COMISIA EUROPEANĂ

Bruxelles, 25.1.2012
COM(2012) 12 final

RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

în temeiul articolului 29 alineatul (2) din Decizia-cadru a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală

{SEC(2012) 75 final}

RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

în temeiul articolului 29 alineatul (2) din Decizia-cadru a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală

1. INTRODUCERE

1.1. Context

Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008[1] (denumită în continuare „decizia-cadru") privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală instituie un cadru legislativ general pentru protecția datelor în cadrul cooperării polițienești și judiciare în materie penală. Decizia a intrat în vigoare la 19 ianuarie 2009[2].

Decizia-cadru era necesară deoarece la acea dată nu exista un instrument general la nivel european care să reglementeze prelucrarea datelor în domeniul cooperării polițienești și judiciare în materie penală[3]. Articolul 3 din Directiva 95/46/CE privind protecția datelor cu caracter personal și libera circulație a acestor date prevede că directiva nu se aplică „prelucrării datelor cu caracter personal puse în practică pentru exercitarea activităților din afara domeniului de aplicare a dreptului comunitar, cum ar fi cele prevăzute de titlul VI din Tratatul privind Uniunea Europeană și, în orice caz, prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului sau activitățile statului în domeniul dreptului penal".

Obiectivul deciziei-cadru este de a asigura, la nivelul UE, un nivel ridicat de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice atunci când datele cu caracter personal sunt prelucrate în cadrul cooperării polițienești și judiciare în materie penală. În același timp, ar trebui garantat un nivel ridicat de siguranță publică[4]. Decizia-cadru nu împiedică statele membre să ofere un grad mai ridicat de garanții pentru protejarea datelor cu caracter personal colectate sau prelucrate la nivel național[5].

Domeniul de aplicare[6] a deciziei-cadru se limitează la prelucrarea datelor cu caracter personal în scopul prevenirii, cercetării, depistării, urmăririi penale a infracțiunilor sau în scopul executării pedepselor penale, date care sunt sau au fost transmise sau puse la dispoziție:

- între statele membre;

---

1 JO L 350, 30.12.2008, p. 60.
2 Articolul 30.
3 Considerentul 5 al Directivei 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, JO L 281, 23.11.1995, p. 31.
4 Articolul 1.
5 Articolul 1 alineatul (5).
6 Articolul 1 alineatul (2).

- de statele membre autorităților sau sistemelor de informații instituite în temeiul titlului VI din Tratatul privind Uniunea Europeană („Cooperarea polițienească și judiciară în materie penală”); sau

- autorităților competente ale statelor membre de către autorități sau sisteme de informații instituite în temeiul Tratatului privind Uniunea Europeană sau a Tratatului de instituire a Comunității Europene.

Datele cu caracter personal care au fost transferate de la un stat membru la un altul pot fi, de asemenea, transferate către state terțe sau organisme internaționale, cu condiția îndeplinirii anumitor condiții[7].

Decizia-cadru se aplică integral Regatului Unit și Irlandei, deoarece este o dezvoltare a *acquis*-ului Schengen. Regatul Unit și Irlanda participă la decizia-cadru în conformitate cu articolul 5 din Protocolul privind integrarea acquis-ului Schengen în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul de instituire a Comunității Europene, precum și la Decizia 2000/365/CE și, respectiv, la Decizia 2002/192/CE.

În ceea ce privește Islanda, Norvegia, Elveția și Liechtenstein, decizia-cadru constituie o dezvoltare a *acquis*-ului Schengen, în sensul acordului și protocoalelor încheiate fie de Consiliul Uniunii Europene, fie de Uniunea Europeană cu Islanda și Norvegia, Confederația Elvețiană și Liechtenstein, precum și în sensul Deciziei 1999/437/CE, a Deciziei 2008/149/JAI și a Deciziei 2008/262/JAI a Consiliului.

1.2. Conținutul Deciziei-cadru 2008/977/JAI

Domeniul de aplicare al deciziei-cadru nu reglementează prelucrarea, la nivel național, a datelor cu caracter personal de către autoritățile judiciare sau polițienești competente din statele membre [articolul 1 alineatul (2)].

