos, în prezent pe rolul Curții de Justiție a Uniunii Europene.

produse anumitor persoane, prin e-mail. În acest caz, farmacia nu se poate baza pe interesul său legitim atunci când creează și utilizează profiluri ale clienților săi în scopuri de marketing. Există o serie de probleme ridicate de crearea de profiluri descrisă în acest caz. Informațiile sunt deosebit de sensibile și pot divulga multe date despre aspecte cu privire la care multe persoane se așteaptă să rămână confidențiale[120]. Măsura și modalitatea creării de profiluri (utilizarea datelor din istoricul de navigare, algoritmi de predicție) sugerează, de asemenea, un nivel ridicat de ingerință. Consimțământul pe baza articolului 7 litera (a) și a articolului 8 alineatul (2) litera (a) (atunci când sunt implicate date sensibile) ar putea, cu toate acestea, să fie considerat o alternativă, dacă este cazul.

Mesajele necomerciale nesolicitate, inclusiv pentru campanii politice sau strângerea de fonduri caritabile

Exemplul 6: Un candidat la alegerile locale utilizează în mod direcționat registrul electoral

Un candidat la alegerile locale utilizează registrul electoral[121] pentru a trimite o scrisoare de prezentare, în scopul de a-și promova campania pentru viitoarele alegeri, fiecărui alegător potențial din circumscripția sa electorală. Candidatul utilizează datele obținute din registrul electoral numai ca să trimită scrisoarea și nu păstrează datele după încheierea campaniei.

O astfel de utilizare a registrului local se încadrează în sfera așteptărilor rezonabile ale persoanelor vizate, atunci când aceasta are loc în perioada preelectorală: interesul operatorului este clar și legitim. Utilizarea limitată și cu un obiectiv bine stabilit a informațiilor contribuie, de asemenea, la înclinarea balanței în favoarea interesului legitim al operatorului. O astfel de utilizare a registrelor electorale poate fi, de asemenea, reglementată prin lege la nivel național, din punct de vedere al interesului public, cu stipularea unor reguli, limitări și garanții specifice privind utilizarea registrului electoral. În acest caz, trebuie să se asigure respectarea unor astfel de norme specifice pentru a garanta legitimitatea prelucrării.

Exemplul 7: O organizație non-profit colectează informații în scopuri de direcționare

O organizație filozofică dedicată dezvoltării umane și sociale decide să organizeze activități de colectare de fonduri pe baza profilului membrilor săi. În acest scop, aceasta colectează date de pe site-urile de socializare prin intermediul unor programe ad-hoc care vizează persoanele care au apreciat („like") pagina organizației, au apreciat sau au împărtășit („share") mesajele organizației afișate pe pagină, au vizionat regulat anumite elemente sau au retransmis („re-tweet") la mesajele organizației. Ulterior aceasta trimite mesaje și buletine informative membrilor săi, în funcție de profilurile lor. De exemplu, persoanele în vârstă care dețin un câine și care au apreciat articole referitoare la adăposturile pentru animale primesc diferite de apeluri de strângere de fonduri de la familii cu copii mici; persoane din grupuri etnice diferite primesc, de asemenea, mesaje diferite.

[120] Dincolo de orice restricții impuse de legislația în materie de protecție a datelor, publicitatea pentru medicamentele eliberate pe bază de rețetă medicală este, de asemenea, strict reglementată în UE și există, de asemenea, o serie de restricții privind publicitatea pentru medicamentele eliberate fără rețetă. În plus, trebuie luate în considerare cerințele prevăzute la articolul 8 cu privire la categoriile speciale de date (cum ar fi datele privind sănătatea).

[121] Se presupune că în statul membru în care se aplică exemplul este stabilit prin lege un registru electoral.

