AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei – Plan de acțiune pentru implementarea sistemelor de transport inteligente în Europa și propunerea însoțitoare de Directivă a Parlamentului European și a Consiliului de instituire a cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport

(2010/C 47/02)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolul 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,

având în vedere 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,

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, în special articolul 41,

având în vedere solicitarea unui aviz, primită la 11 februarie 2009 din partea Comisiei Europene, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001,

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

1. La 16 decembrie 2008, Comisia a adoptat comunicarea care definește planul de acțiune pentru implementarea sistemelor de transport inteligente în Europa (denumită în continuare „comunicarea") ([1]). Comunicarea este însoțită de o propunere de Directivă a Parlamentului European și a Consiliului de instituire a cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport (denumită în continuare „propunerea") ([2]). Comisia a transmis AEPD spre consultare comunicarea și propunerea însoțitoare, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 ([3]).

2. AEPD salută faptul că este consultată și recomandă ca această consultare să fie menționată în considerentele propunerii, astfel cum este menționată în alte texte legislative asupra cărora AEPD a fost consultată, în conformitate cu Regulamentul (CE) nr. 45/2001.

I.1. Comunicarea Comisiei – Plan de acțiune pentru implementarea sistemelor de transport inteligente în Europa

3. „Sistemele de transport inteligente" („STI") sunt aplicații avansate care utilizează tehnologiile informației și comunicațiilor (TIC) și care intră în componența diferitelor moduri de transport în vederea interacțiunii acestora. În domeniul transportului rutier, STI vor furniza servicii inovatoare, în modurile de transport și gestionarea traficului, diferiților utilizatori cum ar fi călătorii, utilizatorii și operatorii infrastructurii de transport rutier, administratorii parcurilor de vehicule și operatorii serviciilor de urgență.

4. Ținând seama de accentuarea implementării STI în diferite moduri de transport ([4]) în Uniunea Europeană, Comisia a adoptat un plan de acțiune care vizează accelerarea introducerii și utilizării aplicațiilor și serviciilor STI în domeniul

([1]) COM(2008) 886 final. Consiliul a adoptat concluziile privind comunicarea respectivă în cadrul celei de a 2935-a reuniuni a Consiliului Transporturi, Telecomunicații și Energie din 30-31 martie 2009.

([2]) COM(2008) 887 final.

([3]) 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.

([4]) Există numeroase inițiative la nivelul UE care integrează STI în diferitele moduri de transport, inclusiv transportul aerian (SESAR), căile navigabile interioare (RIS), traficul feroviar (ERTMS, TAF-TSI), transportul maritim (VTMIS, AIS, LRIT) și transportul rutier (eToll, eCall), a se vedea COM(2008) 886 final p. 3.

transportului rutier. Planul vizează de asemenea asigurarea interacțiunii cu alte moduri de transport, ceea ce va facilita furnizarea de servicii multimodale. Implementarea coerentă a STI în Europa va oferi avantaje în privința mai multor obiective comunitare, inclusiv eficiența, durabilitatea, siguranța și securitatea transportului, contribuind la piața internă a UE și la competitivitate. Dată fiind diversitatea obiectivelor urmărite pentru implementarea STI, comunicarea a evidențiat șase domenii prioritare de acțiune pentru perioada 2009-2014. În vederea punerii în aplicare a planului, Comisia propune definirea cadrului juridic la nivelul UE prin intermediul unei directive în care vor fi definite o serie de măsuri în domenii prioritare stabilite.

I.2. **Propunerea de Directivă a Parlamentului European și a Consiliului de instituire a cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport**

5. Propunerea stabilește cadrul pentru implementarea transnațională a aplicațiilor STI și vizează facilitarea asigurării unor servicii transfrontaliere armonizate, în special pentru informațiile de trafic și de călătorie și pentru managementul traficului. Aceasta prevede ca statele membre să ia anumite măsuri tehnice pentru facilitarea schimburilor de date între utilizatori, autoritățile publice, părțile interesate relevante și furnizorii de servicii STI și să integreze sistemele STI de siguranță și securitate în vehicule și în infrastructura rutieră. Specificațiile tehnice pentru aplicațiile și sistemele STI în patru domenii prioritare ([5]) enumerate în planul de acțiune vor fi definite prin procedura comitetului ([6]), elementele de bază ale acestora fiind specificate în anexa II. Scopurile specifice pentru care vor fi folosite STI în aceste domenii nu sunt totuși clare. Mai mult, implementarea STI se poate extinde la mult mai multe domenii decât cele patru stabilite inițial pentru elaborarea unor specificații tehnice armonizate. Deși propunerea vizează în principal implementarea viitoarelor aplicații și servicii STI, aceasta va viza de asemenea, acolo unde este posibil, tehnologiile existente sau actualmente în curs de dezvoltare în domeniu (precum eCall, eToll etc.).

6. Propunerea a fost transmisă Parlamentului European, care și-a adoptat poziția la prima lectură ([7]) la 23 aprilie 2009. În urma unei solicitări de consultare din partea Consiliului din 29 ianuarie 2009, Comitetul Economic și Social European a adoptat un aviz privind propunerea la 13 mai 2009 ([8]).

I.3. **Punctele centrale ale avizului**

7. AEPD salută consultarea privind propunerea de plan de implementare a STI înaintată de Comisie. Nu este prima dată când AEPD abordează chestiuni legate de planul de acțiune privind STI. AEPD a emis un aviz privind propunerea Comisiei de facilitare a aplicării transfrontaliere a normelor în domeniul siguranței rutiere ([9]) și a contribuit la lucrările Grupului de lucru „Articolul 29” privind un document de lucru referitor la eCall ([10]).

8. Sistemele inteligente de transport se bazează pe colectarea, prelucrarea și schimbul unor date extrem de variate, din surse publice și private; prin urmare, acestea reprezintă un domeniu cu o mare intensitate de date. Implementarea STI se va baza într-o mare măsură pe tehnologiile de geolocalizare, precum poziționarea prin satelit și tehnologiile fără contact, precum RFID, care vor facilita furnizarea unei game variate de servicii publice și/sau comerciale bazate pe localizare (de exemplu, informații despre trafic în timp real, eFreight, eCall, eToll, rezervări de locuri de parcare etc.). Unele informații care vor fi prelucrate prin STI sunt agregate – cum ar fi cele privind traficul, accidentele și posibilitățile – și nu privesc o persoană individuală, în timp ce alte informații sunt legate de persoane identificate sau identificabile și, prin urmare, reprezintă date cu caracter personal în sensul articolului 2 litera (a) din Directiva 95/46/CE.