În general, instrumentele legislative sectoriale specifice pentru cooperarea polițienească și judiciară în materie penală care conțin dispoziții privind protecția datelor personale și care au fost adoptate **anterior** datei de intrare în vigoare a deciziei-cadru prevalează în raport cu decizia-cadru (articolul 28). Instrumentele considerate a stabili un „set complet și coerent de norme” în ceea ce privește protecția datelor nu intră sub incidența deciziei-cadru (considerentul 39). Alte măsuri sectoriale specifice care conțin norme privind protecția datelor cu un domeniu de aplicare mai restrâns prevalează în raport cu decizia-cadru numai în cazul în care aceste norme sunt mai restrictive decât cele ale deciziei-cadru. Altfel se aplică decizia-cadru (considerentul 40).

Decizia-cadru precizează obiectivele protecției datelor în cadrul activităților polițienești și judiciare. Prevede norme privind legalitatea prelucrării datelor cu caracter personal pentru a se asigura că orice informație care ar putea fi schimbată este prelucrată legal și în conformitate cu principiile fundamentale ale calității datelor.

Decizia-cadru definește, de asemenea, drepturile persoanelor vizate, pentru a garanta protecția datelor cu caracter personal fără a pune în pericol finalitatea cercetărilor penale. Astfel, persoanele vizate trebuie să fie informate și să aibă acces la datele lor cu caracter personal.

---

[7] Articolul 13.

Autoritățile naționale de supraveghere, acționând în deplină independență în exercitarea funcțiilor care le-au fost atribuite, trebuie să ofere consiliere și să monitorizeze aplicarea măsurilor adoptate de statele membre pentru a transpune decizia-cadru.

1.3. Obligația Comisiei de a raporta cu privire la punerea în aplicare

În temeiul articolului 29 alineatul (1) din decizia-cadru, statele membre trebuie să ia măsuri pentru a se conforma prezentei decizii înainte de 27 noiembrie 2010.

Conform articolului 29 alineatul (2), statele membre trebuie să comunice Secretariatului General al Consiliului și Comisiei textul dispozițiilor care transpun în dreptul lor intern obligațiile impuse prin decizia-cadru, precum și informațiile privind autoritățile de supraveghere prevăzute la articolul 25 din decizia-cadru.

Comisia trebuie să elaboreze un raport pe baza informațiilor prezentate de statele membre. Până la 27 noiembrie 2011, Consiliul trebuie să evalueze măsura în care statele membre s-au conformat prezentei decizii-cadru.

1.4. Sursele de informații care stau la baza prezentului raport

Până la **9 noiembrie 2011**, 26 din cele 27 de state membre, precum și Liechtenstein, Norvegia, Islanda și Elveția, au transmis Comisiei informații privind punerea în aplicare a deciziei-cadru.

Din aceste **26** de state membre, **14** state membre au precizat că legislația lor în vigoare pune în aplicare decizia-cadru (Belgia, Republica Cehă, Danemarca, Germania, Estonia, Irlanda, Ungaria, Letonia, Lituania, Luxemburg, Austria, Slovacia, Suedia și Regatul Unit). Germania, Irlanda, Estonia și Suedia au afirmat că analizează în continuare dacă sunt necesare măsuri suplimentare de punere în aplicare.

Se poate considera că **9** state membre au pus în aplicare decizia-cadru doar parțial, întrucât au comunicat că legislația de punere în aplicare trebuie încă să fie adoptată.

Patru state membre fie nu au răspuns la cererea de informații a Comisiei (România), fie au menționat că nu au pus încă în aplicare decizia-cadru (Grecia, Italia[8], Cipru).

Conținutul informațiilor, în special în ceea ce privește gradul de detaliere, furnizate de statele membre ca răspuns la chestionarul Comisiei variază. Tabelul 1 oferă o prezentare generală a răspunsurilor: reflectă evaluarea statelor membre cu privire la stadiul punerii în aplicare a deciziei-cadru.