Faptul că sunt prelucrate categorii speciale de date (convingeri filozofice) necesită conformitatea cu articolul 8, o condiție care pare să fie îndeplinită deoarece prelucrarea are loc în cadrul activităților legitime ale organizației. Totuși, în cazul de față, aceasta nu este o condiție suficientă: modul în care sunt utilizate datele depășește așteptările rezonabile ale persoanelor. Volumul de date colectate, lipsa de transparență privind colectarea și reutilizarea datelor publicate inițial pentru un anumit scop în alt scop contribuie la concluzia că, în cazul de față, nu poate fi invocat articolul 7 litera (f). Prin urmare, nu ar trebui să se permită prelucrarea, cu excepția cazului în care se poate utiliza un alt temei, de exemplu, consimțământul persoanelor acordat în temeiul articolului 7 litera (a).

Executarea unor creanțe legale, inclusiv recuperarea datoriilor prin proceduri necontencioase

Exemplul 8: Litigiu privind calitatea lucrărilor de renovare

Un client contestă calitatea lucrărilor de renovare a bucătăriei și refuză să plătească prețul întreg. Societatea de construcții transferă date relevante și proporționale avocatului acesteia, pentru că acesta să-i poată reaminti clientului de plata datorată și să negocieze un acord cu clientul în cazul în care acesta continuă să refuze să plătească.

În acest caz, primele măsuri întreprinse de societatea de construcții utilizând informațiile de bază ale persoanei vizate (de exemplu, nume, adresă, datele de referință ale contractului), constând în a trimite o scrisoare de atenționare persoanei vizate (direct sau prin intermediul avocatului, astfel cum s-a întâmplat în acest caz), pot intra sub incidența prelucrării necesare pentru executarea contractului [articolul 7 litera b)]. Măsurile suplimentare luate[122], inclusiv implicarea unei firme de recuperare a datoriilor, trebuie însă să fie evaluate în temeiul articolului 7 litera (f), având în vedere, printre altele, gradul de ingerință al acestora și impactul asupra persoanei vizate, astfel cum se arată în exemplul următor.

Exemplul 9: Clientul dispare cu un autoturism achiziționat pe credit

Un client nu plătește ratele scadente pentru o mașină sport costisitoare achiziționată pe credit și apoi „dispare”. Distribuitorul auto semnează un contract cu un „agent de recuperare a datoriilor” terț. Agentul de recuperare a datoriilor desfășoară o anchetă intruzivă „în stilul aplicării legii”, utilizând, printre altele, practici precum supravegherea video discretă și urmărirea convorbirilor telefonice.

Cu toate că interesele distribuitorului auto și ale agentului de recuperare a datoriilor sunt legitime, balanța echilibrului nu se înclină în favoarea acestora din cauza metodelor invazive utilizate pentru a colecta informații, unele dintre acestea fiind explicit interzise prin lege (urmărirea convorbirilor telefonice). Concluzia ar fi diferită în cazul în care, de exemplu, distribuitorul auto și agentul de recuperare a datoriilor ar realiza numai verificări limitate pentru a confirma datele de contact ale persoanei vizate în scopul de a intenta o acțiune în instanță.

[122] În prezent, între diferitele state membre există un grad de variație în ceea ce privește măsurile care pot fi considerate necesare pentru executarea unui contract.

Prevenirea fraudei, a utilizării abuzive a serviciilor sau a spălării de bani

Exemplul 10: Verificarea datelor clienților înainte de deschiderea unui cont bancar

O instituție financiară utilizează proceduri rezonabile și proporționale – în conformitate cu orientările cu caracter neobligatoriu ale autorității guvernamentale competente de supraveghere financiară – pentru a verifica identitatea oricărei persoane care dorește să deschidă un cont. Aceasta păstrează evidența informațiilor utilizate pentru a verifica identitatea persoanei în cauză.

Interesul operatorului este legitim, prelucrarea datelor implică doar informațiile necesare limitate (o practică standard în sectorul său de activitate și care ar trebui să fie așteptată, în mod rezonabil, de către persoanele vizate și recomandată de autoritățile competente). Au fost instituite garanții corespunzătoare pentru a limita orice impact nejustificat și disproporționat asupra persoanelor vizate. Prin urmare, operatorul poate invoca articolul 7 litera (f). Alternativ și în măsura în care acțiunile întreprinse sunt impuse în mod specific de legislația aplicabilă, s-ar putea aplica articolul 7 litera (c).