9. AEPD consideră că este extrem de important ca acțiunile prevăzute pentru implementarea STI să fie coerente cu cadrul juridic existent, astfel cum a fost citat în propunere, în special cu Directiva 95/46/CE privind protecția datelor ([11]) și Directiva 2002/58/CE privind confidențialitatea și comunicațiile electronice ([12]).

([5]) Articolul 4 din propunere are în vedere definirea măsurilor tehnice în următoarele domenii: (i) utilizarea optimă a datelor rutiere, din trafic și de călătorie, (ii) continuitatea serviciilor STI de management al traficului și al mărfurilor pe coridoarele europene de transport și în aglomerațiile urbane, (iii) siguranța și securitatea rutieră și (iv) integrarea vehiculului în infrastructura de transport.

([6]) Propunerea stabilește o procedură de reglementare cu control, în conformitate cu articolul 5 alineatele (1)-(4) și cu articolul 7 din Decizia 1999/468/CE.

([7]) Rezoluția legislativă a Parlamentului European din 23 aprilie 2009 referitoare la propunerea de Directivă a Parlamentului European și a Consiliului de instituire a cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport, T6-0283/2009.

([8]) Avizul Comitetului Economic și Social European privind propunerea de Directivă a Parlamentului European și a Consiliului de instituire a cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport, TEN/382, 13 mai 2009.

([9]) Avizul Autorității Europene pentru Protecția Datelor privind propunerea de Directivă a Parlamentului European și a Consiliului de facilitare a aplicării transfrontaliere a normelor în domeniul siguranței rutiere, 2008/C 310/02, JO C 310, 5.12.2008, p. 9.

([10]) Documentul de lucru al Grupului de lucru „Articolul 29” referitor la protecția datelor și la implicațiile asupra vieții private în cadrul inițiativei privind eCall, WP 125, 26 septembrie 2006. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

([11]) 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, JO L 281, 23.11.1995, p. 31.

([12]) 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 (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37.

10. Chestiunile nesoluționate privind confidențialitatea și protecția datelor au fost identificate de Comisie ca fiind unul din principalele obstacole pentru promovarea STI. Aceste chestiuni vor fi dezvoltate în prezentul aviz după cum urmează:

— la capitolul II, cadrul juridic înaintat de Comisie pentru implementarea STI va fi analizat din perspectiva protecției datelor;

— capitolul III va evidenția chestiunile legate de protecția datelor care trebuie abordate mai îndeaproape pentru implementarea corespunzătoare a STI:

— ca un prim punct, avizul subliniază necesitatea asigurării „confidențialității încă din stadiul de proiect" în elaborarea STI și subliniază în continuare chestiunile importante care trebuie abordate în proiectarea aplicațiilor STI și a sistemelor de prelucrare a datelor;

— al doilea punct se va axa pe unele considerații legate de confidențialitate care trebuie abordate mai îndeaproape pentru furnizarea serviciilor STI.

II. ANALIZA CADRULUI JURIDIC PROPUS PENTRU IMPLEMENTAREA STI

11. Propunerea de directivă a Comisiei cuprinde două dispoziții [considerentul (9) și articolul 6] privind confidențialitatea, securitatea și reutilizarea informațiilor. Articolul 6 alineatul (1) din propunerea Comisiei prevede că operarea STI se efectuează în conformitate cu normele privind protecția datelor stabilite, *inter alia*, de Directiva 95/46/CE și de Directiva 2002/58/CE. Articolul 6 alineatul (2) din propunerea Comisiei are în vedere măsuri concrete de protecție a datelor, în principal din perspectiva securității: articolul 6 alineatul (2) din propunere prevede că „statele membre se asigură că datele și evidențele STI sunt protejate împotriva utilizării abuzive, în special împotriva accesului neautorizat, modificării sau pierderii". În fine, articolul 6 alineatul (3) din propunerea Comisiei prevede că „Directiva 2003/98/CE este aplicabilă".

12. La prima lectură, Parlamentul European a propus amendamente la articolul 6. În special, au fost adăugate trei noi paragrafe la articolul 6 alineatul (1) care vizează utilizarea datelor anonime, după caz, prelucrarea datelor sensibile numai cu consimțământul informat al persoanei vizate și garantarea faptului că datele cu caracter personal sunt prelucrate „numai dacă procesarea este necesară pentru buna funcționare a aplicației și/sau serviciului STI". De asemenea, articolul 6 alineatul (2) este modificat prin adăugarea faptului că datele și evidențele STI „nu pot fi utilizate în alte scopuri decât cele menționate în prezenta directivă."

13. AEPD salută faptul că a fost luată în considerare protecția datelor în redactarea propunerii și că aceasta reprezintă o condiție generală pentru implementarea corespunzătoare a STI în Europa. AEPD recunoaște faptul că este nevoie de o armonizare coerentă a prelucrării datelor la nivelul UE în scopul asigurării viabilității aplicațiilor și serviciilor STI în Europa.

14. Cu toate acestea, AEPD observă că acest cadru juridic propus este prea amplu și general pentru a putea aborda în mod corespunzător îngrijorările legate de confidențialitate și de protecția datelor, generate de implementarea STI în statele membre. Nu este clar în ce moment funcționarea serviciilor STI va duce la colectarea și prelucrarea de date cu caracter personal, care sunt scopurile precise pentru care sunt prelucrate datele și care este temeiul juridic care justifică o astfel de prelucrare. Mai mult, utilizarea tehnologiilor de localizare pentru implementarea STI generează riscul dezvoltării unor servicii intruzive din perspectiva confidențialității în cazul în care implică colectarea și schimbul de date cu caracter personal. Mai mult, propunerea nu stabilește clar rolurile și responsabilitățile diferiților operatori care intervin pe parcursul implementării STI și, prin urmare, este greu de stabilit care operatori vor fi operatori de date și vor răspunde ([13]), prin urmare, de respectarea obligațiilor privind protecția datelor. Operatorii STI se vor confrunta cu probleme deosebite în cazul în care aceste chestiuni nu sunt clarificate de actul juridic, dat fiind faptul că vor fi cei care, în ultimă instanță, vor fi însărcinați cu aplicarea măsurilor stabilite în directiva propusă.