---

[8] **Italia** a informat Comisia că instrumentele specifice de punere în aplicare nu au fost încă adoptate în mod oficial. Face trimitere la Codul privind protecția datelor cu caracter personal, la Codul de procedură penală și la alte acte care conțin dispoziții aplicabile prelucrării datelor în aceste domenii. Alte state membre au o abordare diferită și indică faptul că normele privind protecția datelor în vigoare se aplică, de asemenea, prelucrării datelor cu caracter personal de către poliție și justiție la nivel național, precum și prelucrării la nivel transfrontalier de către poliție și justiție în materie penală. De asemenea, au informat Comisia cu privire la măsurile de aplicare suplimentare, care sunt în prezent în curs de pregătire.

2. TRANSPUNEREA DECIZIEI-CADRU

2.1. Decizia-cadru bazată pe ex-articolul 34 alineatul (2) litera (b) din Tratatul privind Uniunea Europeană

Prezenta decizie-cadru are ca temei Tratatul privind Uniunea Europeană, în special articolul 30, articolul 31 litera (e) și articolul 34 alineatul (2) litera (b).

Deciziile-cadru ca instrumente juridice pot fi cel mai bine comparate cu o directivă, întrucât au forță juridică obligatorie pentru statele membre în ceea ce privește rezultatul care trebuie obținut, dar lasă la latitudinea autorităților naționale alegerea formei și a metodelor. Cu toate acestea, deciziile-cadru nu au efect direct[9].

Pe baza articolului 10 din Protocolul privind dispozițiile tranzitorii cu privire la actele adoptate în temeiul titlurilor V și VI din Tratatul privind Uniunea Europeană înainte de intrarea în vigoare a Tratatului de la Lisabona (Protocolul nr. 36), anexat la tratate, competențele Comisiei în temeiul articolului 258 din Tratatul privind funcționarea Uniunii Europene nu sunt aplicabile (și cele ale CEJ sunt în continuare limitate) în ceea ce privește actele aferente „fostului pilon trei" pentru o perioadă de tranziție de cinci ani de la intrarea în vigoare a Tratatului de la Lisabona (și anume, până la 1 decembrie 2014).

În cele ce urmează sunt prezentate detalii privind aplicarea a patru dispoziții principale ale deciziei-cadru, conform celor indicate de statele membre ca răspuns la solicitarea Comisiei din 9 decembrie 2010.

2.1.1. Domeniul de aplicare a măsurilor naționale de punere în aplicare

Decizia-cadru se aplică numai în cazul prelucrării datelor cu caracter personal transmise sau puse la dispoziție între statele membre [articolul 1 alineatul (2)]. Prelucrarea, la nivel național, a datelor cu caracter personal în materie penală de către poliție și justiție nu intră în domeniul de aplicare a deciziei-cadru.

Tabelul 2 din anexă oferă o imagine de ansamblu a măsurilor de punere în aplicare în statele membre. Majoritatea statelor membre au făcut referire la legislația generală privind protecția datelor ca fiind una dintre măsurile de punere în aplicare a deciziei-cadru și au adăugat o trimitere la legislația sectorială aplicabilă pentru poliție, justiție, autorități vamale și fiscale. Unele state membre au decis să nu adopte instrumente legislative, ci să pună în aplicare decizia prin emiterea de circulare administrative (de exemplu, Germania și Regatul Unit).

Majoritatea statelor membre au indicat că **legislația generală privind protecția datelor se aplică prelucrării datelor cu caracter personal de către poliție și justiție atât la nivel național, cât și în context transfrontalier[10], de cele mai multe ori în paralel cu legile de procedură penală și legile privind poliția (datele prelucrate de poliție)[11]**. Treisprezece state membre (Belgia, Republica Cehă, Germania, Estonia, Italia, Luxemburg, Ungaria, Malta, Țările de Jos, Slovenia, Slovacia, Finlanda și Suedia) au făcut trimitere la legi de

---

9 A se vedea cauza C-105/03, Pupino, hotărârea din 16.5.2005, punctul 34, 43-45, 47, 61, în care CEJ a statuat că instanțele naționale care interpretează legislația națională au obligația de a depune eforturi pentru a realiza o interpretare consecventă, inclusiv în ceea ce privește deciziile-cadru.