Exemplul 11: Schimbul de informații pentru combaterea spălării banilor

O instituție financiară – după obținerea avizului autorității competente pentru protecția datelor – pune în aplicare proceduri bazate pe criterii specifice și limitate pentru a face schimb de date cu privire la suspiciuni de abuz al normelor privind combaterea spălării banilor cu alte societăți din cadrul aceluiași grup, cu limitare strictă privind accesul, securitatea și interzicerea oricărei alte utilizări ulterioare în alte scopuri.

Din motive similare celor explicate mai sus și în funcție de faptele în speță, prelucrarea datelor s-ar putea baza pe articolul 7 litera (f). Alternativ și în măsura în care acțiunile întreprinse sunt impuse în mod specific de legislația aplicabilă, s-ar putea aplica articolul 7 litera (c).

Exemplul 12: Lista neagră a persoanelor agresive dependente de droguri

Un grup de spitale creează o listă neagră comună a persoanelor „agresive” în căutare de droguri, cu scopul de a le interzice accesul în toate incintele medicale ale spitalelor participante.

Chiar dacă interesul operatorilor în menținerea incintelor în condiții de siguranță și securitate este legitim, acesta trebuie să fie pus în balanță cu dreptul fundamental la viață privată și cu alte preocupări întemeiate, cum ar fi necesitatea de a nu exclude persoanele vizate de la accesul la tratament medical. Faptul că sunt prelucrate date sensibile (de exemplu, date privind sănătatea legate de dependența de droguri) sprijină, de asemenea, concluzia că, în acest caz, este puțin probabil ca prelucrarea să fie acceptabilă în temeiul articolului 7 litera (f)[123]. Prelucrarea ar putea fi acceptabilă dacă aceasta ar fi, de exemplu, reglementată de o lege care prevede garanții specifice (verificări și controale, transparență, prevenirea

[123] De asemenea, trebuie să se ia în considerare cerințele prevăzute la articolul 8 cu privire la categoriile speciale de date (cum ar fi datele privind sănătatea).

deciziilor automatizate), asigurându-se că aceasta nu ar conduce la discriminare sau încălcarea drepturilor fundamentale ale persoanelor[124]. Într-un astfel de caz, în funcție de faptul dacă legea specială impune sau doar permite prelucrarea, poate fi invocat ca temei juridic articolul 7 litera (c) sau articolul 7 litera (f).

Monitorizarea angajaților în scopuri de asigurare a siguranței sau de gestionare

Exemplul 13: Orele de lucru ale avocaților sunt utilizate atât pentru facturare, cât și pentru stabilirea primelor

Numărul de ore comisionabile lucrate de către avocați la o firmă de avocatură este prelucrat atât pentru facturarea serviciilor, cât și pentru stabilirea primelor anuale. Sistemul este explicat în mod transparent angajaților, care au un drept explicit de a-și exprima dezacordul față de concluziile în ceea ce privește atât facturarea, cât și plata primelor, care trebuie să fie discutat ulterior cu personalul de conducere.

Prelucrarea pare necesară pentru realizarea interesului legitim al operatorului și nu pare să existe o modalitate mai puțin intruzivă pentru atingerea acestui scop. Impactul asupra angajaților este, de asemenea, limitat, datorită garanțiilor și procedurilor existente. Prin urmare, articolul 7 litera (f) ar putea constitui un temei juridic adecvat în acest caz. În plus, s-ar putea argumenta că prelucrarea datelor pentru unul sau ambele scopuri este necesară, de asemenea, pentru executarea contractului.

Exemplul 14: Monitorizarea electronică a utilizării internetului[125]

Angajatorul monitorizează utilizarea internetului de către angajați în timpul orelor de lucru pentru a verifica dacă aceștia nu utilizează în mod excesiv resursele de tehnologia informației ale întreprinderii în scopuri personale. Datele colectate includ fișiere temporare și cookie-urile generate de calculatoarele angajaților, care arată site-urile de internet vizitate și descărcările efectuate în timpul programului de lucru. Datele sunt prelucrate fără consultarea prealabilă a persoanelor vizate și a reprezentanților sindicatului întreprinderii/comitetului de întreprindere. De asemenea, informațiile furnizate persoanelor vizate cu privire la practicile respective sunt insuficiente.

Cantitatea și natura datelor colectate reprezintă o intruziune importantă în viața privată a angajaților. Pe lângă aspecte privind proporționalitatea, transparența cu privire la practici, strâns legată de așteptările rezonabile ale persoanelor vizate, reprezintă, de asemenea, un factor important care trebuie luat în considerare. Chiar dacă angajatorul are un interes legitim să limiteze timpul petrecut de angajați vizitând site-uri care nu sunt direct relevante pentru munca lor, metodele utilizate nu respectă testul comparativ prevăzut la articolul 7 litera (f). Angajatorul ar trebui să utilizeze metode mai puțin intruzive (de exemplu, limitarea

[124] A se vedea documentul de lucru privind listele negre (WP65), adoptat la 3 octombrie 2002.

[125] Unele state membre consideră că o monitorizare electronică limitată poate fi „necesară pentru executarea unui contract” și, prin urmare, se poate baza pe temeiul juridic de la articolul 7 litera (b), mai degrabă decât pe cel de la articolul 7 litera (f).

accesibilității anumitor site-uri), care, conform celor mai bune practici, sunt discutate și convenite cu reprezentanții angajaților și comunicate angajaților în mod transparent.

Sistemele de denunțare

Exemplul 15: Sistem de denunțare pentru respectarea unor obligații legale străine

O sucursală UE a unui grup american stabilește un sistem de denunțare limitat pentru raportarea încălcărilor grave din domeniul contabilității și finanțelor. Entitățile grupului sunt supuse unui cod de bună guvernanță care solicită o consolidare a procedurilor de control intern și de gestionare a riscurilor. Din cauza activităților sale internaționale, sucursala UE trebuie să furnizeze date financiare fiabile altor membrii ai grupului din SUA. Sistemul este conceput pentru a fi în conformitate cu legislația americană și cu orientările furnizate de autoritățile naționale pentru protecția datelor din UE.

Printre garanții, angajaților li se oferă orientări clare privind circumstanțele în care sistemul ar trebui să fie utilizat, prin sesiuni de formare și alte mijloace. Personalul este avertizat să nu abuzeze de sistem – de exemplu, prin afirmații false sau nefondate împotriva altor membri ai personalului. Acestora li se explică, de asemenea, că, în cazul în care preferă, pot utiliza sistemul în mod anonim sau, dacă doresc, își pot declara identitatea. În cel din urmă caz, angajații sunt informați cu privire la circumstanțele în care datele care permit identificarea acestora vor fi comunicate angajatorului sau transmise către alte agenții.

În cazul în care sistemul ar trebui să fie stabilit în conformitate cu dreptul UE sau cu dreptul unui stat membru al UE, prelucrarea s-ar putea baza pe articolul 7 litera (c). Cu toate acestea, obligațiile juridice străine nu se califică drept o obligație legală în sensul articolului 7 litera (c) și, prin urmare, o astfel de obligație nu ar putea justifica prelucrarea în conformitate cu articolul 7 litera (c). Cu toate acestea, prelucrarea s-ar putea baza pe articolul 7 litera (f), de exemplu, în cazul în care există un interes legitim pentru garantarea stabilității piețelor financiare sau lupta împotriva corupției și cu condiția ca sistemul să includă suficiente garanții, în conformitate cu orientările furnizate de autoritățile de reglementare relevante din UE.

Exemplul 16: Sistem de denunțare intern fără existența unor proceduri coerente

O societate de servicii financiare decide să instituie un sistem de denunțare deoarece suspectează furtul pe scară largă și fapte de corupție în rândul personalului său și dorește să încurajeze angajații să ofere informații unii despre alții. Pentru a face economii, societatea decide să opereze sistemul la nivel intern, utilizând personal format din membri ai departamentului de resurse umane. Pentru a încuraja angajații să utilizeze sistemul, societatea oferă o recompensă în bani „fără a adresa nicio întrebare” angajaților ale căror activități de denunțare conduc la identificarea unui comportament inadecvat și la recuperarea de sume de bani.

Societatea are un interes legitim în detectarea și prevenirea furtului și a corupției. Cu toate acestea, sistemul său de denunțare este atât de prost conceput și cu puține garanții, încât interesul său prejudiciază atât interesele, cât și dreptul la viață privată al angajaților, în special cei care pot fi victimele unor rapoarte false depuse exclusiv în scopuri de câștig financiar. Faptul că sistemul este operat la nivel intern mai degrabă decât în mod independent reprezintă o altă problemă, la fel ca și lipsa de formare și de orientări pentru utilizarea sistemului.

Securitatea fizică, securitatea informatică și a rețelelor

Exemplul 17: Controale biometrice într-un laborator de cercetare

Un laborator de cercetare științifică care lucrează cu virusuri letale utilizează un sistem de intrare biometric din cauza riscului important pentru sănătatea publică în cazul în care virusurile ar scăpa din incintă. Se aplică garanțiile corespunzătoare, inclusiv faptul că datele biometrice sunt stocate pe cardurile personale ale angajaților și nu într-un sistem centralizat.

Chiar dacă datele sunt sensibile în sens larg, motivul pentru prelucrarea lor este în interesul public. Acest aspect, precum și faptul că riscurile de abuz sunt reduse prin utilizarea adecvată de garanții fac articolul 7 litera (f) o bază adecvată pentru prelucrare.

Exemplul 18: Camere de luat vederi ascunse pentru a identifica vizitatorii și angajații care fumează

O întreprindere utilizează camere de luat vederi ascunse pentru a identifica angajații și vizitatorii care fumează în zone neautorizate ale clădirii.

Deși operatorul are un interes legitim pentru a asigura conformitatea cu normele pentru nefumători, mijloacele utilizate pentru atingerea acestui scop sunt – în general – disproporționate și nejustificat de invazive. Există metode mai puțin intruzive și mai transparente (de exemplu, detectoare de fum și semne vizibile). Prin urmare, prelucrarea nu respectă dispozițiile articolului 6, care prevede ca datele să fie „neexcesive” în ceea ce privește scopurile în care sunt colectate sau prelucrate ulterior. În același timp, aceasta nu va satisface probabil testul comparativ prevăzut la articolul 7.

Cercetarea științifică

Exemplul 19: Cercetări privind efectele divorțului și ale șomajului părinților asupra educației copiilor

În cadrul unui program de cercetare adoptat de guvern și autorizat de un comitet de etică relevant, se efectuează un studiu privind relația dintre divorț, șomajul părinților și nivelul de educație al copiilor. Deși acestea nu sunt clasificate drept „categorii speciale de date”, cercetarea se concentrează, cu toate acestea, asupra unor aspecte care pentru multe familii ar fi considerate informații cu caracter personal extrem de intime. Cercetarea va permite orientarea asistenței educaționale speciale către copii care, în caz contrar, ar putea să absenteze, să aibă un nivel redus de educație, să intre în rândul șomerilor și al infractorilor ca adulți. Legislația statului membru în cauză permite în mod explicit prelucrarea datelor cu caracter personal (altele decât categoriile speciale de date) în scopuri de cercetare, cu condiția ca activitățile de cercetare să fie necesare pentru protejarea intereselor publice importante și să fie efectuate sub rezerva unor garanții adecvate, care sunt ulterior detaliate în continuare în legislația de punere în aplicare. Cadrul juridic include cerințe specifice, dar și un cadru privind răspunderea care permite o evaluare de la caz la caz a autorizării cercetării (în cazul în care aceasta a fost efectuată fără consimțământul persoanelor în cauză) și măsurile specifice care trebuie aplicate pentru protecția persoanelor vizate.

Cercetătorul dispune de o infrastructură de cercetare sigură și informațiile relevante îi sunt furnizate, în condiții de securitate, de registrele de evidență a populației, instanțe, agențiile de șomaj și școli. Centrul de cercetare „taie" identitatea persoanelor, astfel încât documentele de divorț, șomaj și educație pot fi corelate, dar fără a dezvălui identitatea „civică" a persoanelor – de exemplu, numele și adresele acestora. În continuare, toate datele originale sunt șterse în mod iremediabil. De asemenea, se iau măsuri suplimentare pentru a asigura separarea funcțională (și anume, faptul că datele vor fi utilizate doar în scopuri de cercetare) și pentru a reduce orice risc de reidentificare.

Membrii personalului care lucrează la centrul de cercetare beneficiază de formare riguroasă în materie de securitate și sunt personal răspunzători – eventual chiar penal – pentru orice încălcare a securității de care sunt responsabili. Sunt luate măsuri tehnice și organizatorice, de exemplu pentru a se asigura că membrii personalului care utilizează stick-urile de memorie USB nu pot lua date cu caracter personal în afara centrului.

Este în interesul legitim al centrul de cercetare să desfășoare activitatea de cercetare, pentru care există un interes public major. De asemenea, aceasta este în interesul legitim al ocupării forței de muncă, al educației și al altor organisme implicate în sistem, întrucât rezultatele le vor permite să planifice și să ofere servicii persoanelor care au cel mai mult nevoie de acestea. Aspectele privind viața privată ale sistemului au fost bine concepute și garanțiile care sunt instituite asigură că interesele legitime ale organizațiilor implicate în realizarea cercetării nu sunt depășite de interesele sau drepturile privind viață privată ale părinților sau ale copiilor ale căror evidențe constituie baza cercetării.

Exemplul 20: Studiu de cercetare privind obezitatea

O universitate dorește să desfășoare activități de cercetare privind nivelurile de obezitate infantilă în mai multe orașe și comunități rurale. Deși, în general, aceasta a avut dificultăți în ceea ce privește accesul la datele relevante de la școli și alte instituții, universitatea a reușit să convingă câteva zeci de cadre didactice să monitorizeze pentru o perioadă de timp copiii din clasele lor care suferă de obezitate și să le adreseze întrebări despre alimentația lor, nivelurile de activitate fizică, nivelul de utilizare a jocurilor de calculator și așa mai departe. Cadrele didactice au notat, de asemenea, numele și adresele copiii intervievați, astfel încât să li se poată trimite un cupon pentru achiziționarea de muzică online ca recompensă pentru participarea la cercetare. Ulterior, cercetătorii au alcătuit o bază de date a copiilor, corelând nivelurile obezității cu activitatea fizică și alți factori. Exemplarele pe suport de hârtie ale chestionarelor completate – aflate încă într-o formă care identifică fiecare copil – sunt păstrate în arhivele universității pe o perioadă nedeterminată de timp și fără măsuri adecvate de securitate. Fotocopii ale tuturor chestionarelor sunt transmise, la cerere, oricărui student la medicină sau doctorand de la aceeași universitate sau de la universități partenere din întreaga lume care sunt interesate de utilizarea ulterioară a datelor de cercetare.

Deși este în interesul legitim al universității să efectueze cercetarea, există mai multe aspecte ale proiectului de cercetare care determină ca interesele sau drepturile la viață privată ale copiilor să prevaleze asupra acestui interes. Pe lângă metodologia de cercetare, care este lipsită de rigoare științifică, problema rezultă, în special, din absența din proiectul de cercetare a unor abordări care să sporească protecția vieții private, precum și din accesul larg la datele cu caracter personal colectate. Evidențele privind copiii nu sunt în niciun moment codificate sau anonimizate și nu s-au luat alte măsuri care să asigure securitatea datelor sau separarea funcțională. De asemenea, nu s-a obținut consimțământul valabil prevăzut la articolul 7

litera (a) și la articolul 8 alineatul (2) litera (a) și nu este clar dacă li s-a explicat copiilor sau părinților pentru ce vor fi utilizate datele lor cu caracter personal sau cu cine vor fi partajate acestea.

Obligație legală străină

Exemplul 21: Respectarea cerințelor dreptului fiscal al unei țări terțe

Băncile din UE colectează și transferă anumite date ale clienților lor în scopul respectării de către clienți a obligațiilor fiscale dintr-o țară terță. Colectarea și transferul sunt specificate și au loc în condiții și cu garanții convenite între UE și țara terță în cadrul unui acord internațional.

În timp ce o obligație legală străină în sine nu poate fi considerată un temei legitim pentru prelucrare în conformitate cu articolul 7 litera (c), o astfel de obligație poate constitui totuși un temei legitim în cazul în care survine în cadrul unui acord internațional. În acest caz, prelucrarea ar putea fi considerată necesară pentru conformarea cu o obligație legală încorporată în cadrul juridic intern de acordul internațional. Cu toate acestea, în cazul în care nu există un astfel de acord, colectarea și transferul vor trebui să fie evaluate în temeiul articolului 7 litera (f) și pot fi considerate acceptabile sub rezerva instituirii unor garanții adecvate de tipul celor aprobate de autoritatea competentă pentru protecția datelor (a se vedea, de asemenea, *exemplul 15* de mai sus).

Exemplul 22: Transferul de date privind disidenții

La cerere, o întreprindere din UE transferă date ale rezidenților străini unor regimuri opresive dintr-o țară terță care dorește să acceseze datele disidenților (de exemplu, date privind traficul lor de mesaje electronice, conținutul mesajelor electronice, istoricul navigării pe internet sau mesajele private din rețelele de socializare).

În acest caz, spre deosebire de exemplul anterior, nu există un acord internațional care ar permite aplicarea articolului 7 litera (c) ca temei juridic. De asemenea, mai multe elemente pledează împotriva utilizării articolului 7 litera (f) ca temei pentru prelucrare. Deși operatorul poate avea un interes economic în a se asigura că se conformează solicitărilor guvernului străin (în caz contrar, acesta ar putea suferi un tratament mai puțin favorabil din partea guvernului țării terțe în comparație cu alte întreprinderi), legitimitatea și proporționalitatea transferului este foarte discutabilă în contextul drepturilor fundamentale a Uniunii Europene. Posibilul impact enorm asupra persoanelor în cauză (de exemplu, discriminare, închisoare, pedeapsa cu moartea) pledează, de asemenea, într-o mare măsură, în favoarea intereselor și drepturilor persoanelor vizate.

Reutilizarea datelor publice

Exemplul 23: Clasamentul politicienilor[126]

Un ONG din domeniul transparenței utilizează datele disponibile în mod public referitoare la politicieni (promisiuni făcute în momentul alegerii lor și evidențele efective ale voturilor) pentru a-i include într-un clasament pe baza măsurii în care aceștia și-au respectat promisiunile.

Chiar dacă impactul asupra politicienilor în cauză poate fi semnificativ, faptul că prelucrarea se bazează pe informații publice și are loc în legătură cu responsabilitățile lor publice, cu scopul clar de a spori transparența și răspunderea, face ca balanța echilibrului să se încline spre interesul operatorului[127].

Copiii și alte persoane vulnerabile

Exemplul 24: Site internet cu informații pentru adolescenți

Un site internet al unui ONG care oferă consiliere pentru adolescenți cu privire la aspecte precum consumul de droguri, sarcini nedorite și abuzul de alcool colectează date prin intermediul propriului server despre vizitatorii site-ului. Imediat după aceasta, site-ul anonimizează datele și le transformă în statistici generale despre secțiunile site-ului care sunt cele mai populare în rândul vizitatorilor provenind din diferite regiuni geografice ale țării.

Articolul 7 litera (f) ar putea fi utilizat ca temei juridic chiar dacă este vorba despre date privind persoane vulnerabile, întrucât prelucrarea este în interesul public și sunt instituite garanții stricte (datele sunt imediat anonimizate și utilizate doar pentru crearea de statistici), ceea ce contribuie la înclinarea balanței în favoarea operatorului.

Soluțiile de protejare a vieții private din faza de concepție ca garanții suplimentare

Exemplul 25: Accesul la numerele de telefon mobil ale utilizatorilor și non-utilizatorilor unei aplicații: „compară și uită”

Datele cu caracter personal ale persoanelor sunt prelucrate pentru a verifica dacă acestea și-au dat deja consimțământul neechivoc în trecut (și anume, „compară și uită” ca garanție).

Un dezvoltator de aplicații are obligația să dispună de consimțământul neechivoc al persoanei vizate pentru prelucrarea datelor sale cu caracter personal: de exemplu, dezvoltatorul de aplicații dorește să acceseze și să colecteze întreaga agendă de adrese electronice a utilizatorilor aplicației, inclusiv numerele de telefon mobil ale contactelor care nu utilizează aplicația. Pentru a putea face acest lucru, acesta ar trebui mai întâi să evalueze dacă titularii

[126] A se vedea și a se compara, de asemenea, cu exemplul 7 de mai sus.

[127] La fel precum în *exemplele 1 și 2*, se presupune că publicarea este exactă și proporțională – lipsa de garanții și alți factori pot modifica echilibrul intereselor în funcție de faptele în speță.

numerelor de telefon mobil din agendele utilizatorilor aplicației și-au acordat consimțământul neechivoc [în temeiul articolul 7 litera (a)] pentru ca datele lor să fie prelucrate.

Pentru această prelucrare inițială limitată (și anume, acces pe termen scurt pentru citire la agenda de adrese a unui utilizator al aplicației), dezvoltatorul de aplicații se poate baza pe articolul 7 litera (f) ca temei juridic, sub rezerva garanțiilor. Garanțiile ar trebui să includă măsuri tehnice și organizatorice pentru a se asigura că întreprinderea utilizează accesul doar pentru a sprijini utilizatorul să identifice care dintre persoanele sale de contact sunt deja utilizatori și care, prin urmare, și-au acordat deja consimțământul neechivoc ca întreprinderea să colecteze și să prelucreze numere de telefon în acest scop. Numerele de telefon mobil ale non-utilizatorilor pot fi colectate și utilizate doar pentru scopul strict limitat de a verifica dacă aceștia și-au acordat consimțământul neechivoc ca datele lor să fie prelucrate și ar trebui să fie șterse imediat după aceea.

Combinarea de informații cu caracter personal în cadrul serviciilor web

Exemplul 26: Combinarea de informații cu caracter personal în cadrul serviciilor web

O întreprindere care furnizează diferite servicii de internet, inclusiv motoare de căutare, partajare de materiale video și rețele sociale, elaborează o politică de confidențialitate incluzând o clauză care îi permite „să combine toate informațiile cu caracter personal" colectate pentru fiecare dintre utilizatorii săi în ceea ce privește diversele servicii pe care le utilizează, fără a defini nicio perioadă de păstrare a datelor. Potrivit întreprinderii, acest lucru se realizează pentru a „garanta cea mai bună calitate posibilă a serviciului".

Întreprinderea pune anumite instrumente la dispoziția diferitelor categorii de utilizatori, astfel încât aceștia să își poată exercita drepturile (de exemplu, dezactivarea publicității selective, opțiunea de a refuza setarea unui anumit tip de cookie).

Cu toate acestea, instrumentele disponibile nu permit utilizatorilor să controleze în mod efectiv prelucrarea datelor acestora: utilizatorii nu pot controla combinările specifice ale datelor lor între servicii și nu pot refuza combinarea datelor despre ei. În ansamblu, există un dezechilibru între interesul legitim al întreprinderii și protecția drepturilor fundamentale ale utilizatorilor, iar articolul 7 litera (f) nu ar trebui să fie invocat ca temei juridic pentru prelucrare. Articolul 7 litera (a) ar fi un temei mai adecvat, sub rezerva îndeplinirii condițiilor pentru un consimțământ valabil.