15. Prin urmare, există riscul ca lipsa de claritate a cadrului juridic propus să creeze diversitate în implementarea STI în Europa, iar acest lucru, în loc să reducă diferențele dintre statele membre va duce, dimpotrivă, la incertitudine, fragmentare și incoerențe considerabile, din cauza nivelurilor diferite de protecție a datelor din Europa. Aceasta poate duce, de asemenea, la nerespectarea garanțiilor esențiale pentru protecția datelor. AEPD subliniază necesitatea armonizării în continuare a acestor chestiuni la nivelul UE. Prin urmare, AEPD recomandă modificări ale cadrului juridic propus din punctul de vedere al protecției datelor. Autoritatea recomandă ferm ca Parlamentul și Consiliul să insereze în propunere modificările propuse precum și, acolo unde este posibil, dispoziții suplimentare pentru

([13]) În conformitate cu articolul 2 litera (d), articolul 6 alineatul (2) și articolul 23 din Directiva 95/46/CE, menționată la nota 11.

clarificarea chestiunilor nesoluționate (precum definirea și responsabilitățile factorilor implicați în STI, elaborarea unor contracte armonizate pentru furnizarea de servicii STI etc.). AEPD subliniază, de asemenea, că statele membre vor avea responsabilitatea punerii în aplicare în mod corespunzător a directivei, astfel încât operatorii să poată dezvolta sisteme și servicii care oferă un nivel adecvat de protecție a datelor în întreaga Europă.

II.1. **Activitățile de prelucrare a datelor trebuie să se bazeze pe un cadru juridic corespunzător**

16. Nu este clar în ce moment va începe prelucrarea datelor cu caracter personal o dată ce echipamentul STI este integrat într-un vehicul sau potrivit cărui temei juridic va fi efectuată prelucrarea. Operatorii se pot baza pe diferite temeiuri juridice pentru prelucrarea datelor, între altele consimțământul neechivoc al utilizatorilor, un contract sau o obligație legală pe care operatorul trebuie să o respecte. Este necesară armonizarea temeiului juridic pe care se va baza prelucrarea datelor prin STI pentru a garanta faptul că sistemele funcționează în întreaga Europă și că utilizatorii nu au de suferit de pe urma divergențelor dintre modurile în care se desfășoară prelucrarea în fiecare țară a UE.

17. Într-o serie de cazuri, sistemele STI vor fi integrate din oficiu în vehicule. Este cazul, în special, al sistemelor STI de siguranță și securitate care trebuie să intre în componența vehiculelor în temeiul propunerii. Totuși, propunerea nu definește ce sunt „sistemele STI de siguranță și securitate" și ar trebui, prin urmare, clarificat mai în detaliu care anume sunt aplicațiile și sistemele STI care trebuie să intre în componența vehiculelor. Mai mult, ar trebui clarificat dacă activarea și utilizarea dispozitivului se va face voluntar sau va fi obligatorie pentru utilizatori. Alegerea efectuării prelucrării datelor pe o bază obligatorie ar trebui făcută numai pentru scopuri precise, pe baza unor justificări temeinice (de exemplu, urmărirea mărfurilor pentru managementul acestora) și cu garanții corespunzătoare în ceea ce privește prelucrarea datelor referitoare la persoane fizice. În cazul în care utilizarea STI se face pe o bază voluntară, ar trebui puse în aplicare garanții corespunzătoare pentru a preveni faptul ca, prin simpla prezență a sistemului în vehicul, să se considere că utilizatorii vehiculului au consimțit implicit la utilizarea acestui sistem.

18. AEPD este favorabilă opțiunii potrivit căreia serviciile STI sunt furnizate pe o bază voluntară. Aceasta implică faptul că utilizatorii trebuie să poată consimți liber la utilizarea sistemului și la scopurile particulare pentru care acesta va fi utilizat. Atunci când serviciul furnizat se bazează pe date de localizare, trebuie oferite informații corespunzătoare utilizatorului (în conformitate, în special, cu articolul 9 din Directiva 2002/58/CE), care trebuie să fie în măsură să își retragă consimțământul. Mai clar, aceasta implică introducerea unui mod simplu de dezactivare a dispozitivului și/sau a caracteristicii, fără constrângeri tehnice sau financiare pentru utilizator ([14]), atunci când utilizatorul nu mai este de acord cu utilizarea sistemului și/sau a unei caracteristici date. Ar trebui introduse garanții suplimentare pentru a garanta faptul că utilizatorii nu sunt discriminați atunci când refuză utilizarea unui serviciu.

19. În cazul în care anumite activități de prelucrare sunt obligatorii și altele sunt supuse consimțământului utilizatorului, trebuie asigurată transparența în legătură cu diferitele operațiuni efectuate de prelucrare a datelor, prin oferirea informațiilor corespunzătoare utilizatorilor în legătură cu natura obligatorie și/sau voluntară a fiecărei prelucrări în parte și cu sfera de cuprindere a acestei prelucrări. Mai mult, va fi esențială implementarea unor garanții de securitate corespunzătoare pentru ca nicio dată să nu fie culeasă și prelucrată în afara sferei de cuprindere stabilite prin lege și/sau convenite pe o bază voluntară.

20. Din perspectiva efectului transnațional al serviciilor STI, AEPD recomandă de asemenea elaborarea unor contracte paneuropene standard pentru a garanta că serviciile furnizate prin STI oferă aceleași garanții de protecție a datelor în toată Europa și, în special, că informațiile oferite utilizatorilor sunt suficient de clare în legătură cu caracteristicile specifice utilizate, cu impactul utilizării tehnologiilor specifice asupra protecției datelor acestora, și în legătură cu modul în care își pot exercita drepturile. Atunci când sunt adăugate noi caracteristici, ar trebui ca furnizorii de servicii să ia măsuri suplimentare pentru a oferi informații clare și specifice utilizatorilor în legătură cu aceste caracteristici suplimentare și pentru a obține în mod corespunzător consimțământul lor pentru utilizarea noilor caracteristici.

II.2. **Scopurile și modalitățile prelucrării datelor trebuie definite mai în detaliu**

21. AEPD observă că propunerea nu definește cu precizie serviciile și scopurile specifice pentru care aplicațiile STI ar putea fi utilizate, care rămân astfel deschise. Aceasta lasă loc pentru flexibilitate în practică, dar înseamnă că acele chestiuni nesoluționate privind confidențialitatea și protecția datelor – identificate de Comisie ca fiind unul din principalele obstacole pentru promovarea STI (a se vedea punctul 10) – pot rămâne nesoluționate și ar putea dăuna punerii în aplicare echilibrate a măsurilor propuse.

22. AEPD subliniază faptul că este deosebit de important ca operațiunile de prelucrare efectuate pentru furnizarea unor servicii STI specifice să nu fie efectuate doar în conformitate cu temeiul juridic adecvat, ci și pentru scopuri specificate, explicite și legitime și ca prelucrarea preconizată să fie proporțională și necesară pentru aceste scopuri (articolul 6 din Directiva 95/46/CE). Prin urmare, ar trebui analizată posibila necesitate a unor acte juridice suplimentare la nivelul UE cu privire la utilizările specifice ale STI în scopul garantării unui temei juridic armonizat și adecvat pentru activitățile de prelucrare care urmează să fie desfășurate și în scopul evitării discrepanțelor în implementarea serviciilor STI între statele membre.