10 Aceasta era situația înainte de adoptarea deciziei-cadru (a se vedea Documentul de lucru al serviciilor Comisiei, Evaluarea impactului, SEC (2005) 1241, 4.10.2005, punctul 5.1.2.).

11 A se vedea tabelul 2.

procedură penală sau la legislație similară. Șapte state membre (Republica Cehă, Germania, Ungaria, Țările de Jos, Slovenia, Finlanda și Suedia) au menționat existența unei legi specifice privind poliția (datele prelucrate de poliție)[12]. Trei state membre (de exemplu Bulgaria, Portugalia, Lituania) au menționat că au adoptat, de asemenea, legislație specifică pentru punerea în aplicare a anumitor dispoziții ale deciziei-cadru care nu sunt reglementate de legislația generală și care se aplică numai în cazul prelucrării transfrontaliere a datelor cu caracter personal[13].

Trei state membre au considerat domeniul de aplicare restrâns al deciziei-cadru ca fiind problematic. Italia și Țările de Jos au semnalat dificultăți în ceea ce privește diferențierea în practică între prelucrarea transfrontalieră a datelor în temeiul Deciziei-cadru 2008/977 și prelucrarea la nivel național, precum și complexitatea aferentă pentru autoritățile de asigurare a aplicării legii din statele membre de a se adapta la aplicarea unor norme diferite de prelucrare a aceloraşi date cu caracter personal. Polonia a indicat deficiențele deciziei-cadru, în general, și a subliniat, în special, sprijinul pentru obiectivul Comisiei de a institui un cadru cuprinzător și de a extinde normele generale privind protecția datelor la domeniul cooperării polițienești și judiciare în materie penală[14].

2.1.2. Informații pentru persoanele vizate (articolul 16, considerentele 26 - 27)

În temeiul deciziei-cadru, statele membre trebuie să se asigure că autoritățile lor competente informează persoanele vizate cu privire la faptul că datele lor sunt prelucrate sau transmise unui alt stat membru în scopul prevenirii, cercetării, depistării și urmăririi penale a infracțiunilor sau în scopul executării sancțiunilor penale. Forma, conținutul, metoda și excepțiile (respectiv nefurnizarea sau furnizarea restrânsă a informațiilor) prevăzute în acest scop trebuie stabilite în conformitate cu dreptul intern. Aceasta se poate realiza într-un cadru general, prin adoptarea unei legi sau publicarea unei liste a operațiunilor de prelucrare. În cazul în care datele sunt transferate în alt stat membru, fiecare stat membru poate solicita celuilalt stat membru să nu informeze persoana vizată.

Tabelul 3 evidențiază faptul că **aproape toate** statele membre au indicat că oferă persoanelor vizate **unele** informații privind prelucrarea datelor lor cu caracter personal. **Franța** a menționat că nu face aceasta. Nici **Danemarca** nu acordă acest drept, dar a precizat că inspectorul responsabil în materie de prelucrare a datelor trebuie să țină un registru și să informeze publicul.

Dreptul la informare face obiectul unor **limitări în marea majoritate a statelor membre**. Legislația națională fie limitează acest drept în scopul prevenirii, cercetării, depistării și urmăririi penale a infracțiunilor, fie prevede faptul că prelucrarea datelor de către inspectori de date speciali (poliția și/sau sistemul judiciar) beneficiază de derogare în ceea ce privește aplicarea acestui drept. În unele cazuri, se prevăd limitări/derogări fără a preciza activitățile la care se referă. Un număr considerabil de state membre indică astfel de limitări în cazul poliției, poliției militare, instanțelor, autorităților vamale și fiscale.

---

12 A se vedea tabelul 2.

13 A se vedea comentariile formulate de Țările de Jos.

14 A se vedea, de asemenea, contribuția Poloniei (Ministerul de Interne) la consultarea publică lansată de Comisie la sfârșitul anului 2010 (la care Polonia a făcut trimitere în răspunsul la chestionar): http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/pl_min_pl.pdf.

Țările de Jos consideră că obligația generală de informare a persoanei vizate nu este pe deplin compatibilă cu natura activității poliției și sistemului judiciar, dar că există anumite dispoziții în vigoare în baza cărora se poate prevedea ca persoana vizată să fie informată, într-o măsură suficientă, cu privire la prelucrarea datelor de către poliție și autoritățile judiciare (de exemplu, legile cuprind informații cu privire la cazurile și condițiile de prelucrare a datelor; procurorul informează persoana vizată cu privire la exercitarea competențelor speciale de cercetare, în cazul în care acest lucru este permis în scopurile cercetării). De asemenea, Țările de Jos au declarat că nu este necesară aplicarea acestei dispoziții deoarece articolul 16 alineatul (1) se referă doar la legislația națională a statelor membre.

Decizia-cadru instituie dreptul persoanelor vizate la informare, dar nu conține detalii cu privire la metode sau la eventualele scutiri. Chiar și în cazul în care, conform statelor membre, dreptul la informare este în general acordat, modul de punere în aplicare variază semnificativ.

2.1.3. Dreptul de acces al persoanelor vizate (articolul 17)

Decizia-cadru prevede că persoana vizată are dreptul să obțină, fără constrângere, întârzieri sau cheltuieli excesive:

(a) fie cel puțin confirmarea din partea inspectorului sau a autorităților naționale de supraveghere cu privire la transmiterea sau punerea la dispoziție a datelor care o privesc sau cu privire la lipsa acestor acțiuni, precum și informații cu privire la destinatarii sau categoriile de destinatari cărora li s-au dezvăluit datele și comunicarea datelor care fac obiectul prelucrării; fie

(b) cel puțin o confirmare din partea autorității naționale de supraveghere că toate verificările aplicabile au fost efectuate.

Statele membre pot legifera măsuri de restricționare a dreptului de acces, în scopul de a evita obstrucționarea anchetelor, cercetărilor sau procedurilor oficiale sau legale; de a evita prejudicierea prevenirii, identificării, cercetării și urmăririi penale a infracțiunilor sau a executării sentințelor penale; de a proteja securitatea publică; de a proteja siguranța națională; precum și de a proteja persoana vizată sau drepturile și libertățile celorlalți [articolul 17 alineatul (2)]. Refuzul inspectorului de furnizare a acestor informații trebuie prezentat în scris [articolul 17 alineatul (3)].

Informațiile furnizate de statele membre și compilate în tabelul 4 cu privire la dreptul la acces reflectă situația în ceea ce privește furnizarea de informații către persoana vizată. Se poate concluziona că **toate statele membre**[15] **acordă persoanelor vizate sub o anumită formă dreptul de acces la date**. În general, acest drept este înscris în legislația generală a țării privind protecția datelor. De asemenea, multe state membre reglementează aspectele legate de dreptul de acces în legislația sectorială specifică (precum legile privind poliția).

În egală măsură, toate statele membre prevăd **scutiri de la acordarea dreptului de acces**. Motivele invocate cel mai frecvent pentru neacordarea dreptului de acces sunt:

– prevenirea, cercetarea, identificarea și urmărirea penală a infracțiunilor;

---

15 Se poate ajunge la această concluzie deși unele state membre nu au furnizat specificații (a se vedea detaliile din tabelul 3).

– securitatea națională, apărarea și securitatea publică;

– interesele economice și financiare ale unui stat membru și ale UE (inclusiv aspectele monetare, bugetare și fiscale)[16];

– protejarea drepturilor și libertăților persoanei vizate sau a altor persoane.

În ceea ce privește **modul de acordare a accesului la datele cu caracter personal**, unele state membre au abordat această problemă în mod explicit, altele nu. Unele state membre au menționat că acordă persoanelor vizate dreptul de a trimite o cerere de acces la datele lor, direct autorității competente (și anume Austria, Germania, Bulgaria, Finlanda, Irlanda, Letonia, Malta, Țările de Jos, Polonia, Slovacia, Suedia, Regatul Unit), în timp ce altele acceptă numai accesul „indirect" (Belgia, Franța). În acest ultim caz, autoritatea națională de supraveghere, și nu persoana vizată, are acces la toate datele personale referitoare la persoana vizată. În Finlanda și Lituania, persoanele vizate au posibilitatea de a alege. În Portugalia, accesul direct este regula generală, însă există posibilitatea accesului indirect în cazurile în care prelucrarea datelor cu caracter personal are impact asupra securității statului sau asupra prevenirii sau cercetării infracțiunii. Situația este similară în Luxemburg, unde accesul general se acordă direct, dar în cazul în care se aplică o excepție, cererea de acces trebuie adresată autorității de supraveghere a protecției datelor.

Decizia-cadru conține norme generale care prevăd dreptul persoanelor vizate de a avea acces la datele lor. Decizia nu specifică detaliat ce tip de informații trebuie furnizate persoanei vizate. De asemenea, statele membre pot decide dacă persoanele vizate își pot exercita dreptul de acces direct sau dacă trebuie să recurgă la calea indirectă.

2.1.4. Autoritățile naționale de supraveghere (articolul 25)

Decizia-cadru 2008/977 recunoaște că instituirea în statele membre a unor autorități de supraveghere care își exercită funcțiile în deplină independență este „un element esențial al protecției datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare între statele membre" (considerentul 33). Aceasta prevede, de asemenea, că autoritățile de supraveghere deja existente în statele membre, în temeiul directivei „ar trebui, de asemenea, să poată" prelua această responsabilitate (considerentul 34). Articolul 25 din Decizia-cadru 2008/977 reflectă o parte importantă a prevederilor privind autoritățile de supraveghere prevăzute la articolul 28 [alineatele (1)-(4), alineatul (7)] din Directiva 95/46/CE în ceea ce privește competențele autorității, obligația sa de a acționa în deplină independență și secretul profesional. Fiecare autoritate trebuie să dispună de o serie de competențe, inclusiv competențe de cercetare (inclusiv accesul la date și colectarea informațiilor necesare), competențe efective de intervenție (ca de exemplu emiterea și publicarea unor avize anterior operațiunilor de prelucrare; dispunerea blocării, ștergerii sau distrugerii datelor; impunerea unei interdicții temporare sau definitive în ceea ce privește prelucrarea; avertizarea sau admonestarea inspectorului; supunerea chestiunii în atenția parlamentelor naționale sau a altor instituții politice și competența de a acționa în instanță.

Din tabelul 5 reiese că, în majoritatea cazurilor, autoritățile naționale de supraveghere responsabile de monitorizarea aplicării normelor generale în materie de protecție a datelor răspund, de asemenea, de supravegherea aplicării Deciziei-cadru 2008/977.

---

[16] Aceasta nu este o scutire menționată în mod expres la articolul 17 din Decizia-cadru 2008/977. Cu toate acestea, reflectă o scutire menționată la articolul 13 alineatul (1) din Directiva 95/46/CE.

Conform Suediei, Consiliul de inspectare a datelor nu a fost încă desemnat ca autoritate de supraveghere competentă în temeiul articolului 25 din decizia-cadru.

Unele state membre au ridicat în mod expres problema prelucrării datelor de către organele judiciare[17]. Danemarca a arătat că administrația instanțelor răspunde de supravegherea modului în care organele judiciare prelucrează datele, iar Austria a menționat că autoritatea de supraveghere din domeniul protecției datelor nu are competența de a lua decizii privind plângerile în legătură cu încălcarea normelor de protecție a datelor de către organele judiciare. În Luxemburg supravegherea prelucrării datelor este, în general, de competența Comisiei pentru protecția datelor. Activitățile de prelucrare efectuate în cadrul unei dispoziții de drept intern care pune în aplicare o convenție internațională sunt supravegheate de către o autoritate care este formată din *Procureur Général d'Etat* sau delegatul său și din doi membri ai Comisiei pentru protecția datelor, care sunt propuși de acesta din urmă și sunt numiți de ministru.

2.1.5. Alte probleme ridicate de statele membre

Din cele 26 de state membre, 20 de state membre, din care opt nu au răspuns la această întrebare (Belgia, Danemarca, Estonia, Grecia, Ungaria, Luxemburg, Cipru și Austria), nu au menționat probleme specifice în legătură cu decizia-cadru. După cum reiese din tabelul 6, șase state membre au formulat observații cu privire la problemele de interes pentru ele, precum următoarele aspecte:

- Polonia a considerat că decizia-cadru cuprindea numeroase deficiențe, care ar trebui remediate și și-a exprimat sprijinul pentru reformă în vederea instituirii unui sistem amplu și coerent de protecție a datelor la nivelul UE;

- Italia și Țările de Jos au semnalat dificultăți în ceea ce privește diferențierea în practică între prelucrarea transfrontalieră a datelor în temeiul Deciziei-cadru 2008/977 și prelucrarea la nivel național, precum și dificultatea aferentă pentru autoritățile de asigurare a aplicării legii din statele membre de a face față unor norme diferite de prelucrare a aceloraşi date cu caracter personal;

- Italia, Republica Cehă și Țările de Jos au criticat normele privind transferurile internaționale prevăzute de decizia-cadru. În special, Italia a declarat că este necesar să se prevadă un nivel adecvat și mai uniform de protecție a datelor pentru transferurile de date în țări terțe. Țările de Jos au considerat problematică lipsa de criterii din decizia-cadru pentru a stabili nivelul adecvat de protecție a unei țări terțe, având drept urmare aplicarea variabilă în statele membre. În fine, Republica Cehă a considerat că normele privind transferurile internaționale prevăzute de decizia-cadru sunt „nerealiste".

- Franța a făcut referire la o problemă specifică la nivel național cu privire la perioadele de stocare a datelor cu caracter personal transmise către și dintr-o țară terță, existând cerințe diferite în acest sens; - Slovacia a susținut că este necesar să se distingă mai bine între prelucrarea datelor de către poliție și organele judiciare (acțiunile în instanță);

---

[17] A se vedea considerentul 35 ultima teză din decizia-cadru, conform căreia competențele autorităților de supraveghere „nu ar trebui să afecteze normele specifice stabilite pentru procedurile penale sau independența justiției".

- Atât Republica Cehă, cât și Țările de Jos au arătat că obligativitatea respectării unor norme diverse de protecție a datelor la nivel internațional (ca de exemplu Consiliul Europei), la nivelul UE și la nivel național de către organele de asigurare a aplicării legii generează confuzie.

3. PERSPECTIVE

Prezentul raport evaluează stadiul aplicării și funcționării deciziei-cadru cu privire la protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală.

Dificultățile practice întâmpinate de o serie de state membre atunci când se face distincție între normele pentru prelucrarea datelor în context intern și internațional ar putea fi soluționate printr-un set unic de norme care reglementează prelucrarea datelor atât la nivel național, cât și în context transfrontalier. Domeniul de aplicare și eventualele scutiri la nivelul UE cu privire la dreptul persoanelor vizate la informare ar necesita clarificări suplimentare. Criteriile minime armonizate privind dreptul de acces al persoanelor vizate ar putea consolida drepturile persoanelor vizate, prevăzând în același timp scutiri pentru a permite poliției și organelor judiciare să își desfășoare în mod corect sarcinile.

În temeiul articolului 16 din Tratatul privind funcționarea Uniunii Europene, care consacră dreptul la protecția datelor cu caracter personal, există acum posibilitatea instituirii unui cadru cuprinzător pentru protecția datelor care asigură atât un nivel ridicat de protecție a datelor persoanelor fizice în domeniul cooperării polițienești și judiciare în materie penală, cât și schimbul de date cu caracter personal între autoritățile polițienești și judiciare ale statelor membre, în condiții mai bune, cu respectarea deplină a principiului subsidiarității.