

I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor referitor la propunerile Comisiei pentru un regulament al Parlamentului European și al Consiliului privind utilizările abuzive ale informațiilor privilegiate și manipulările pieței și pentru o directivă a Parlamentului European și a Consiliului privind sancțiunile penale pentru utilizările abuzive ale informațiilor privilegiate și manipulările pieței

(2012/C 177/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date ⁽¹⁾,

având în vedere 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 ⁽²⁾, în special articolul 28 alineatul (2),

ADOPTĂ PREZENTUL AVIZ:

1. INTRODUCERE

1.1. Consultarea AEPD

1. Prezentul aviz face parte dintr-un pachet de patru avize ale AEPD referitoare la sectorul financiar, adoptate în aceeași zi ⁽³⁾.
2. La 20 octombrie 2011, Comisia a adoptat o propunere de regulament al Parlamentului European și al Consiliului privind utilizările abuzive ale informațiilor privilegiate și manipulările pieței („propunerea de regulament”) și o propunere de directivă a Parlamentului European și a Consiliului privind sancțiunile penale pentru utilizările abuzive ale informațiilor privilegiate și manipulările pieței („propunerea de directivă”). Propunerile de regulament și de directivă (denumite în mod colectiv „propunerile”) au fost trimise de către Comisia AEPD și au fost primite la 31 octombrie 2011. La 6 decembrie 2011, Consiliul Uniunii Europene a consultat AEPD în privința propunerilor.

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

⁽²⁾ JO L 8, 12.1.2001, p. 1.

⁽³⁾ Avizele AEPD din 10 februarie 2012 privind pachetul legislativ referitor la revizuirea legislației din domeniul bancar, agențiile de rating de credit, piețele de instrumente financiare (MiFID/MiDIR) și abuzurile de piață.

3. AEPD a fost consultată în mod informal înainte de adoptarea propunerii de regulament. AEPD observă că unele dintre observațiile sale au fost incluse în propunere.
4. AEPD salută faptul că este consultată de către Comisie și Consiliu.

1.2. Obiectivele și domeniul de aplicare al propunerilor

5. Directiva privind abuzul de piață (Market Abuse Directive, MAD) ⁽¹⁾, adoptată la începutul anului 2003, a introdus un cadru juridic comun la nivelul UE pentru prevenirea, identificarea și impunerea de sancțiuni atât pentru utilizările abuzive ale informațiilor privilegiate, cât și pentru manipulările pieței.
6. La câțiva ani de la intrarea acesteia în vigoare, Comisia a evaluat aplicarea MAD și a identificat o serie de probleme, precum inconsecvențe în reglementarea anumitor instrumente și piețe, deficiențe în aplicarea efectivă (autoritățile de reglementare nu dispun de anumite informații și competențe, iar sancțiunile lipsesc sau nu au un caracter destul de disuasiv), lipsa clarității privind anumite concepte esențiale și sarcini administrative asupra emitenților.
7. Având în vedere aceste probleme și importante modificări aduse peisajului financiar ca urmare a evoluțiilor legislative, de piață și tehnologice, Comisia a adoptat propuneri legislative pentru reformarea MAD care constau în propunerile de regulament și de directivă. Obiectivele de politică ale revizuirii propuse sunt creșterea încrederii investitorilor și a integrității pieței și asigurarea adaptării la noile evoluții din sectorul financiar.
8. În special, propunerea de regulament extinde sfera cadrului privind abuzul de piață, califică tentativele de manipulare a pieței și de utilizare abuzivă a informațiilor privilegiate drept infracțiuni specifice, consolidează competențele de anchetare acordate autorităților competente și introduce norme minime pentru măsuri administrative, sancțiuni și amenzi.
9. Propunerea de directivă impune statelor membre să introducă sancțiuni penale pentru actele intenționate de utilizare abuzivă a informațiilor privilegiate sau de manipulare a pieței și pentru instigarea, complicitatea și tentativa de săvârșire a oricăreia dintre aceste infracțiuni. De asemenea, extinde răspunderea asupra persoanelor juridice, inclusiv, atunci când este posibil, răspunderea penală a persoanelor juridice.

1.3. Scopul avizului AEPD

10. Unele dintre măsurile planificate din propuneri pentru creșterea integrității pieței și protecția investitorilor au impact asupra drepturilor persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ale acestora.
11. În special, atunci când autoritățile competente anchetează sau cooperează în scopul identificării, raportării și/sau sancționării utilizării abuzive a informațiilor privilegiate sau a abuzului de piață, sunt colectate, prelucrate și comunicate date cu caracter personal. În plus, mecanismul pentru încurajarea persoanelor în sensul raportării încălcărilor va implica, de asemenea, prelucrarea datelor cu caracter personal aparținând atât persoanei care raportează încălcările, cât și persoanei „incriminate”. În sfârșit, regimul de sancțiuni va afecta dreptul la protecția datelor cu caracter personal, în măsura în care vor fi publicate sancțiuni care menționează identitatea persoanei responsabile pentru încălcarea propunerii de regulament.
12. Deși propunerea de regulament conține mai multe dispoziții care pot afecta dreptul persoanei la protecția datelor sale cu caracter personal, propunerea de directivă nu implică în sine prelucrarea datelor cu caracter personal. Prin urmare, prezentul aviz se va axa pe propunerea de regulament, în special pe următoarele aspecte: 1. aplicabilitatea legislației din domeniul protecției datelor; 2. listele persoanelor care au acces la informații privilegiate; 3. atribuțiile autorităților competente; 4. sistemele instituite pentru identificarea și raportarea tranzacțiilor suspecte; 5. schimbul de informații cu țări terțe; 6. publicarea sancțiunilor și raportarea încălcărilor.

⁽¹⁾ Directiva 2003/6/CE a Parlamentului European și a Consiliului din 28 ianuarie 2003 privind utilizările abuzive ale informațiilor confidențiale și manipulările pieței (abuzul de piață), JO L 96, 12.4.2003, p. 16.

2. ANALIZA PROPUNERILOR

2.1. Aplicabilitatea legislației din domeniul protecției datelor

13. Atât considerentele ⁽¹⁾, cât și dispozițiile ⁽²⁾ din propunerea de regulament menționează Carta drepturilor fundamentale, Directiva 95/46/CE și Regulamentul (CE) nr. 45/2001. În special, articolul 22 din propunerea de regulament prevede în mod explicit ca regulă generală că „în ceea ce privește procedurile de prelucrare a datelor cu caracter personal efectuate de statele membre în cadrul prezentului regulament, autoritățile competente aplică prevederile Directivei 95/46/CE. În ceea ce privește procedurile de prelucrare a datelor cu caracter personal efectuate de AEVMP în cadrul prezentului regulament, AEVMP respectă prevederile Regulamentului (CE) nr. 45/2001”. De asemenea, dispoziția prevede o perioadă de păstrare a datelor cu caracter personal de maximum 5 ani.
14. AEPD salută cu deosebită satisfacție această dispoziție importantă și apreciază în general atenția acordată în mod specific legislației în materie de protecție a datelor în propunerea de regulament. Totuși, AEPD sugerează că această dispoziție ar trebui reformulată, astfel încât să sublinieze aplicabilitatea legislației actuale în materie de protecție a datelor. De asemenea, referirea la Directiva 95/46/CE ar trebui clarificată, prin menționarea faptului că dispozițiile se aplică în conformitate cu normele naționale de aplicare a Directivei 95/46/CE. AEPD observă că unele dispoziții ale propunerii de regulament se referă în mod explicit la Directiva 95/46/CE și/sau la Regulamentul (CE) nr. 45/2001. Aceasta subliniază aplicarea normelor relevante privind protecția datelor în cazuri specifice, dar nu înseamnă că normele nu sunt aplicabile atunci când nu sunt menționate în mod explicit în fiecare dispoziție care implică (eventual) prelucrarea datelor cu caracter personal.
15. La fel ca în considerentul 33, în alte considerente ar trebui să se utilizeze în mod constant formularea „statele membre respectă” în loc de „ar trebui să respecte” legislația relevantă în materie de protecție a datelor, deoarece aceasta din urmă este în vigoare și nu există o marjă de apreciere în privința aplicabilității sale.

2.2. Listele persoanelor care au acces la informații privilegiate

16. Propunerea de regulament conține o dispoziție prin care emitenții unui instrument financiar sau participanții pe piața certificatelor de emisii sunt obligați să stabilească o listă cu persoanele care lucrează pentru ei pe baza unui contract de muncă sau a altei forme de colaborare, care au acces la informații privilegiate [articolul 13 alineatul (1)]. Emitenții ale căror instrumente financiare sunt admise la tranzacționare pe o piață de creștere pentru IMM-uri sunt scutiți de această obligație, cu excepția cazului în care există o solicitare în acest sens din partea autorității competente [articolul 13 alineatul (2)].
17. AEPD recunoaște necesitatea acestei liste ca instrument important pentru autoritățile competente atunci când anchetează posibile utilizări abuzive ale informațiilor privilegiate sau abuzuri de piață. Totuși, în măsura în care aceste liste vor implica prelucrarea datelor cu caracter personal, legea de bază ar trebui să conțină principalele norme și garanții în materie de protecție a datelor. Prin urmare, AEPD recomandă introducerea, într-o dispoziție de fond din propunerea de regulament, a unei referiri explicite la scopul unei astfel de liste. Într-adevăr, scopul este unul dintre elementele esențiale ale oricărei prelucrări în conformitate cu articolul 6 din Directiva 95/46/CE.
18. În conformitate cu articolul 13 alineatul (4) din propunerea de regulament, Comisia adoptă, prin intermediul unor acte delegate, măsuri de stabilire a conținutului unei liste (inclusiv a informațiilor cu privire la identitatea persoanelor și la motivele pentru care sunt incluse pe lista celor care au acces la informații privilegiate) și a condițiilor în care este întocmită o astfel de listă (inclusiv condițiile de actualizare, perioada de păstrare și responsabilitățile persoanelor incluse în listă). Totuși, AEPD recomandă:
- includerea principalelor elemente ale listei (în orice caz, motivele includerii persoanelor respective) chiar în propunerea de regulament;
 - includerea unei referi la necesitatea consultării AEPD atunci când actele delegate privesc prelucrarea datelor cu caracter personal.

2.3. Atribuțiile autorităților competente

19. Articolul 17 alineatul (2) enumeră competențele minime de supraveghere și de investigație de care dispun autoritățile competente pentru a-și îndeplini atribuțiile în conformitate cu propunerea de regulament.

⁽¹⁾ A se vedea considerentele 33, 35, 39 și 40 din propunerea de regulament.

⁽²⁾ A se vedea articolul 17 alineatul (4), articolele 22, 23 și articolul 29 alineatul (1) litera (c) din propunerea de regulament.

20. Două dintre competențele menționate necesită o atenție deosebită, deoarece afectează drepturile la viața privată și la protecția datelor: competența de a intra în sedii private în vederea confiscării de documente în orice formă și competența de a solicita înregistrările convorbirilor telefonice și ale schimburilor de date.

2.3.1. Competența de a intra în sedii private

21. Competența de a intra în sedii private în vederea confiscării de documente, în orice formă, este extrem de invazivă și aduce atingere dreptului la viață privată. Astfel, aceasta ar trebui să facă obiectul unor condiții stricte și să fie însoțită de garanții adecvate⁽¹⁾. Articolul 17 alineatul (2) litera (e) impune ca accesul în sediile private să se facă pe baza unei autorizații prealabile din partea autorității judiciare, în conformitate cu legislația națională, și atunci când există bănuiele întemeiate că documentele legate de obiectul anchetei ar putea fi concludente pentru a dovedi utilizarea abuzivă a informațiilor privilegiate sau manipularea pieței. AEPD apreciază faptul că textul reglementează atribuțiile autorității competente impunând drept condiții pentru accesul în sedii private suspiciunea rezonabilă privind încălcarea propunerii de regulament sau de directivă și autorizarea prealabilă din partea unei autorități judiciare. Cu toate acestea, AEPD consideră că cerința generală a unei autorizări judiciare prealabile, indiferent dacă aceasta este sau nu prevăzută de legislația internă, este atât justificată, cât și necesară având în vedere posibilul caracter invaziv al competenței în cauză.
22. Considerentul 30 din propunerea de regulament menționează cazurile în care este necesar accesul la sedii private: persoana căreia i s-au solicitat deja informații nu se conformează (în totalitate sau parțial) acestei obligații sau există motive pentru a considera că, dacă s-ar formula o astfel de solicitare, persoana în cauză nu s-ar conforma sau că documentele sau informațiile la care se referă solicitarea ar fi retrase, modificate sau distruse. AEPD salută aceste precizări. Totuși, AEPD consideră că acestea reprezintă garanții suplimentare, care sunt necesare pentru a asigura conformitatea cu dreptul la viață privată și, prin urmare, ar trebui să fie introduse într-o dispoziție de fond, ca o condiție a accesului la sedii private.

2.3.2. Competența de a solicita înregistrările convorbirilor telefonice și ale schimburilor de date

23. Articolul 17 alineatul (2) autorizează autoritățile competente să „solicite înregistrări ale convorbirilor telefonice și ale schimburilor de date existente deținute de operatorii de telecomunicații sau de societățile de investiții”, dar precizează că această cerință este condiționată de „bănuiele întemeiate” că aceste înregistrări „ar putea fi concludente pentru a dovedi utilizarea abuzivă a informațiilor privilegiate sau manipularea pieței” în temeiul propunerii de regulament sau de directivă. Totuși, aceste înregistrări nu includ „conținutul comunicărilor respective”. În plus, articolul 17 alineatul (3) prevede că atribuțiile menționate la alineatul (2) sunt exercitate în conformitate cu legislația națională.
24. Datele referitoare la utilizarea mijloacelor de comunicații electronice pot cuprinde o gamă largă de informații cu caracter personal, precum identitatea persoanelor care inițiază sau primesc apelul, ora și durata apelului, rețeaua folosită, localizarea geografică a utilizatorului în cazul aparatelor portabile etc. Unele date de trafic privind utilizarea internetului și a e-mailului (de exemplu, lista site-urilor vizitate) pot oferi, de asemenea, detalii importante despre conținutul comunicării. În plus, prelucrarea datelor privind traficul contravine secretului corespondenței. Având în vedere acest aspect, Directiva 2002/58/CE⁽²⁾ (Directiva asupra confidențialității și comunicațiilor electronice) a instituit principiul conform căruia datele privind traficul trebuie șterse sau trecute în anonimat atunci când nu mai sunt necesare în vederea transmiterii comunicației⁽³⁾. Conform articolului 15 alineatul (1) din această directivă, statele membre pot include în legislația națională derogări în anumite scopuri legitime, dar derogările trebuie să fie necesare, corespunzătoare și proporționale în cadrul unei societăți democratice, pentru atingerea acestor scopuri⁽⁴⁾.

⁽¹⁾ A se vedea în special CEDO, 23 februarie 1993, Funcke/Franța, 10828/84.

⁽²⁾ Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (JO L 201, 31.7.2002, p. 37).

⁽³⁾ A se vedea articolul 6 alineatul (1) din Directiva 2002/58/CE (JO L 201, 31.7.2002, p. 37).

⁽⁴⁾ Articolul 15 alineatul (1) din Directiva 2002/58/CE prevede că astfel de restrângeri „constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (de exemplu, siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46/CE. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat [...]”.

25. AEPD recunoaște că obiectivele urmărite de Comisie în propunerea de regulament sunt legitime. De asemenea, AEPD înțelege necesitatea unor inițiative care să vizeze consolidarea supravegherii piețelor financiare pentru a menține soliditatea acestora și pentru a proteja mai bine investitorii și economia în general. Totuși, competențele de anchetare legate în mod direct de datele privind traficul, având în vedere caracterul lor potențial invaziv, trebuie să respecte cerințele de necesitate și proporționalitate, adică să se limiteze la ceea ce este adecvat pentru atingerea obiectivului urmărit și să nu depășească ceea ce este necesar pentru atingerea acestuia⁽¹⁾. Prin urmare, este esențial din această perspectivă ca dispozițiile să fie formulate clar în ceea ce privește domeniul lor de aplicare personal și material, precum și circumstanțele și condițiile în care pot fi folosite. În plus, trebuie prevăzute garanții adecvate împotriva riscului de abuzuri.
26. Înregistrările convorbirilor telefonice și schimburilor de date vizate vor include, în mod evident, date cu caracter personal în sensul Directivei 95/46/CE, al Directivei 2002/58/CE și al Regulamentului (CE) nr. 45/2001. Considerentul 31 din propunerea de regulament menționează că „înregistrările convorbirilor telefonice și ale schimburilor de date [...] pot stabili identitatea unei persoane responsabile de diseminarea informațiilor false sau înșelătoare, pot demonstra că anumite persoane s-au aflat în contact la un anumit moment sau că există o relație între două sau mai multe persoane”⁽²⁾. Prin urmare, trebuie să se asigure respectarea deplină a condițiilor prelucrării corecte și legale a datelor cu caracter personal, astfel cum sunt prevăzute în directive și în regulament.

2.3.3. Cerința privind autorizația judiciară

27. AEPD observă că, în conformitate cu articolul 17 alineatul (3), această competență se exercită în conformitate cu legislația națională, fără a se face referire în mod explicit la o autorizație judiciară prealabilă, cum este cazul competenței de a intra în sedii private. AEPD consideră că cerința generală a unei autorizări judiciare prealabile în toate cazurile – indiferent dacă legislația națională prevede sau nu acest lucru – ar fi justificată având în vedere posibilul caracter invaziv al competenței în cauză și în interesul aplicării armonizate a legislației în toate statele membre ale UE. De asemenea, trebuie avut în vedere faptul că mai multe legi ale statelor membre prevăd garanții speciale privind inviolabilitatea domiciliului împotriva controalelor, a perchezițiilor sau a confiscărilor disproporționate și nereglementate atent, în special atunci când acestea sunt realizate de instituții cu rol administrativ.
28. În plus, AEPD recomandă introducerea cerinței ca autoritățile competente să solicite înregistrările convorbirilor telefonice și ale schimburilor de date printr-o decizie oficială, care să precizeze temeiul juridic și scopul cererii, informațiile solicitate, termenul în care trebuie furnizate informațiile, precum și dreptul destinatarului cererii de a se adresa Curții de Justiție pentru analizarea deciziei.

2.3.4. Definiția înregistrărilor convorbirilor telefonice și ale schimburilor de date

29. Propunerea de regulament nu definește noțiunile de „înregistrări ale convorbirilor telefonice și ale schimburilor de date”. Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice) face referire numai la „date de transfer”, dar nu și la „înregistrări ale convorbirilor telefonice și ale schimburilor de date”. Este de la sine înțeles că semnificația exactă a acestor noțiuni determină impactul pe care competența de anchetare o poate avea asupra vieții private și protecției datelor persoanelor vizate. AEPD sugerează utilizarea terminologiei deja existente în definiția „datelor de transfer” din Directiva 2002/58/CE.
30. Articolul 17 alineatul (2) litera (f) face referire la „înregistrări ale convorbirilor telefonice și ale schimburilor de date existente deținute de operatorii de telecomunicații”. Directiva asupra confidențialității și comunicațiilor electronice stabilește principiul conform căruia datele de transfer trebuie să fie șterse atunci nu mai sunt necesare în scopurile comerciale pentru care au fost colectate. Totuși, conform articolului 15 alineatul (1) din această directivă, statele membre pot fi exceptate de la această obligație în sensul aplicării legii. Directiva privind păstrarea datelor intenționează să alinieze inițiativele statelor membre în temeiul articolului 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, în ceea ce privește păstrarea datelor în vederea investigării, a depistării și a urmăririi penale a infracțiunilor „grave”.

(1) A se vedea, de exemplu, cauzele conexe C-92/09 și C-93/09, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-92/09)/Land Hessen, nepublicate încă în Culegere, punctul 74.

(2) A se vedea, de asemenea, p. 12 din expunerea de motive a propunerii de regulament.

31. Întrebarea este dacă înregistrările convorbirilor telefonice și ale schimburilor de date menționate la articolul 17 alineatul (2) litera (f) fac referire la datele disponibile ca urmare a stocării traficului și a datelor de localizare reglementate de Directiva asupra confidențialității și comunicațiilor electronice sau la datele suplimentare prevăzute de Directiva privind păstrarea datelor. Ultima opțiune ar genera motive grave de îngrijorare, deoarece derogările prevăzute la articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice (și anume prevenirea, detectarea, investigarea și urmărirea penală a unor fapte penale) ar fi utilizate pentru a crește numărul scopurilor în care sunt păstrate datele în temeiul Directivei privind păstrarea datelor (și anume investigarea, detectarea și urmărirea penală a unor fapte penale „grave”). Cu alte cuvinte, datele păstrate în temeiul Directivei privind păstrarea datelor ar fi astfel folosite în scopuri care nu sunt prevăzute de directivă. Aceasta ar implica o încurajare din partea UE pentru utilizarea „lacunei legislative” care reprezintă una dintre principalele deficiențe ale actualei Directive privind păstrarea datelor ⁽¹⁾.
32. Prin urmare, AEPD recomandă cu insistență specificarea categoriilor de înregistrări telefonice și schimburi de date care pot fi solicitate de autoritățile competente. Aceste date trebuie să fie adecvate, relevante și să nu depășească limitele scopurilor pentru care sunt accesate și prelucrate. De asemenea, AEPD recomandă limitarea sferei articolului 17 alineatul (2) litera (f) la datele prelucrate (deținute) în mod normal de operatorii de telecomunicații în cadrul Directivei 2002/58/CE asupra confidențialității și comunicațiilor electronice. Aceasta exclude, în principiu, accesul la datele reținute în sensul Directivei privind păstrarea datelor, în măsura în care acest acces nu este în scopul investigării, al detectării și al urmăririi penale a unor fapte penale „grave” ⁽²⁾.
33. Articolul 17 alineatul (2) litera (f) prevede accesul la „înregistrări ale convorbirilor telefonice și ale schimburilor de date [...] deținute de [...] societățile de investiții”. Textul ar trebui să specifice categoriile de înregistrări și să explice care sunt societățile la care se face referire. AEPD presupune că înregistrările vor coincide cu cele menționate în propunerea de directivă a Parlamentului European și a Consiliului privind piețele instrumentelor financiare („propunerea MiFID”). AEPD subliniază că a prezentat o serie de observații referitoare la această propunere, prin care a recomandat și clarificarea acestor noțiuni ⁽³⁾. De asemenea, în măsura în care datele privind apelurile telefonice și schimburile de date se referă la conversațiile telefonice și la comunicațiile electronice menționate la articolul 16 alineatul (7) din propunerea MiFID, AEPD a recomandat definirea scopului înregistrării acestor comunicații, precum și specificarea tipului de comunicații și a categoriilor de date ale acestora care vor fi înregistrate ⁽⁴⁾.
34. În sfârșit, AEPD observă cu satisfacție că textul impune drept condiție pentru accesul la înregistrări existența unei bănuieli întemeiate privind încălcarea propunerii de regulament sau a propunerii de directivă și că exclude în mod explicit accesul autorităților competente la conținutul comunicațiilor.

2.4. Sisteme funcționale de detectare și raportare a tranzacțiilor suspecte

35. Articolul 11 alineatul (1) din propunerea de regulament prevede că orice persoană care administrează activitățile unui loc de tranzacționare adoptă și menține modalități și proceduri efective cu scopul de a preveni și a identifica abuzurile de piață. De asemenea, alineatul (2) prevede că orice persoană care efectuează tranzacții cu instrumente financiare cu titlu profesional trebuie să dețină sisteme funcționale de detectare și raportare a ordinelor și tranzacțiilor care pot constitui utilizări abuzive ale informațiilor

⁽¹⁾ În această privință, a se vedea Avizul AEPD din 31 mai 2011 privind Raportul de evaluare al Comisiei către Consiliu și Parlamentul European referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE), de exemplu, punctul 24.

⁽²⁾ AEPD dorește să reamintească problemele legate de lipsa unei definiții la nivel european a „infracțiunilor grave”. AEPD a subliniat că, într-adevăr, raportul de evaluare al Comisiei referitor la Directiva privind păstrarea datelor arată că opțiunea de a lăsa definirea precisă a „infracțiunilor grave” la latitudinea statelor membre a condus la apariția unei varietăți de scopuri de utilizare a datelor. Comisia a afirmat că „majoritatea statelor membre care au transpus directiva, în conformitate cu legislația națională, permit accesul la datele păstrate și utilizarea acestora în scopuri care depășesc cadrul directivei, inclusiv prevenirea și combaterea criminalității, în general, și a riscurilor la adresa vieții și integrității corporale”. A se vedea Avizul AEPD din 31 mai 2011 privind Raportul de evaluare al Comisiei către Consiliu și Parlamentul European referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE), punctele 24, 71 și 72.

⁽³⁾ Conform articolului 71 alineatul (2) litera (d), autoritatea competentă desemnată prin propunerea MiFID poate solicita înregistrări ale convorbirilor telefonice și ale schimburilor de date existente deținute de societățile de investiții atunci când există bănuieli întemeiate de încălcare a propunerii MiFID.

⁽⁴⁾ A se vedea Avizul AEPD din 10 februarie 2012 privind propunerea de directivă a Parlamentului European și a Consiliului privind piețele instrumentelor financiare, de abrogare a Directivei 2004/39/CE a Parlamentului European și a Consiliului, și propunerea de regulament al Parlamentului European și al Consiliului privind piețele instrumentelor financiare și de modificare a Regulamentului [EMIR] privind instrumentele derivate extrabursiere, contrapărțile centrale și registrele de tranzacții.

privilegiate, manipulări ale pieței sau tentative de participare la manipularea pieței sau la utilizarea abuzivă a informațiilor privilegiate. În caz de suspiciuni, autoritatea competentă este informată fără întârziere. Comisia va adopta standardele tehnice de reglementare pentru a stabili modalitățile și procedurile adecvate menționate la alineatul (1) și pentru a determina sistemele și modelele de notificare menționate la alineatul (2) [articolul 11 alineatul (3) ultima teză].

36. În măsura în care aceste sisteme vor implica, cel mai probabil, date cu caracter personal (de exemplu, monitorizarea tranzacțiilor efectuate de persoane menționate în listele persoanelor care au acces la informații privilegiate), AEPD dorește să sublinieze că aceste standarde ar trebui elaborate în conformitate cu principiul „confidențialității prin proiectare”, adică integrarea protecției datelor și a vieții private chiar din momentul proiectării noilor produse, servicii și proceduri care implică prelucrarea datelor cu caracter personal⁽¹⁾. În plus, AEPD recomandă includerea unei referiri la necesitatea consultării AEPD în măsura în care aceste standarde de reglementare privesc prelucrarea datelor cu caracter personal.

2.5. Schimbul de informații cu state terțe

37. AEPD remarcă referirea la Directiva 95/46/CE, în special la articolele 25 sau 26, precum și garanțiile specifice menționate la articolul 23 din propunerea de regulament, referitoare la divulgarea datelor cu caracter personal către țări terțe. Având în vedere riscurile caracteristice unor astfel de transferuri, sunt considerate garanții adecvate: evaluarea de la caz la caz, verificarea necesității transferului, cerința de autorizare expresă prealabilă din partea autorității competente a unui nou transfer de date către și de către o țară terță, precum și existența unui nivel corespunzător de protecție a datelor cu caracter personal în țara terță care primește datele cu caracter personal.

2.6. Publicarea sancțiunilor

2.6.1. Publicarea obligatorie a sancțiunilor

38. Articolul 26 alineatul (3) din propunerea de regulament obligă statele membre să se asigure că autoritățile competente publică fiecare măsură sau sancțiune administrativă aplicată pentru încălcarea propunerii de regulament în cel mai scurt timp, inclusiv cel puțin informații privind natura încălcării și identitatea persoanelor responsabile, exceptând situația în care această divulgare periclitează stabilitatea piețelor financiare.
39. Publicarea sancțiunilor ar contribui la creșterea caracterului disuasiv, deoarece autorii efectivi și potențiali ar fi descurajați să săvârșească infracțiuni pentru a evita afectarea semnificativă a reputației. În plus, în acest fel va crește transparența, deoarece operatorii de pe piață ar ști că a fost comisă o încălcare de către o anumită persoană. Această obligație este restrânsă numai atunci când publicarea informațiilor ar aduce un prejudiciu disproporționat părților implicate, caz în care autoritățile competente publică sancțiunile fără a indica identitatea persoanelor responsabile.
40. AEPD salută referirea de la considerentul 35 la Carta drepturilor fundamentale și, în special, la dreptul la protecția datelor cu caracter personal în momentul adoptării și publicării sancțiunilor. Cu toate acestea, AEPD nu are convingerea că publicarea obligatorie a sancțiunilor, în forma sa actuală, îndeplinește cerințele legislației privind protecția datelor astfel cum au fost interpretate de Curtea de Justiție în hotărârea Schecke⁽²⁾. AEPD este de părere că scopul, necesitatea și proporționalitatea măsurii nu sunt stabilite în mod suficient și că, în orice caz, ar trebui prevăzute garanții adecvate împotriva riscurilor la adresa drepturilor persoanelor.

2.6.2. Necesitatea și proporționalitatea publicării

41. În hotărârea Schecke, Curtea de Justiție a anulat dispozițiile unui regulament al Consiliului și ale unui regulament al Comisiei, care prevedeau obligația de publicare a informațiilor referitoare la beneficiarii fondurilor agricole, inclusiv identitatea beneficiarilor și sumele primite de aceștia. Curtea a susținut că publicarea în cauză constituia o prelucrare de date cu caracter personal care intra sub incidența articolului 8 alineatul (2) din Carta drepturilor fundamentale a Uniunii Europene („Carta”) și, astfel, reprezenta o încălcare a drepturilor recunoscute la articolele 7 și 8 din Cartă.

⁽¹⁾ A se vedea Avizul AEPD din 14 ianuarie 2011 privind Comunicarea Comisiei către Parlamentul European, Consiliul, Comitetul Economic și Social și Comitetul Regiunilor – „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană” (JO C 181, 22.6.2011, p. 1), punctele 108-115.

⁽²⁾ Cauzele conexe C-92/09 și C-93/09, Schecke, punctele 56-64.

42. După ce a afirmat că, potrivit analizei sale, „derogările de la protecția datelor cu caracter personal și restrângerile de la aceasta trebuie să fie efectuate în limitele strictului necesar”, Curtea a continuat prin a analiza scopul publicării și proporționalitatea acestora. Curtea a concluzionat că nu există indicii potrivit cărora, atunci când au adoptat actele legislative în cauză, Consiliul și Comisia ar fi luat în considerare modalități de publicare a informațiilor care să fie consecvente cu obiectivul unei astfel de publicări și care, în același timp, să îi afecteze într-o mai mică măsură pe respectivii beneficiari.
43. Articolul 26 alineatul (3) din propunerea de regulament pare să fie afectat de aceleași deficiențe subliniate de CEJ în hotărârea *Schecke*. Trebuie reținut că, atunci când o dispoziție care impune divulgarea publică a unor informații cu caracter personal este evaluată din perspectiva respectării cerințelor de protecție a datelor, este deosebit de important să existe un scop clar și bine definit care se intenționează a fi urmărit prin publicarea în cauză. Numai în condițiile existenței unui astfel de scop clar și bine definit se poate stabili dacă publicarea respectivelor date cu caracter personal este cu adevărat necesară și proporțională ⁽¹⁾.
44. După ce a citit propunerea și documentele însoțitoare (respectiv, raportul de evaluare a impactului), AEPD este de părere că scopul și, implicit, necesitatea acestei măsuri nu sunt clar stabilite. În timp ce considerentele propunerii nu menționează aceste aspecte, evaluarea impactului se referă doar la efectele pozitive generale (și anume efectul disuasiv asupra abuzurilor de piață, contribuția la protecția investitorilor, tratamentul egal al emitenților, o mai bună aplicare a legii) și se limitează la menționarea faptului că „publicarea sancțiunilor are o deosebită importanță pentru creșterea transparenței și menținerea încrederii în piața financiară” și că „publicarea sancțiunilor impuse va contribui la obiectivul de descurajare și crește integritatea pieței și protecția investitorilor” ⁽²⁾. O declarație formulată în termeni atât de generali nu pare suficientă pentru a demonstra necesitatea măsurii propuse. Dacă scopul general este creșterea caracterului disuasiv, se pare că Comisia ar fi trebuit să explice, în special, motivul pentru care nu ar fi fost suficiente sancțiuni financiare mai severe (sau alte sancțiuni care nu sunt echivalente cu metoda dezaprobării publice).
45. În plus, raportul de evaluare a impactului nu pare să ia în considerare metode mai puțin agresive, precum luarea deciziei de publicare de la caz la caz. În special, ultima opțiune poate reprezenta, *prima facie*, o soluție mai proporțională, îndeosebi atunci când se consideră că publicarea este, în sine, o sancțiune – astfel cum se recunoaște la articolul 26 alineatul (1) litera (d) – care trebuie, astfel, să fie evaluată de la caz la caz, în funcție de circumstanțele relevante, precum gravitatea încălcării, gradul de responsabilitate personală, recidiva, pierderile suferite de părți terțe etc. ⁽³⁾.
46. Raportul de evaluare a impactului nu explică de ce publicarea în cazuri individuale nu este o opțiune suficientă. Acesta se limitează la a menționa că publicarea sancțiunilor impuse „va contribui la obiectivul eliminării opțiunilor și aprecierii proprii, prin eliminarea, atunci când este posibil, a marjei de apreciere de care dispun statele membre în prezent, de a nu solicita o astfel de publicare” ⁽⁴⁾. În opinia AEPD, posibilitatea de a evalua cazul din perspectiva circumstanțelor specifice reprezintă o soluție mai proporțională și, astfel, o opțiune preferată în raport cu publicarea obligatorie în toate cazurile. De exemplu, această marjă de apreciere ar permite autorității competente să evite publicarea în cazuri de încălcări mai puțin grave, când nu au fost cauzate prejudicii importante, când partea a demonstrat o atitudine cooperantă etc. Prin urmare, evaluarea impactului nu elimină îndoielile privind necesitatea și proporționalitatea măsurii.

2.6.3. Necesitatea de garanții adecvate

47. Propunerea de regulament ar fi trebuit să prevadă garanții adecvate prin care să asigure un echilibru corect între diferitele interese implicate. Mai întâi, sunt necesare garanții în ceea ce privește dreptul persoanelor incriminate de a contesta o decizie în instanță, precum și prezumția de nevinovăție.

⁽¹⁾ A se vedea, de asemenea, în această privință, Avizul AEPD din 15 aprilie 2011 privind normele financiare aplicabile bugetului anual al Uniunii (JO C 215, 21.7.2011, pp. 13-18).

⁽²⁾ A se vedea evaluarea impactului, p. 166.

⁽³⁾ Respectiv, în conformitate cu articolul 27 din propunerea de regulament privind criteriile de stabilire a sancțiunilor.

⁽⁴⁾ A se vedea evaluarea impactului, p. 167.

Articolul 26 alineatul (3) ar fi trebuit să conțină o formulare specifică în acest sens, astfel încât să oblige autoritățile competente să adopte măsuri corespunzătoare privind ambele situații în care decizia face obiectul unui recurs și, ulterior, este anulată de o instanță ⁽¹⁾.

48. În al doilea rând, propunerea de regulament ar trebui să garanteze respectarea într-o manieră proactivă a drepturilor persoanelor vizate. AEPD salută faptul că versiunea finală a propunerii prevede posibilitatea ca publicarea să fie exclusă în cazurile în care aceasta ar putea cauza prejudicii disproporționate. Totuși, o atitudine proactivă ar trebui să presupună o informare prealabilă a persoanelor vizate în privința publicării deciziei prin care sunt sancționați, precum și în privința faptului că beneficiază de dreptul de opoziție, în temeiul articolului 14 din Directiva 95/46/CE ⁽²⁾, din considerente întemeiate și legitime.
49. În al treilea rând, deși propunerea de regulament nu specifică mediul în care ar trebui publicate informațiile, în practică se presupune că, în majoritatea statelor membre, forma adoptată va fi cea a publicării pe internet. Publicările pe internet ridică probleme și riscuri specifice, legate în special de nevoia de a garanta menținerea informațiilor online doar pe perioada necesară și faptul că datele nu pot fi manipulate sau modificate. Utilizarea motoarelor externe de căutare presupune, de asemenea, riscul ca informațiile să poată fi scoase din context și transmise prin internet și în afara acestuia în moduri care nu pot fi controlate cu ușurință ⁽³⁾.
50. Având în vedere cele mai sus, este necesar ca statele membre să fie obligate să se asigure că datele cu caracter personal ale persoanelor vizate sunt păstrate online doar pentru o perioadă de timp rezonabilă, după care sunt șterse în mod sistematic ⁽⁴⁾. În plus, ar trebui să se impună statelor membre să asigure instituirea de măsuri de securitate și garanții adecvate, în special pentru protecția împotriva riscurilor legate de utilizarea motoarelor externe de căutare ⁽⁵⁾.

2.6.4. Concluzie

51. AEPD este de părere că dispoziția referitoare la publicarea obligatorie a sancțiunilor – în forma sa actuală – nu respectă drepturile fundamentale la viața privată și protecția datelor. Legiuitorul ar trebui să evalueze cu atenție necesitatea sistemului propus și să verifice dacă obligația de publicare depășește ceea ce este necesar pentru atingerea obiectivului de interes public urmărit și dacă nu există metode mai puțin restrictive de a îndeplini același obiectiv. Sub rezerva rezultatului acestui test de proporționalitate, obligația de publicare ar trebui, în orice caz, să fie însoțită de garanții adecvate care să asigure respectarea prezumției de nevinovăție, dreptul de opoziție al persoanelor vizate, securitatea/exactitatea datelor și ștergerea acestora după o perioadă de timp adecvată.

2.7. Raportarea încălcărilor

52. Articolul 29 din propunerea de regulament obligă statele membre să instituie mecanisme eficiente de raportare a încălcărilor, cunoscute și sub denumirea de „scheme de informare”. Deși pot reprezenta un instrument eficient de asigurare a conformității, aceste sisteme ridică importante preocupări din perspectiva protecției datelor ⁽⁶⁾.

⁽¹⁾ De exemplu, autoritățile naționale ar putea lua în considerare următoarele măsuri: să amâne publicarea până la respingerea recursului sau, potrivit sugestiei din raportul de evaluare a impactului, să arate în mod clar că decizia poate fi contestată și că persoana beneficiază de prezumția de nevinovăție până în momentul în care decizia devine definitivă și să publice o rectificare atunci când decizia este anulată de o instanță.

⁽²⁾ A se vedea Avizul AEPD din 10 aprilie 2007 privind finanțarea politicii agricole comune (JO C 134, 16.6.2007, pp. 1-3).

⁽³⁾ A se vedea, în această privință, documentul publicat de autoritatea italiană pentru protecția datelor, cu titlul „Datele cu caracter personal conținute în registrele și documentele organismelor administrative publice: Linii directoare privind prelucrarea acestora de către organisme publice în vederea publicării și difuzării prin internet”, disponibil pe site-ul autorității italiene pentru protecția datelor: <http://www.garanteprivacy.it/garante/docjsp?ID=1803707>

⁽⁴⁾ Aceste aspecte sunt legate, de asemenea, de dreptul general de „a fi uitat”, a cărui includere în noul cadru legislativ de protecție a datelor cu caracter personal este încă în dezbateri.

⁽⁵⁾ Aceste măsuri și garanții pot consta, de exemplu, în excluderea indexării datelor prin intermediul motoarelor externe de căutare.

⁽⁶⁾ Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal a publicat un aviz privind aceste scheme în 2006, în care abordează aspecte legate de protecția datelor, caracteristice acestui fenomen: Avizul nr. 1/2006 privind aplicarea normelor UE privind protecția datelor în cazul schemelor de informare în domeniul contabilității, al controalelor contabile interne, al auditării, al combaterii corupției și infracționalității bancare și financiare (Avizul Grupului de lucru privind informarea). Avizul este disponibil pe site-ul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

53. AEPD salută prezența în propunerea de regulament a unor garanții specifice, care urmează să fie dezvoltate ulterior la nivel național, privind protecția persoanelor care raportează suspiciuni de încălcări și, la nivel mai general, protecția datelor cu caracter personal. AEPD înțelege că propunerea de regulament stabilește doar elementele principale ale schemei care urmează să fie aplicată de statele membre. Cu toate acestea, dorește să atragă atenția asupra următoarelor aspecte suplimentare.
54. Ca în cazul altor avize ⁽¹⁾, AEPD evidențiază necesitatea introducerii unei referiri specifice la nevoia de a respecta confidențialitatea referitoare la identitatea denunțătorilor și informatorilor. AEPD subliniază că informatorii se află într-o poziție delicată. Persoanele care furnizează astfel de informații trebuie să primească garanții că identitatea lor va fi păstrată confidențială, în special față de persoana cu privire la care este raportată o presupusă ilegalitate ⁽²⁾. Confidențialitatea identității informatorilor ar trebui să fie garantată în toate etapele procedurii, în măsura în care acest lucru nu contravine reglementărilor naționale privind procedurile judiciare. În special, ar putea fi necesar ca identitatea să fie divulgată în contextul extinderii anchetelor sau al declanșării de proceduri juridice ulterioare, inițiate în urma anchetei (inclusiv în cazul în care se constată că au fost prezentate declarații false cu rea intenție) ⁽³⁾. Având în vedere cele de mai sus, AEPD recomandă adăugarea la articolul 29 alineatul (1) litera (b) a următoarei dispoziții: „identitatea acestor persoane ar trebui garantată în toate etapele procedurii, cu excepția cazului în care divulgarea este impusă de legislația internă, în contextul extinderii anchetelor sau inițierii de proceduri juridice ulterioare”.
55. AEPD observă cu satisfacție că articolul 29 alineatul (1) litera (c) impune statelor membre să asigure protecția datelor cu caracter personal aparținând atât persoanei incriminate, cât și celei care incriminează, în conformitate cu principiile stabilite în Directiva 95/46/CE. Totuși, AEPD sugerează eliminarea sintagmei „principiile stabilite în”, pentru a face referirea mai cuprinzătoare și obligatorie. În ceea ce privește necesitatea de a respecta legislația în materie de protecție a datelor în cursul punerii în aplicare practice a schemelor, AEPD dorește să sublinieze în special recomandările Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal în avizul său din 2006 referitor la schemele de informare. În cursul punerii în aplicare a schemelor naționale, entitățile competente ar trebui să aibă în vedere, printre altele, necesitatea de a respecta proporționalitatea prin limitarea, într-o măsură cât mai mare, a categoriilor de persoane îndreptățite să raporteze, a categoriilor de persoane care pot fi incriminate și a încălcărilor pentru care pot fi incriminate; necesitatea de a favoriza rapoartele identificate și confidențiale în detrimentul rapoartelor anonime; necesitatea de a dispune divulgarea identității informatorilor atunci când aceștia au prezentat declarații răuvoitoare și necesitatea de a respecta perioade stricte de păstrare a datelor.

3. CONCLUZII

56. AEPD salută atenția acordată în special protecției datelor în propunerea de regulament.
57. AEPD adresează următoarele recomandări:
- specificarea în articolul 13 a scopului listelor cu persoanele care au acces la informații privilegiate;
 - introducerea în articolul 17 alineatul (2) litera (e), referitor la competența de a intra în sedii private, a condiției generale de autorizare judiciară prealabilă;
 - introducerea în articolul 17 alineatul (2) litera (f), referitor la competența de a solicita datele privind convorbirile telefonice și schimburile de date, a cerinței generale de autorizare judiciară prealabilă și a cerinței privind o decizie oficială care să specifice: (i) temeiul juridic; (ii) scopul cererii; (iii) informațiile solicitate; (iv) termenul în care trebuie furnizate informațiile; și (v) dreptul destinatarului cererii de a se adresa Curții de Justiție pentru analiza deciziei;

⁽¹⁾ A se vedea, de exemplu, Avizul privind normele financiare aplicabile bugetului anual al Uniunii din 15 aprilie 2011 și Avizul privind investigațiile efectuate de OLAF din 1 iunie 2011, ambele disponibile la: <http://www.edps.europa.eu>

⁽²⁾ Importanța păstrării confidențialității referitoare la identitatea informatorilor a fost deja amintită de AEPD într-o scrisoare adresată Ombudsmanului European la 30 iulie 2010, în cazul 2010-0458, disponibilă pe site-ul AEPD (<http://www.edps.europa.eu>). A se vedea, de asemenea, avizele AEPD privind verificările prealabile din 3 februarie 2012, 23 iunie 2006, privind investigațiile interne ale OLAF (cazul 2005-0418), și din 4 octombrie 2007 privind investigațiile externe ale OLAF (cazurile 2007-47, 2007-48, 2007-49, 2007-50, 2007-72).

⁽³⁾ A se vedea Avizul privind normele financiare aplicabile bugetului anual al Uniunii din 15 aprilie 2011, disponibil la: <http://www.edps.europa.eu>

- specificarea categoriilor de înregistrări ale convorbirilor telefonice și ale schimburilor de date deținute de operatorii de telecomunicații și de societățile de investiții pe care le pot solicita autoritățile competente, precum și limitarea sferei articolului 17 alineatul (2) litera (f) la datele prelucrate („deținute”) în mod normal de operatorii de telecomunicații în cadrul Directivei 2002/58/CE;
- adăugarea la articolul 29 alineatul (1) litera (b) a unei dispoziții cu următorul conținut: „identitatea acestor persoane ar trebui garantată în toate etapele procedurii, cu excepția cazului în care divulgarea este impusă de legislația internă, în contextul extinderii anchetelor sau inițierii de proceduri juridice ulterioare”;
- având în vedere îndoielile exprimate în prezentul aviz, evaluarea necesității și proporționalității sistemului propus de publicare obligatorie a sancțiunilor. Sub rezerva rezultatului testului de necesitate și proporționalitate, asigurarea, în orice caz, de garanții adecvate care să asigure respectarea prezumției de nevinovăție, a dreptului de opoziție al persoanelor vizate, securitatea/exactitatea datelor și ștergerea acestora după o perioadă de timp adecvată.

Adoptat la Bruxelles, 10 februarie 2012.

Giovanni BUTTARELLI
*Adjunctul Autorității Europene pentru Protecția
Datelor*