23. Potrivit cadrului propus, nu s-au hotărât încă modalitățile prelucrării datelor și ale schimburilor de date pentru utilizarea STI. Numeroși parametri tehnici, a căror alegere va avea diferite implicații asupra confidențialității și protecției datelor, vor fi hotărâți abia ulterior, prin

([14]) A se vedea doc. WP 125 privind eCall, p. 4, menționat la nota 10.

procedura comitetului. Ținând seama de protecția specifică acordată confidențialității și de protecția datelor ca drepturi fundamentale apărate de articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale și de articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene, se poate pune întrebarea dacă și în ce măsură definirea operațiunilor de prelucrare a datelor ar trebui decisă prin procedura comitetului.

24. Într-o societate democratică, deciziile privind principiile și modalitățile esențiale care au impact asupra drepturilor fundamentale ar trebui luate în cadrul unei proceduri legislative complete, care include controalele corespunzătoare. În cazul de față, aceasta înseamnă că deciziile care au un impact major asupra confidențialității și protecției datelor persoanelor fizice, precum scopurile și modalitățile activităților de prelucrare a datelor cu caracter obligatoriu și definirea modalităților de implementare a STI în noi domenii, ar trebui adoptate de Parlamentul European și de Consiliu, și nu prin procedura comitetului.

25. Din această perspectivă, AEPD recomandă ferm ca Grupul de lucru „Articolul 29" și AEPD să fie implicate, atunci când acest lucru este relevant, în activitatea comitetului creat în temeiul articolului 8 din propunere și în acțiunile viitoare întreprinse în legătură cu implementarea STI, prin consultarea cu suficient timp înainte de elaborarea măsurilor relevante.

26. Mai mult, AEPD ia notă de amendamentele adoptate de Parlamentul European în legătură cu articolul 6 din propunere. AEPD constată în primul rând că amendamentul privind încurajarea, după caz, a utilizării datelor anonime, deși binevenit în principiu, nu va rezolva toate îngrijorările legate de protecția datelor, dat fiind faptul că numeroase date colectate și schimbate prin STI pot fi considerate date cu caracter personal. Pentru ca prelucrarea datelor cu caracter personal să se facă pe o bază anonimă, trebuie să nu existe nicio posibilitate pentru nimeni și în nicio etapă a prelucrării – ținând seama de toate mijloacele care ar putea fi folosite în mod rezonabil fie de către operator, fie de către orice altă persoană – de a asocia datele cu date privind o persoană identificată, altfel aceste date constituie date cu caracter personal în sensul articolului 2 litera (a) din Directiva 95/46/CE ([15]). Mai mult, pe baza amendamentelor propuse de Parlamentul European, AEPD recomandă modificarea articolului 6 din propunere după cum urmează:

— evaluarea necesității prelucrării datelor cu caracter personal prin STI ar trebui să aibă în vedere scopurile legitime și specifice pentru care datele sunt prelucrate (în conformitate cu articolele 6 și 7 din Directiva 95/46/CE). Funcționarea aplicației STI ([16]) nu poate reprezenta în sine un scop legitim care să justifice prelucrarea datelor, dat fiind faptul că aplicația este doar un mijloc de colectare și schimb de date, a căror utilizare trebuie în mod necesar orientată către scopuri specifice;

— amendamentul ([17]) referitor la interzicerea utilizării datelor și evidențelor STI „în alte scopuri decât cele menționate în prezenta directivă" nu oferă garanții suficiente, în special dat fiind faptul că scopurile specifice și serviciile pentru care STI vor fi utilizate nu sunt stabilite clar și exhaustiv în directivă. Având în vedere că se vor desfășura numeroase activități de prelucrare a datelor prin STI în scopuri cât se poate de variate, ar trebui garantat faptul că datele colectate în timpul prelucrării pentru un scop dat nu sunt utilizate în alte scopuri care sunt incompatibile, astfel cum prevede articolul 6 alineatul (1) litera (b) din Directiva 95/46/CE. În consecință, AEPD recomandă ca articolul 6 alineatul (2) să fie modificat în continuare pentru a se asigura că datele și evidențele STI nu sunt utilizate „în alte scopuri decât cele pentru care au fost colectate și într-un mod incompatibil cu aceste scopuri."

III. PROTECȚIA DATELOR ÎN CADRUL SISTEMELOR DE TRANSPORT INTELIGENTE

27. Este fundamental ca rolurile diferiților factori implicați în STI să fie clarificate pentru a identifica cine răspunde de garantarea funcționării corespunzătoare a sistemelor din perspectiva protecției datelor. Prin urmare, ar trebui clarificat mai în detaliu cine răspunde de implementarea aplicațiilor și sistemelor al căror proiect va fi stabilit prin procedura comitetului, precum și cine răspunde, din rândul factorilor implicați, pentru conformitatea prelucrării datelor cu legislația privind protecția datelor (și anume operatorii de date). AEPD va evidenția în continuare unele dintre îngrijorările legate de confidențialitate și de protecția datelor, care ar trebui abordate în cadrul procedurii comitetului și de către operatorii de date atunci când proiectează arhitectura aplicațiilor și sistemelor. De asemenea, Autoritatea va sublinia unele dintre chestiunile legate de protecția datelor care trebuie abordate de legiuitor și de operatorii de date cu privire la furnizarea serviciilor STI.

III.1. „Confidențialitatea încă din stadiul de proiect"

28. Aplicarea corectă a principiilor protecției datelor stabilite în Directiva 95/46/CE este o condiție de bază a succesului implementării STI în Comunitate. Aceste principii au implicații asupra proiectării arhitecturii sistemelor și aplicațiilor. AEPD recomandă adoptarea abordării „confidențialitate încă din stadiul de proiect" într-o etapă timpurie a

([15]) Astfel cum se precizează la considerentul 26 din Directiva 95/46/CE, „pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată".

([16]) Amendamentul 34 care introduce un nou articol 6 alineatul (1) litera (b) prevede că: „Datele cu caracter personal sunt prelucrate numai dacă procesarea este necesară pentru buna funcționare a aplicației și/sau serviciului STI".

([17]) Amendamentul 36 care introduce următorul text la articolul 6 alineatul (2): „și nu pot fi utilizate în alte scopuri decât cele menționate în prezenta directivă."

proiectării STI, pentru a defini arhitectura, operarea și managementul aplicațiilor și sistemelor. Această abordare este subliniată în mod deosebit în Directiva 1999/5/CE ([18]) în ceea ce privește proiectarea echipamentelor hertziene și echipamentelor terminale de telecomunicații.

29. Proiectarea aplicațiilor și sistemelor STI se va face în mai multe etape, de către diferiți factori, care ar trebui să țină cu toții seama de confidențialitate și de protecția datelor. Comisia și Comitetul STI vor avea responsabilitatea inițială specifică de a defini, prin procedura comitetului, măsurile, inițiativele de standardizare, procedurile și cele mai bune practici care ar trebui să promoveze „confidențialitatea încă din stadiul de proiect".

30. „Confidențialitatea încă din stadiul de proiect" ar trebui încurajată la toate nivelurilor proceselor și în toate formele acestora:

— la nivel organizațional, confidențialitatea ar trebui avută în vedere în definirea procedurilor necesare pentru schimbul de date între toate punctele de schimb relevante – acest lucru poate avea un impact direct asupra tipului de schimb și asupra tipului de date care fac obiectul schimbului – cerințele privind securitatea și confidențialitatea ar trebui încorporate în standarde, în cele mai bune practici, în specificațiile tehnice și în sisteme;

— cerințele privind securitatea și confidențialitatea ar trebui încorporate în standarde, în cele mai bune practici, în specificațiile tehnice și în sisteme;

— la nivel tehnic, AEPD recomandă elaborarea, de exemplu prin procedura comitetului, a celor mai bune tehnici disponibile ([19]) (BAT) privind confidențialitatea, protecția datelor și securitatea în sectoare specifice și/sau pentru anumite scopuri, în care diferiții parametri de securitate care trebuie puși în aplicare de-a lungul ciclului de viață al sistemului ar fi definiți pentru a garanta conformitatea cu cadrul de reglementare al UE.

31. AEPD atrage atenția asupra unora dintre aspectele care trebuie abordate în mod special în elaborarea aplicațiilor și arhitecturii sistemelor indicate mai jos. Acestea sunt legate de datele colectate, de interoperabilitatea sistemelor și de securitatea datelor.

III.1.(a) *Minimizarea datelor și anonimitatea*

32. În conformitate cu articolul 6 alineatul (1) litera (c) din Directiva 95/46/CE, numai datele cu caracter personal care sunt necesare și pertinente în ceea ce privește anumite scopuri pot fi colectate și prelucrate.

33. AEPD subliniază importanța realizării unei clasificări adecvate a informațiilor și datelor care urmează să fie prelucrate prin STI înainte de proiectarea aplicațiilor și sistemelor, pentru a evita o colectare masivă și inadecvată a datelor cu caracter personal. În acest sens, trebuie să fie avute în vedere:

— sursa datelor (dacă provin de la o sursă publică, un furnizor de telecomunicații, un furnizor de servicii STI, alți operatori, un vehicul, un utilizator de vehicul sau alte persoane vizate);

— natura datelor (de exemplu, informații agregate, date anonime, date cu caracter personal, date sensibile);

— scopul/scopurile în care se intenționează să fie utilizate datele și

— în ceea ce privește sistemele de cooperare, ar trebui să se clarifice care date sunt inserate/extrase de la vehicul, schimbate cu alt vehicul și/sau infrastructură sau între infrastructuri, și în ce scopuri.

34. Caracteristicile unice ar trebui să fie analizate cu atenție în conformitate cu scopurile urmărite pentru a evalua necesitatea colectării de date cu caracter personal. AEPD subliniază importanța atingerii echilibrului adecvat între drepturile fundamentale ale persoanelor vizate și interesele diverșilor actori implicați, ceea ce înseamnă că sunt prelucrate cât mai puține posibil date cu caracter personal. În cea mai mare măsură, arhitectura aplicațiilor și sistemelor ar trebui proiectată astfel încât să fie colectate numai datele cu caracter personal care sunt strict necesare pentru îndeplinirea obiectivelor care trebuie atinse.

35. În cazul în care datele cu caracter personal nu sunt necesare sau sunt necesare numai într-o fază inițială a prelucrării, acestea nu ar trebui colectate sau ar trebui făcute anonime cât mai repede posibil. Astfel, este deosebit de important nu numai să fie evaluată necesitatea colectării datelor, ci și necesitatea păstrării acestora în diferite sisteme. Termene-limită specifice pentru stocarea datelor cu caracter personal ar trebui definite pentru toți actorii lanțului de servicii, care ar trebui diferențiate în funcție de tipul de date și scopul pentru care au fost culese acestea ([20]). În consecință, atunci când păstrarea datelor cu caracter personal nu mai este necesară pentru scopurile pentru care acestea au fost culese sau prelucrate ulterior, acestea ar trebui făcute anonime, adică ar trebui să înceteze să fie legate de o persoană identificată sau identificabilă.

36. Proiectarea arhitecturii sistemelor și procedurile pentru schimbul de date ar trebui să vină în sprijinul prelucrării a cât mai puține date cu caracter personal posibil. În acest sens, ar trebui să se țină seama de toate etapele prelucrării și toți factorii care intervin în etapele furnizării de servicii STI. În timp ce unele date pot fi schimbate și prelucrate pe o bază anonimă, alte date, chiar și atunci când schimbul are loc pe bază neidentificată, pot fi asociate cu date privind o persoană identificată și, prin urmare, constituie

([18]) În special articolul 3 alineatul (3) litera (c) din Directiva 1999/5/CE a Parlamentului European și a Consiliului din 9 martie 1999 privind echipamentele hertziene și echipamentele terminale de telecomunicații și recunoașterea reciprocă a conformității acestora.

([19]) Cele mai bune tehnici disponibile înseamnă stadiul cel mai eficient și mai avansat în dezvoltarea activităților și a metodelor lor de exploatare care indică adecvarea din punct de vedere practic a anumitor tehnici pentru a constitui, în principiu, referința pentru ca aplicațiile și sistemele STI să fie în conformitate cu cerințele privind confidențialitatea, protecția datelor și securitatea, prevăzute de cadrul de reglementare al UE.

([20]) De exemplu, păstrarea datelor privind traficul și a datelor de localizare prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului prin rețele de comunicații publice este reglementată prin Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE.

date cu caracter personal în sensul articolului 2 litera (a) din Directiva 95/46/CE ([21]). Date fiind scopurile pentru care STI vor fi utilizate, pare a fi dificil să se garanteze că o cantitate mare de date culese prin STI vor fi prelucrate pe bază anonimă, deoarece identitatea persoanei va fi necesară la un moment dat pentru scopuri specifice, de exemplu pentru facturare. În consecință, ar fi necesară cel puțin luarea de măsuri speciale – tehnice, de organizare și legale – pentru asigurarea anonimității în anumite domenii.

III.1.(b) *Interoperability, data quality and purpose limitation*

37. Interoperabilitatea aplicațiilor și sistemelor este un element-cheie pentru implementarea cu succes a STI. Va avea loc o activitate de armonizare prin care vor fi definite specificațiile tehnice ale interfețelor care urmează să fie integrate, pentru a le permite să fie interoperaționale cu alte aplicații care intră în componența altor moduri și/sau sisteme de transport. În timp ce interoperabilitatea va sprijini facilitarea furnizării unei varietăți de servicii și va contribui la asigurarea continuității acestora pe Europa, aceasta ridică anumite riscuri din punct de vedere al protecției datelor, cum ar fi riscurile de utilizare incorectă sau abuzivă a datelor. Orice interconectare a bazelor de date ar trebui să aibă loc cu respectarea principiilor ([22]) protecției datelor și a garanțiilor practice privind securitatea [a se vedea, de asemenea, secțiunea III.1.(c)].

38. Principiul calității datelor enunțat la articolul 6 litera (d) din Directiva 95/46/CE este fundamental în special în contextul interoperabilității aplicațiilor și sistemelor. Specificațiile tehnice care urmează să fie definite pentru proiectarea interfețelor ar trebui să asigure acuratețea datelor care urmează să fie obținute ca rezultat al interconectării aplicațiilor și sistemelor.

39. Având în vedere că interoperabilitatea sistemelor va facilita interconectarea bazelor de date și asocierea datelor în alte scopuri, AEPD subliniază că orice interconectare ar trebui făcută acordând o atenție specială principiului limitării scopului, stabilit la articolul 6 alineatul (1) litera (b) din Directiva 95/46/CE. Este deosebit de important ca proiectarea arhitecturii sistemelor STI să prevină orice utilizare ulterioară a datelor în alte scopuri decât cele pentru care datele au fost culese. Măsuri adecvate de protejare a securității trebuie încorporate în sistem pentru a preveni utilizarea abuzivă, accesul sau divulgarea neautorizate, precum și efectele colaterale ale dispozitivelor. De exemplu, ar trebui implementate suficiente măsuri de protecție astfel încât dispozitivele nomade să nu fie accesate de părți terțe neautorizate și să nu fie utilizate pentru identificarea și urmărirea persoanelor dincolo de scopurile sistemului.

40. În ceea ce privește legalitatea interconectării înseși, aceasta va trebui evaluată pentru fiecare caz în parte, ținând seama de natura datelor care sunt puse la dispoziție și schimbate prin sisteme și de scopurile pentru care s-a intenționat inițial ca acestea să fie utilizate.

III.1.(c) *Securitatea datelor*

41. Securitatea datelor cu caracter personal este un element-cheie al implementării STI. AEPD salută faptul că securitatea este menționată în mod explicit în planul de acțiune și în propunerea de directivă. Securitatea ar trebui avută în vedere nu numai pe parcursul funcționării dispozitivului STI (în sistemele instalate la bordul vehiculelor și în protocolul de comunicare în transporturi), ci și dincolo de funcționarea dispozitivului – în bazele de date în care datele sunt prelucrate și/sau stocate. Ar trebui definite cerințe tehnice, administrative și organizaționale adecvate pentru toate etapele prelucrării, care să asigure un nivel adecvat de securitate în conformitate cu articolele 16 și 17 din Directiva 95/46/CE (precum și cu articolele 4 și 5 din Directiva 2002/58/CE, atunci când este relevant).

42. Definirea de măsuri de securitate adecvate ar trebui să aibă loc numai după evaluarea atentă a scopurilor specifice pentru care STI vor fi utilizate și a modalităților în care a avut loc prelucrarea. În acest sens, AEDP recomandă ca evaluările de impact ale confidențialității și protecției datelor să se desfășoare în legătură cu sectoarele și/sau cu scopurile specifice ale utilizării (de exemplu pentru sisteme STI de securitate, pentru sisteme de management al mărfurilor etc.). Efectuarea de evaluări de impact privind confidențialitatea și protecția datelor și utilizarea BAT pentru confidențialitatea și protecția datelor vor contribui la definirea celor mai adecvate măsuri de securitate relevante pentru prelucrările specifice efectuate.

III.2. **Considerații suplimentare legate de protecția datelor și de confidențialitate pentru furnizarea serviciilor STI**

43. Armonizarea în continuare a modalităților de implementare a serviciilor STI este necesară la nivelul UE pentru a preveni discrepanțele în implementarea serviciilor STI. În acest sens, AEDP ar dori să atragă atenția asupra celor două aspecte menționate în continuare, care vor necesita în mod special o examinare mai detaliată din punctul de vedere al confidențialității și protecției datelor:

— utilizarea instrumentelor de localizare pentru furnizarea de servicii publice și comerciale bazate pe localizare face necesară implementarea de garanții suplimentare. Într-un astfel de context, o atenție specială ar trebui acordată pentru a stabili dacă și când sunt utilizate servicii STI bazate pe localizare pentru scopuri private sau pentru scopuri profesionale și în ce mod sunt afectate de utilizarea unui astfel de sistem persoanele fizice care utilizează un vehicul în context profesional;

— este deosebit de important ca, în sistemele integrate, rolurile și responsabilitățile diferitelor părți implicate în implementarea STI să fie clarificate.

([21]) A se vedea nota de subsol 15.

([22]) A se vedea, de asemenea, comentariile AEPD referitoare la Comunicarea Comisiei privind interoperabilitatea bazelor de date europene, 10 martie 2006. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

III.2.(a) *Garanții pentru utilizarea instrumentelor de localizare pentru furnizarea de servicii STI bazate pe localizare*

44. Implementarea STI va sprijini dezvoltarea aplicațiilor „de localizare și de urmărire" a bunurilor și va permite implementarea serviciilor publice și comerciale bazate pe localizare. Astfel de servicii se vor baza pe utilizarea tehnologiilor, cum ar fi poziționarea prin satelit și etichetele RFID ([23]). Sistemele de navigație, de localizare și de urmărire se intenționează a fi utilizate pentru o varietate de scopuri, cum ar fi monitorizarea de la distanță, în trafic, a vehiculelor și a mărfurilor (de exemplu în cazul transportului de mărfuri periculoase sau de animale vii), facturarea vehiculelor pe baza unei diversități de parametri, inclusiv distanța parcursă sau anumite ore din zi (de exemplu tarifarea rutieră, sistemele de taxare rutieră electronică) și monitorizarea conducătorilor auto în vederea aplicării unor norme, cum ar fi verificarea duratei de conducere (prin tahografe digitale) și aplicarea de sancțiuni (prin identificarea electronică a vehiculelor).

45. Utilizarea tehnologiilor de localizare este în mod special intruzivă din perspectiva confidențialității deoarece permite urmărirea șoferilor și colectarea de date extrem de variate privind obiceiurile de conducere ale acestora. Astfel cum s-a subliniat de către Grupul de lucru „Articolul 29" ([24]), prelucrarea datelor de localizare este o chestiune deosebit de sensibilă care implică aspectul-cheie al libertății de a circula în mod anonim și care face necesară implementarea de garanții specifice în vederea prevenirii supravegherii persoanelor fizice și utilizării abuzive a datelor.

46. AEPD subliniază că utilizarea instrumentelor de localizare trebuie să fie legală, adică să aibă la bază un temei juridic adecvat, să aibă scopuri explicite și legitime și să fie proporțională cu scopurile de îndeplinit. Legalitatea prelucrării datelor va depinde în mare măsură de modul în care și de scopurile pentru care instrumentele de localizare vor fi folosite. Astfel cum subliniază Grupul de lucru „Articolul 29" în avizul său privind eCall, „nu ar fi acceptabil, din punctul de vedere al protecției datelor, să existe astfel de dispozitive conectate în mod permanent și, în consecință, vehicule care să poată fi urmărite în permanență în vederea posibilei activări a dispozitivelor eCall" ([25]). Prin urmare, este important să se clarifice mai bine circumstanțele specifice în care un vehicul va fi urmărit și impactul asupra utilizatorului. În orice caz, utilizarea dispozitivelor de localizare ar trebui să fie justificată printr-o nevoie legitimă (de exemplu monitorizarea transportului de mărfuri) și limitată strict la ceea ce este necesar pentru respectivul scop. Astfel, este important să se definească în mod precis ce date de localizare se colectează, unde sunt stocate acestea și pentru ce durată sunt păstrate, cu cine și în ce scopuri sunt schimbate, precum și să fie luate toate măsurile necesare pentru a evita orice utilizare incorectă sau abuzivă a datelor.

47. Mai mult, prelucrarea datelor de localizare privind utilizatori ai rețelelor de comunicații publice sau ai serviciilor de comunicații electronice accesibile publicului este strict reglementată prin articolul 9 al Directivei 2002/58/CE. Aceasta prevede în mod special faptul că prelucrarea datelor de localizare ar trebui efectuată pe bază de anonimat sau, în caz contrar, numai cu consimțământul explicit al utilizatorului. Aceasta înseamnă că, înainte de a conveni asupra utilizării unui instrument de localizare, trebuie să se pună la dispoziția utilizatorilor informațiile adecvate, inclusiv tipul de date de localizare prelucrate, scopurile și durata prelucrării și dacă datele vor fi transmise către o parte terță sau nu în vederea furnizării serviciului suplimentar. Trebuie să existe modalități simple, gratuite, pentru ca utilizatorii să poată refuza în mod temporar prelucrarea datelor de localizare pentru fiecare conectare la rețea sau pentru fiecare transmitere a unei comunicări. Prelucrarea datelor de localizare ar trebui să fie limitată strict la persoanele care acționează sub autoritatea furnizorului rețelei publice de comunicații sau al serviciului de comunicații accesibile publicului sau a unei părți terțe care furnizează serviciul suplimentar.

48. Garanții suplimentare trebuie adoptate în cazul în care datele de localizare sunt colectate de la vehicule care sunt utilizate în cursul activității profesionale, pentru a preveni utilizarea tehnologiei de localizare pentru monitorizarea nelegitimă a angajaților. În orice caz, prelucrarea ar trebui limitată la datele de localizare colectate pe durata timpului de lucru – astfel angajații sunt în măsură să deconecteze funcția de localizare în afara orelor de lucru și/sau atunci când utilizează vehiculul în scopuri private.

49. Există un risc ca părțile terțe (cum ar fi societățile de asigurări, angajatorii, autoritățile de aplicare a legii) să solicite accesul la datele colectate prin sistemele de navigație și urmărire, pentru scopuri legitime și specificate (cum ar fi urmărirea mărfurilor, taxarea rutieră electronică etc.) pentru a le utiliza în scopuri secundare, cum ar fi verificarea perioadelor de conducere și de repaus sau verificarea respectării regulilor de circulație și impunerea de sancțiuni. În principiu, accesul la date pentru scopuri secundare nu este permis dacă accesul servește unor scopuri care sunt incompatibile cu cele pentru care

([23]) A se vedea aspectele privind confidențialitatea și protecția datelor ridicate de utilizarea RFID în Avizul Autorității Europene pentru Protecția Datelor privind comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind „Identificarea prin radiofrecvență (RFID) în Europa: etape în direcția elaborării unei politici-cadru" COM(2007) 96, JO C 101, 23.4.2008, p. 1. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf

([24]) Grupul de lucru „Articolul 29", Aviz privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată, WP 115, noiembrie 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

([25]) A se vedea doc. WP 125 privind eCall, p. 5, menționat la nota 10.

acestea au fost colectate. Accesul poate fi permis numai pe baza unei derogări de la acest principiu în cazul în care condițiile pentru un astfel de acces îndeplinesc cerințele stricte prevăzute la articolul 13 din Directiva 95/46/CE. În consecință, orice acces la datele de localizare al părților terțe ar trebui acordat numai în conformitate cu legislația și în mod transparent, pe baza normei legale care stabilește procedurile și modalitățile adecvate de acces la date pentru scopuri specifice și care prevede garanții adecvate pentru persoanele fizice în conformitate cu scopurile suplimentare pentru care datele acestora ar putea servi.

III.2.(b) *Rolurile și responsabilitățile factorilor STI*

50. Încă nu este clar cine va fi operatorul de date în ceea ce privește fiecare parte a prelucrării. În numeroase cazuri, furnizorii de servicii STI vor fi probabil operatorii de date, fie în mod exclusiv în ceea ce privește datele cu caracter personal prelucrate în scopul furnizării propriilor lor servicii STI, fie în comun, în cazurile în care prelucrarea este efectuată împreună cu alți operatori de date. Operatorii implicați în STI în diferite capacități ar trebui să aibă rolul și responsabilitățile, în calitate de operator de date sau de responsabil de prelucrarea datelor, specificate în mod clar în ceea ce privește fiecare parte a prelucrării (de exemplu operatorii de telecomunicații care furnizează servicii de comunicații, precum și servicii STI).

51. Aceste persoane care exercită rolul de operatori de date vor fi responsabile ([26]) pentru asigurarea conformității sistemelor și serviciilor cu toate obligațiile de protecție a datelor și, în special, pentru implementarea sistemelor care includ „confidențialitatea încă din stadiul de proiect", care respectă principiile calității datelor și limitării scopului și care garantează un nivel adecvat de securitate a datelor, astfel cum este descris la Secțiunea III.1.

52. Operatorii de date vor trebui să se asigure că sunt instituite garanții adecvate la toate nivelurile lanțului de factori implicați în implementarea STI. Acest fapt va face necesar, în special, ca aceștia să intre în sisteme contractuale adecvate cu toate părțile interesate implicate în schimbul și prelucrarea datelor, care ar trebui să furnizeze garanții adecvate privind protecția datelor (în special în legătură cu articolele 16 și 17 din Directiva 95/46/CE și cu articolele 4 și 5 din Directiva 2002/58/CE). Este important să se ia act de faptul că, din punctul de vedere al protecției datelor, în timp ce operatorii de date trebuie să se asigure că protecția datelor este asigurată pentru toate etapele prelucrării, aceștia continuă să fie responsabili pentru prelucrare și nu pot exclude responsabilitatea lor prin contract.

IV. **CONCLUZII**

53. AEPD salută planul de implementare a STI propus de Comisie, având ca obiectiv armonizarea prelucrării datelor în întreaga Europă, în vederea facilitării furnizării de servicii STI și prin care protecția datelor este promovată ca o condiție fundamentală pentru implementarea corespunzătoare a STI în Europa.

54. AEPD ia notă de faptul că propunerea de directivă stabilește un cadru general care ridică o serie de probleme privind confidențialitatea și protecția datelor, care vor trebui abordate în continuare la nivelul UE și la nivel național:

— există riscul ca lipsa de claritate a cadrului juridic propus să creeze diversitate în implementarea STI în Europa, ceea ce va duce la niveluri diferite de protecție a datelor în Europa. AEPD subliniază necesitatea armonizării în continuare a acestor chestiuni la nivelul UE pentru clarificarea chestiunilor nesoluționate (cum ar fi definiția rolului și responsabilităților actorilor STI, care sunt aplicațiile și sistemele STI specifice care trebuie să intre în componența vehiculelor, elaborarea unor contracte armonizate pentru furnizarea de servicii STI, scopurile și modalitățile specifice ale utilizării STI etc.). Este fundamental să se identifice cine vor fi operatorii de date în ceea ce privește prelucrarea datelor efectuată, deoarece aceștia vor răspunde de garantarea faptului că, în toate fazele prelucrării, se va ține seama de considerentele privind confidențialitatea și protecția datelor;

— deciziile privind anumite modalități de prelucrare, care ar putea avea un impact major asupra dreptului persoanelor la confidențialitate și la protecția datelor, ar trebui luate de Parlamentul European și de Consiliu și nu prin procedura comitetului;

— este crucial să fie luate în considerare protecția datelor și confidențialitatea încă dintr-o etapă incipientă a prelucrării și în toate etapele prelucrării; implementarea „confidențialității încă din stadiul de proiect" ar trebui încurajată pentru proiectarea de aplicații și sisteme STI și ar trebui încorporată în standarde, în cele mai bune practici, în specificațiile tehnice și în sisteme;

— orice interconectare a aplicațiilor și sistemelor ar trebui efectuată cu respectarea corespunzătoare a principiilor protecției datelor și a garanțiilor practice de securitate;

— referitor la incertitudinile care mai există în acest stadiu privind modalitățile de implementare a STI, AEPD salută în special inițiativa înaintată de Comisie prin comunicarea acesteia conform căreia o evaluare a confidențialității va avea loc în 2011. În plus, AEPD recomandă cu fermitate ca evaluările de impact ale confidențialității și protecției datelor să se desfășoare în legătură cu sectoare și/sau scopuri specifice de utilizare pentru definirea de măsuri de securitate adecvate și recomandă eloborarea Celor mai bune tehnici disponibile privind confidențialitatea, protecția datelor și securitatea în cadrul STI;

— AEPD subliniază în continuare că statele membre vor avea responsabilitatea punerii în aplicare în mod corespunzător a directivei, astfel încât operatorii STI să implementeze sisteme și servicii care oferă un nivel adecvat de protecție a datelor în toată Europa;

([26]) A se vedea nota de subsol 13.

— garanții adecvate ar trebui implementate de operatorii de date care furnizează servicii STI astfel încât utilizarea tehnologiilor de localizare, precum poziționarea prin satelit și etichetele RFID, să nu fie intruzivă pentru viața privată a persoanelor care utilizează vehiculele într-un context strict privat sau într-un context profesional. Aceasta face necesară în special limitarea prelucrării la datele strict necesare în acest scop, asigurându-se că măsuri de securitate adecvate sunt încorporate în sisteme astfel încât datele de localizare să nu fie divulgate unor destinatari neautorizați și furnizând utilizatorilor mijloace eficiente de dezactivare a dispozitivului/caracteristicii de localizare.

55. AEPD recomandă ca articolul 6 al propunerii să fie modificat, în conformitate cu Directiva 95/46/CE, după cum urmează:

— ar trebui încurajată minimizarea datelor pentru prelucrarea datelor efectuată prin STI. În acest sens, se recomandă modificarea articolului 6 alineatul (1) litera (b) din propunere, după cum urmează: „Datele cu caracter personal sunt prelucrate numai dacă procesarea este necesară pentru scopul specific pentru care STI sunt utilizate și în conformitate cu temeiul juridic adecvat”;

— este important ca datele cu caracter personal prelucrate prin sisteme interoperabile să nu fie utilizate pentru alte scopuri care sunt incompatibile cu cele pentru care datele au fost colectate. Prin urmare, se recomandă modificarea articolului 6 alineatul (2) după cum urmează: „și nu pot fi utilizate în alte scopuri decât cele pentru care acestea au fost colectate și nici într-un mod incompatibil cu acele scopuri.”;

— AEPD recomandă adăugarea unei trimiteri explicite la noțiunea de „confidențialitate încă din stadiul de proiect” pentru proiectarea aplicațiilor și sistemelor STI în articolul 6 al propunerii. În plus, AEPD recomandă ca Grupul de lucru „Articolul 29” și AEPD să fie informate și consultate atunci când se întreprind acțiuni suplimentare pe această temă prin procedura comitetului.

56. AEPD recomandă în continuare ca această consultare să fie menționată în considerentele propunerii.

57. Având în vedere considerațiile anterioare, AEPD recomandă ca autoritățile pentru protecția datelor, în special Grupul de lucru „Articolul 29” și AEPD, să fie implicate îndeaproape în inițiativele privind implementarea STI, prin consultarea cu suficient timp înainte de elaborarea măsurilor relevante.

Adoptat la Bruxelles, 22 iulie 2009.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor