

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o sporočilu Komisije z naslovom „Akcijski načrt za uvajanje inteligentnih prometnih sistemov v Evropi“ ter spremljajočem predlogu direktive Evropskega parlamenta in Sveta o določitvi okvira za uvajanje inteligentnih prometnih sistemov v cestnem prometu in vmesnike do drugih vrst prevoza

(2010/C 47/02)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 286 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah in zlasti člena 8 Listine,

ob upoštevanju Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov,

ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij,

ob upoštevanju Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ter zlasti člena 41 Uredbe,

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki jo je 11. februarja 2009 prejel od Evropske komisije –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

1. Komisija je 16. decembra 2008 sprejela sporočilo o opredelitvi Akcijskega načrta za uvajanje inteligentnih prometnih

tnih sistemov v Evropi („sporočilo“) ⁽¹⁾. Sporočilo spremlja predlog direktive Evropskega parlamenta in Sveta o določitvi okvira za uvajanje inteligentnih prometnih sistemov v cestnem prometu in vmesnike do drugih vrst prevoza („predlog“) ⁽²⁾. Komisija je sporočilo in spremljajoči predlog poslala Evropskemu nadzorniku za varstvo podatkov (ENVP), da bi se z njim posvetovala v skladu s členom 28(2) Uredbe (ES) št. 45/2001 ⁽³⁾.

2. ENVP je zadovoljen, da je bil zaprosen za mnenje, in priporoča, da se na to posvetovanje sklicuje v uvodnih izjavah predloga na podoben način kot v številnih drugih zakonodajnih besedilih, v zvezi s katerimi je bil zaprosen za mnenje v skladu z Uredbo (ES) št. 45/2001.

I.1 Sporočilo Komisije – Akcijski načrt za uvajanje ITS v Evropi

3. „Inteligentni prometni sistemi“ (ITS) so napredne aplikacije, ki uporabljajo informacijske in komunikacijske tehnologije (IKT), ki so vgrajene v različne vrste prevoza za povezave med njimi. V cestnem prometu bodo ITS zagotavljali inovativne storitve na področju vrst prevoza in upravljanja prometa različnim uporabnikom, kot so potniki, uporabniki in upravljavci cestnoprometne infrastrukture ter upravljavci vozniških parkov in služb za nujno pomoč.

4. Komisija je ob ugotavljanju vse večjega uvajanja ITS v različnih vrstah prevoza ⁽⁴⁾ v Evropski uniji sprejela akcijski načrt za pospešitev uvajanja in uporabe aplikacij in storitev

⁽¹⁾ COM(2008) 886 konč. Svet je sprejel sklepe v zvezi s sporočilom na 2935. seji Sveta za promet, telekomunikacije in energijo 30. in 31. marca 2009.

⁽²⁾ COM(2008) 887 konč.

⁽³⁾ Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov, UL L 8, 12.1.2001, str. 1.

⁽⁴⁾ Na ravni EU je veliko pobud za integracijo ITS v različnih vrstah prevoza, vključno z zračnim prometom (SESAR), plovbo po celinskih plovniških poteh (RIS) ter železniškim (ERTMS, TAF-TSI), ladijskim (VTMIS, AIS, LRIT) in cestnim prometom (eToll, eCall), glej COM(2008) 886 konč., str. 3.

ITS na področju cestnega prometa. Namen načrta je tudi zagotavljati njihovo povezavo z drugimi vrstami prevoza, kar bo olajšalo izvajanje večmodalnih storitev. Skladno uvajanje ITS v Evropi bo služilo različnim ciljem Skupnosti, vključno z učinkovitostjo, trajnostjo, varnostjo in zanesljivostjo prevoza, v podporo notranjemu trgu EU in kot spodbuda konkurenčnosti. Glede na raznolikost ciljev, ki se uresničujejo v procesu uvajanja ITS, sporočilo opredeljuje šest prednostnih področij za ukrepanje v obdobju 2009–2014. Za izvedbo načrta Komisija predlaga, da se na ravni EU z direktivo določi pravni okvir, v katerem bodo na izbranih prednostnih področjih opredeljeni številni ukrepi.

1.2 Predlog direktive o določitvi okvira za uvajanje ITS v cestnem prometu in vmesnike do drugih vrst prevoza

5. Predlog določa okvir za transnacionalno uvajanje aplikacij ITS, katerega namen je olajšati izvajanje usklajenih čezmejnih storitev, zlasti za prometne in potovalne informacije ter upravljanje prometa. Od držav članic zahteva, da sprejmejo več tehničnih ukrepov za olajšanje izmenjave podatkov med uporabniki, javnimi organi, ustreznimi zainteresiranimi stranmi in ponudniki storitev ITS ter da v vozila in cestno infrastrukturo vključijo sisteme ITS, ki so povezani z varnostjo. Tehnične specifikacije za aplikacije in sisteme ITS na štirih prednostnih področjih izmed tistih⁽⁷⁾, navedenih v akcijskem načrtu, bodo opredeljene s postopkom komitologije⁽⁸⁾, katerega ključni elementi so določeni v prilogi II. Specifični nameni, za katere so bodo na teh področjih uporabljali ITS, pa niso jasni. Poleg tega se uvajanje ITS lahko razširi na veliko več področij kot le na tiste štiri, ki so bila prvotno izbrana za oblikovanje usklajenih tehničnih specifikacij. Čeprav predlog obravnava zlasti uvajanje prihodnjih aplikacij in storitev ITS, bo, kjer je to izvedljivo, vključeval tudi obstoječe ali trenutno razvijajoče se tehnologije na tem področju (kot so eCall, eToll itd.).

6. Predlog je bil poslan v Evropski parlament, ki je sprejel stališče v prvi obravnavi⁽⁷⁾ 23. aprila 2009. Na zahtevo Sveta za posvetovanje z dne 29. januarja 2009 je Evropski

⁽⁷⁾ Člen 4 predloga predvideva opredelitev tehničnih ukrepov na naslednjih področjih: (i) optimalna uporaba cestnih, prometnih in potovalnih podatkov, (ii) kontinuiranost upravljanja prometa in tovora v okviru storitev ITS na evropskih prometnih koridorjih in v sosedstvih, (iii) varnost v cestnem prometu ter (iv) vključitev vozila v prometno infrastrukturo.

⁽⁸⁾ Predlog določa regulativni postopek s pregledom v skladu s členom 5(a)(1) do (4) in členom 7 Sklepa 1999/468/ES.

⁽⁷⁾ Zakonodajna resolucija Evropskega parlamenta z dne 23. aprila 2009 o predlogu Direktive Evropskega parlamenta in Sveta o določitvi okvira za uvajanje inteligentnih prometnih sistemov v cestnem prometu in vmesnike do drugih vrst prevoza, T6-0283/2009.

ekonomsko-socialni odbor 13. maja 2009 sprejel mnenje o predlogu⁽⁸⁾.

1.3 Bistveni elementi mnenja

7. ENVP pozdravlja posvetovanje o predlaganem načrtu uvajanja ITS, ki ga je predstavila Komisija. ENVP se z vprašanji iz akcijskega načrta o ITS ne ukvarja prvič; izdal je že mnenje o predlogu Komisije o lažjem čezmejnem pregonu na področju varnosti v cestnem prometu⁽⁹⁾ in prispeval k delu Delovne skupine iz člena 29 v zvezi z delovnim dokumentom o sistemu eCall⁽¹⁰⁾.

8. Intelligentni prometni sistemi temeljijo na zbiranju, obdelavi in izmenjavi najrazličnejših podatkov iz javnih in zasebnih virov ter tako predstavljajo podatkovno intenzivno področje. Uvajanje ITS bo v veliki meri oprto na tehnologije geolociranja, kot so tehnologije za satelitsko določanje položaja, in brezkontaktno tehnologije, kot je RFID, ki bodo olajšale izvajanje vrste javnih in/ali komercialnih storitev, vezanih na lokacijo (npr. prometne informacije v realnem času, eFreight, eCall, eToll, rezervacija parkirnih mest itd.). Nekatere informacije, ki bodo obdelane prek ITS, se zbirajo – npr. o prometu, nesrečah in priložnostih – in se ne nanašajo na nobenega posameznika, medtem ko se druge informacije nanašajo na določene ali določljive posameznike in se tako obravnavajo kot osebni podatki v smislu člena 2(a) Direktive 95/46/ES.

9. Po mnenju ENVP je bistvenega pomena, da so ukrepi, načrtovani za uvajanje ITS, skladni z obstoječim pravnim okvirom, kakor je naveden v predlogu, zlasti z Direktivo 95/46/ES o varstvu podatkov⁽¹¹⁾ in Direktivo 2002/58/ES o zasebnosti in elektronskih komunikacijah⁽¹²⁾.

⁽⁸⁾ Mnenje Evropskega ekonomsko-socialnega odbora o predlogu direktive Evropskega parlamenta in Sveta o določitvi okvira za uvajanje inteligentnih prometnih sistemov v cestnem prometu in vmesnike do drugih vrst prevoza, TEN/382, 13. maj 2009.

⁽⁹⁾ Mnenje Evropskega nadzornika za varstvo podatkov o predlogu direktive Evropskega parlamenta in Sveta o lažjem čezmejnem pregonu na področju varnosti v cestnem prometu, 2008/C 310/02, UL C 310, 5.12.2008, str. 9.

⁽¹⁰⁾ Delovni dokument Delovne skupine iz člena 29 o varstvu podatkov in posledicah za zasebnost v okviru pobude eCall, WP 125, 26. september 2006. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

⁽¹¹⁾ Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, UL L 281, 23.11.1995, str. 31.

⁽¹²⁾ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), UL L 201, 31.7.2002, str. 37.

10. Komisija je odprta vprašanja na področju zasebnosti in varstva podatkov opredelila kot eno glavnih ovir pri spodbujanju ITS. V tem mnenju se ta vprašanja obravnavajo na naslednji način:

— v poglavju II bo pravni okvir, ki ga je Komisija predlagala za uvajanje ITS, analiziran z vidika varstva podatkov,

— v poglavju III bodo izpostavljeni pomisleki glede varstva podatkov, ki se jim je treba dodatno posvetiti za namen ustreznega uvajanja ITS:

— v prvi točki mnenja bo poudarjena potreba po spoštovanju zasebnosti pri načrtovanju v razvoju ITS, prav tako pa bodo dodatno orisana pomembna vprašanja, ki jih je treba rešiti pri načrtovanju aplikacij ITS in sistemov obdelave podatkov,

— v drugi točki bo poudarek na nekaterih pomislekih glede zasebnosti, ki se jim je treba dodatno posvetiti za namen izvajanja storitev ITS.

II. ANALIZA PRAVNEGA OKVIRA, PREDLAGANEGA ZA UVAJANJE ITS

11. Komisijin predlog direktive vsebuje dve določbi (uvodno izjavo 9 in člen 6), ki obravnavata zasebnost, varnost in ponovno uporabo podatkov. Člen 6(1) predloga Komisije zahteva, da se delovanje ITS izvaja v skladu s pravili o varstvu podatkov, ki so med drugim določena v Direktivi 95/46/ES in Direktivi 2002/58/ES. V členu 6(2) predloga Komisije so določeni konkretni ukrepi za varstvo podatkov predvsem z varnostnega vidika. V členu 6(2) predloga je navedeno, da „države članice [...] zagotovijo, da so podatki in zapisi ITS zaščiteni pred zlorabo, vključno z nepooblaščenim dostopom, spreminjanjem ali izgubo“. In končno, v členu 6(3) predloga Komisije je določeno, da se „uporablja [...] Direktiva 2003/98/ES“.

12. Evropski parlament je v prvi obravnavi predlagal spremembe člena 6. Natančneje, v členu 6(1) so dodani trije novi odstavki, ki zadevajo uporabo anonimnih podatkov, kadar je to primerno, obdelavo občutljivih podatkov le ob

svobodni privolitvi posameznika, na katerega se osebni podatki nanašajo, in zagotavljanje, da se osebni podatki obdelajo le, „če je obdelava potrebna za izvajanje aplikacij in/ali storitev ITS“. Člen 6(2) spreminja tudi dodana določba, da se podatkov in zapisov ITS „ne sme uporabiti za namene, ki niso navedeni v tej direktivi.“

13. ENVP pozdravlja dejstvo, da je bilo pri pripravi osnutka predloga upoštevano tudi varstvo podatkov in da je predlog predstavljen kot splošni pogoj za ustrezno uvajanje ITS v Evropi. ENVP priznava potrebo po skladni harmonizaciji podatkovnih procesov na ravni EU, s katero bi zagotovili učinkovitost aplikacij in storitev ITS po Evropi.

14. Vendar pa ENVP ugotavlja, da je predlagani pravni okvir preveč obširen in splošen, da bi ustrezno obravnaval pomisleke glede zasebnosti in varstva podatkov, ki jih odpira uvajanje ITS v državah članicah. Ni jasno, kdaj bo izvajanje storitev ITS privedlo do zbiranja in obdelave osebnih podatkov, kakšni so specifični nameni, zaradi katerih prihaja do obdelave podatkov, pa tudi ne, kakšna je pravna podlaga, ki takšno obdelavo upravičuje. Poleg tega uporaba lokacijskih tehnologij za namen uvajanja ITS povečuje tveganje razvoja storitev, ki so moteče z vidika zasebnosti, če vključujejo zbiranje in izmenjavo osebnih podatkov. Poleg tega iz predloga niso jasno razvidne vloge in odgovornosti različnih operaterjev, ki posredujejo v verigi uvajanja ITS, zaradi česar je težko ugotoviti, kateri operaterji bodo upravljavci podatkov in torej odgovorni⁽¹³⁾ za izpolnjevanje obveznosti glede varstva podatkov. Če vsa ta vprašanja ne bodo pojasnjena z zakonom, se bodo upravljavci ITS znašli pred velikimi težavami, saj bodo na koncu prav oni odgovorni za izvajanje ukrepov iz predlagane direktive.

15. Zato obstaja tveganje, da bo predlagani pravni okvir s svojo nejasnostjo privedel do različnih načinov izvajanja ITS v Evropi in da ne bo zmanjšal razlik med državami članicami, temveč da bo zaradi različnih ravni varstva podatkov v Evropi povzročil precejšnjo negotovost, drobljenje in nedoslednosti. To bi lahko privedlo tudi do neizpolnjevanja bistvenih zaščitnih ukrepov za varstvo podatkov. ENVP izpostavlja potrebo po nadaljnjem usklajevanju pri teh vprašanjih na ravni EU. ENVP bo predlagal spremembe predlaganega pravnega okvira z vidika varstva podatkov. Močno priporoča, da Parlament in Svet v predlog vneseta predlagane spremembe, pa tudi, kjer je

⁽¹³⁾ Skladno s členi 2(d), 6(2) in 23 Direktive 95/46/ES, omenjene v opombi 11.

to izvedljivo, dodatne določbe za razjasnitev odprtih vprašanj (kot so opredelitev in odgovornosti akterjev ITS, oblikovanje usklajenih pogodb za zagotavljanje storitev ITS itd.). Poleg tega poudarja, da bodo tudi države članice odgovorne za izvajanje direktive na ustrezen način, tako da lahko operaterji razvijajo sisteme in storitve, ki ponujajo ustrezno raven varstva podatkov po Evropi.

II.1 Dejavnosti v zvezi z obdelavo podatkov morajo biti oprte na ustrezno pravno podlago

16. Ni jasno, kdaj se bo obdelava osebnih podatkov začela, potem ko je oprema ITS vgrajena v vozilo, in na kakšni pravni podlagi bo izvedena obdelava. Operaterji se lahko pri obdelavi podatkov opirajo na različne pravne podlage, med drugim na nedvoumno privolitev uporabnikov, pogodbo ali zakonsko obveznost, ki jo bo izpolnil upravljavec podatkov. Uskladiti je treba pravno podlago, na kateri se bo izvajala obdelava podatkov prek ITS, da bi tako zagotovili, da sistemi delujejo po celi Evropi in da uporabniki ne trpijo zaradi različnih načinov obdelave v posameznih državah EU.

17. V številnih primerih bodo sistemi ITS avtomatično vgrajeni v vozila. To še zlasti velja za sisteme ITS, ki omogočajo večjo varnost in ki morajo biti vgrajeni v vozila v skladu s predlogom. Vendar pa predlog ne opredeljuje, kaj „sistemi ITS, ki omogočajo večjo varnost“ sploh so, zato je treba dodatno pojasniti, katere so specifične aplikacije in sistemi ITS, ki morajo biti vgrajeni v vozila. Poleg tega je treba pojasniti, ali bosta aktiviranje in uporaba naprave za uporabnike izvedena prostovoljno ali obvezno. Odločitev za obvezno izvedbo obdelave podatkov se lahko sprejme le za posebne namene ob upoštevanju prepričljivih razlogov (npr. sledenje blaga za upravljanje tovora) in z ustreznimi zaščitnimi ukrepi, kar zadeva obdelavo podatkov, ki se nanašajo na posameznike. Če je uporaba ITS prostovoljna, je treba z izvedbo ustreznih zaščitnih ukrepov preprečiti, da se zaradi samega obstoja sistema v vozilu ne bi štel, da so uporabniki molče privolili v njegovo uporabo.

18. ENVP meni, da je ustreznije prostovoljno zagotavljanje storitev ITS. To pomeni, da morajo imeti uporabniki možnost, da svobodno privolijo v uporabo sistema in posebne namene njegove uporabe. Kadar zagotovljena storitev temelji na podatkih o lokaciji, je treba uporabniku dati na voljo ustrezne informacije (v skladu zlasti s členom 9 Direktive 2002/58/ES) in mu omogočiti, da umakne svojo privolitev. To v praksi zahteva uvedbo enostavnega deaktiviranja naprave in/ali funkcije brez tehničnih ali finančnih obveznosti za uporabnika⁽¹⁴⁾, kadar se ta ne strinja več z uporabo sistema in/ali posamezne funkcije. Izvajati bi bilo treba dodatne varnostne ukrepe, da uporabniki v primeru zavrnitve uporabe storitve ne bi bili diskriminirani.

19. Kadar so nekatere dejavnosti v zvezi z obdelavo obvezne, za druge pa je potrebna privolitev uporabnika, je treba zagotoviti preglednost različnih opravljenih postopkov za obdelavo podatkov, in sicer z zagotavljanjem ustreznih informacij uporabnikom o obvezni ali prostovoljni naravi posamezne obdelave in njenem obsegu. Poleg tega bo treba izvajati ustrezne zaščitne ukrepe za zagotovitev varnosti, da bi preprečili zbiranje in obdelavo podatkov zunaj zakonsko določenega obsega in/ali obsega, določenega s prostovoljno privolitvijo.

20. ENVP ob upoštevanju transnacionalnega učinka storitev ITS priporoča tudi oblikovanje vseevropskih standardnih pogodb, s katerimi bi zagotovili, da se pri storitvah ITS izvajajo enaki zaščitni ukrepi za varstvo podatkov po vsej Evropi ter da so informacije za uporabnike glede uporabljenih posebnih funkcij, učinka uporabe posebnih tehnologij za varstvo njihovih podatkov in uveljavljanja njihovih pravic dovolj jasne. Ponudniki storitev morajo pri dodajanju novih funkcij poskrbeti za jasne in konkretne informacije za uporabnike glede teh dodatnih funkcij ter pridobiti ustrezno privolitev za njihovo uporabo.

II.2 Namene in načine obdelave podatkov je treba podrobneje opredeliti

21. ENVP opozarja, da predlog ne opredeljuje dovolj podrobno posebnih storitev in namenov možne uporabe aplikacij ITS, ki ostajajo nedorečeni. To sicer omogoča prilagodljivost v praksi, vendar pomeni, da utegnejo odprta vprašanja na področju zasebnosti in varstva podatkov, ki jih je Komisija opredelila za eno glavnih ovir pri spodbujanju ITS (glej točko 10), ostati nerešena in ovirati uravnoteženo izvajanje predlaganih ukrepov.

22. ENVP poudarja, da je zelo pomembno, da se postopki obdelave pri zagotavljanju posebnih storitev ITS ne izvedejo zgolj v skladu z ustrezno pravno podlago, pač pa tudi za posebne, izrecne in legitimne namene, ter da je predvidena obdelava potrebna in sorazmerna s temi nameni (člen 6 Direktive 95/46/ES). Razmisliti bi bilo torej treba o dodatni zakonodaji na ravni EU glede posebnih uporab ITS, da bi zagotovili usklajen in ustrezen pravni okvir za izvedbo dejavnosti v zvezi z obdelavo ter preprečili različno uvajanje storitev ITS v posameznih državah članicah.

23. V predlaganem okviru načini obdelave podatkov in izmenjave podatkov za uporabo ITS še niso opredeljeni. Mnogi tehnični parametri, izbor katerih bo različno vplival na zasebnost in varstvo podatkov, bodo določeni pozneje v okviru postopka komitologije. Ob upoštevanju, da sta zasebnost in varstvo podatkov kot temeljni pravici še

⁽¹⁴⁾ Glej WP 125 o klicu v sili (eCall), str. 4, naveden v opombi 10.

posebej zaščiteni s členom 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin ter člena 7 in 8 Listine Evropske unije o temeljnih pravicah, bi se lahko zastavilo vprašanje, ali je primerno, da se postopki obdelave podatkov opredelijo s postopkom komitologije, in do kakšne mere.

24. V demokratični družbi je treba odločitve o bistvenih načelih in načinih, ki vplivajo na temeljne pravice, sprejemati s celotnim zakonodajnim postopkom, v katerega so vključeni tudi ustrezni pregledi in protiuteži. V tem konkretnem primeru bi morala odločitve o vprašanih, ki bistveno vplivajo na zasebnost in varstvo osebnih podatkov, kot so nameni in načini izvajanja obveznih dejavnosti v zvezi z obdelavo podatkov ter opredelitev načinov uvajanja ITS na novih področjih, sprejemati Evropski parlament in Svet, ne pa komitologija.
25. ENVP glede na navedeno močno priporoča, da Delovna skupina iz člena 29 in ENVP po potrebi sodelujeta pri delu odbora iz člena 8 predloga in pri prihodnjih sprejetih ukrepih za uvajanje ITS, in sicer v okviru dovolj zgodnjih posvetovanj še pred oblikovanjem zadevnih ukrepov.
26. ENVP se je tudi seznanil s spremembami, ki jih je v povezavi s členom 6 predloga sprejel Evropski parlament; v zvezi s spremembo glede spodbujanja uporabe anonimnih podatkov, kadar je to primerno, opozarja, da je načeloma sicer pozitivna, vendar ne rešuje vseh pomislekov glede varstva podatkov, saj se veliko podatkov, ki se zbirajo in izmenjujejo prek ITS, lahko obravnava kot osebne podatke. Da bi se osebni podatki lahko obdelovali anonimno, bi moralo biti vsem osebam v vseh fazah obdelave – ob upoštevanju vseh sredstev, ki bi jih najverjetneje uporabila upravljavec ali katera druga oseba – onemogočeno, da bi podatke povezali s podatki o določenem posamezniku. V nasprotnem primeru so tovrstni podatki opredeljeni kot osebni podatki v smislu člena 2(a) Direktive 95/46/ES ⁽¹⁵⁾. ENVP poleg tega na podlagi sprememb, ki jih je predlagal Evropski parlament, priporoča, da se člen 6 predloga spremeni, kakor sledi:

— Potrebo po obdelavi osebnih podatkov z ITS bi bilo treba oceniti ob upoštevanju legitimnih in določenih namenov, za katere se obdelujejo podatki (v skladu s

členoma 6 in 7 Direktive 95/46/ES). Izvajanje aplikacij ITS ⁽¹⁶⁾ samo po sebi ne more biti zakonit namen, ki upravičuje obdelavo podatkov, saj je aplikacija le sredstvo za zbiranje in izmenjavo podatkov, njena uporaba pa bi morala biti usmerjena v konkretne namene.

- Sprememba ⁽¹⁷⁾ glede prepovedi uporabe podatkov in zapisov ITS „za namene, ki niso navedeni v tej direktivi“, ne določa ustreznih zagotovil, zlasti zato, ker določeni nameni in storitve, za katere se bodo uporabljali ITS, v direktivi niso jasno in dovolj podrobno navedeni. Glede na to, da se bodo z ITS izvajale različne dejavnosti v zvezi z obdelavo podatkov za najrazličnejše namene, bi bilo treba zagotoviti, da se podatki, zbrani pri obdelavi za določen namen, ne uporabijo za druge namene, ki so nezdružljivi (kot je določeno v členu 6(1)(b) Direktive 95/46/ES). ENVP zato priporoča, da bi bilo treba člen 6(2) nadalje spremeniti, da bi zagotovili, da se podatki in zapisi ITS ne uporabijo „za namene, ki niso nameni, za katere so bili zbrani, na način, ki je nezdružljiv s temi nameni“.

III. VARSTVO PODATKOV PRI INTELIGENTNIH PROMETNIH SISTEMIH

27. Zelo pomembno je, da se jasno opredelijo vloge posameznih akterjev, ki sodelujejo pri ITS, da bi določili osebe, odgovorne za zagotavljanje pravnega delovanja sistemov z vidika varstva podatkov. Zato bi bilo treba nadalje pojasniti, kdo bo odgovoren za izvajanje aplikacij in sistemov, katerih načrti bodo podrobneje določeni s postopkom komitologije, ter kdo od vrste akterjev bo odgovoren za to, da bo obdelava podatkov skladna z zakonodajo o varstvu podatkov (t. i. upravljavci podatkov). ENVP v nadaljnjem besedilu opozarja na nekatere pomisleke v zvezi z zasebnostjo in varstvom podatkov, ki bi jih bilo treba pri načrtovanju strukture aplikacij in sistemov obravnavati v postopku komitologije. Poleg tega navaja nekaj vprašanih varstva podatkov, ki jih morajo zakonodajalec in upravljavci podatkov obravnavati v zvezi z zagotavljanjem storitev ITS.

III.1 Spoštovanje zasebnosti pri načrtovanju

28. Spoštovanje načel varstva podatkov iz Direktive 95/46/ES je temeljni pogoj za uspešno uvajanje ITS v Skupnosti. Ta načela vplivajo na načrtovanje strukture sistemov in aplikacij. ENVP priporoča, da se pristop spoštovanja zasebnosti pri načrtovanju sprejme že v zgodnji fazi načrtovanja ITS,

⁽¹⁵⁾ Kot je navedeno v uvodni izjavi 26 Direktive 95/46/ES, bi bilo treba „za odločitev o tem, ali je oseba določljiva ali ne, upoštevati vsa sredstva, za katera se pričakuje, da jih bo uporabil bodisi upravljavec ali katera koli druga oseba za določitev take osebe.“

⁽¹⁶⁾ Sprememba 34, ki uvaja nov člen 6(1)(b), se glasi: „Osebni podatki se obdelajo le, če je obdelava potrebna za izvajanje aplikacij in/ali storitev ITS.“

⁽¹⁷⁾ V spremembi 36 se členu 6(2) doda naslednje besedilo: „in da se jih ne sme uporabiti za namene, ki niso navedeni v tej direktivi.“

- da bi tako lahko opredelili strukturo, delovanje in upravljanje aplikacij in sistemov. Ta pristop je zlasti poudarjen v Direktivi 1999/5/ES⁽¹⁸⁾ glede načrtovanja radijske in telekomunikacijske terminalne opreme.
29. Načrte aplikacij in sistemov ITS bodo v več fazah pripravili različni akterji, ki bi pri tem vsi morali upoštevati zasebnost in varstvo podatkov. Komisija in odbor za ITS bosta nosila specifično začetno odgovornost pri določitvi ukrepov, pobud za standardizacijo, postopkov in dobrih praks za spodbujanje spoštovanja zasebnosti pri načrtovanju, in sicer v postopku komitologije.
30. Spoštovanje zasebnosti pri načrtovanju bi bilo treba spodbujati v vseh fazah najrazličnejših postopkov:
- Načelo zasebnosti bi bilo treba na organizacijski ravni upoštevati pri določitvi potrebnih postopkov za izmenjavo podatkov med vsemi zadevnimi točkami za izmenjavo, kar bi lahko neposredno vplivalo na vrsto izmenjave in vrsto izmenjanih podatkov.
 - Zahteve na področju zasebnosti in varnosti bi bilo treba vnesti v standarde, dobre prakse, tehnične specifikacije in sisteme.
 - ENVP na tehnični ravni priporoča razvoj (na primer s postopkom komitologije) najboljših razpoložljivih tehnologij⁽¹⁹⁾ (NRT) za zasebnost, varstvo podatkov in varnost v specifičnih sektorjih in/ali za posebne namene, v katerih bi bili določeni različni varnostni parametri, ki jih je treba izvajati v celotnem življenjskem ciklu sistema, da bi zagotovili skladnost z regulativnim okvirom EU.
31. ENVP opozarja na nekatera vprašanja, ki jih je treba pri načrtovanju aplikacij in strukture sistemov, navedenih v nadaljnjem besedilu, še zlasti obravnavati. Nanašajo se na zbrane podatke, medobratovnost sistemov in varnost podatkov.
- III.1(a) *Zmanjšanje količine podatkov in anonimnost*
32. V skladu s členom 6(1)(c) Direktive 95/46/ES se lahko zbirajo in obdelujejo le osebni podatki, ki so potrebni in pomembni za posebne namene.
33. ENVP poudarja, da je treba informacije in podatke, ki bodo obdelani z ITS, ustrezno razvrstiti še pred načrtovanjem aplikacij in sistemov, da bi tako preprečili množično in neustrezno zbiranje osebnih podatkov. Pri tem je treba upoštevati:
- vir podatkov (javni vir, ponudnik telekomunikacijskih storitev, ponudnik storitev ITS, drugi upravljavci, vozilo, uporabnik vozila ali druge osebe, na katere se podatki nanašajo),
 - vrsto podatkov (npr. zbrani, anonimni, osebni ali občutljivi podatki),
 - namen(-e) predvidene uporabe podatkov.
 - V zvezi s sistemi sodelovanja bi bilo treba jasno določiti, kateri podatki se pošljejo v vozilo/pridobijo iz vozila, izmenjajo z drugim vozilom in/ali infrastrukturo ter pošljejo od ene infrastrukture do druge infrastrukture ter za katere namene.
34. Posamezne funkcije bi bilo treba podrobno preučiti glede na določene namene, da bi ocenili potrebo po zbiranju osebnih podatkov. ENVP poudarja, da je treba doseči ustrezno ravnovesje med temeljnimi pravicami oseb, na katere se podatki nanašajo, in interesi različnih sodelujočih akterjev, to pa pomeni, da se obdelava kar najmanj osebnih podatkov. Strukturo aplikacij in sistemov bi bilo treba v največji možni meri načrtovati tako, da se zbirajo le osebni podatki, ki so resnično potrebni za doseganje namenov.
35. Če osebni podatki niso potrebni ali so potrebni le v začetni fazi obdelave, ne bi smeli biti zbrani ali pa bi morali biti čim prej spremenjeni v anonimne podatke. Zato je še zlasti pomembno, da se ne oceni le potreba po zbiranju podatkov, pač pa tudi njihova hramba v različnih sistemih. Za vse akterje v verigi storitev bi bilo treba določiti posebne časovne omejitve za hrambo osebnih podatkov, ki bi se razlikovale glede na vrsto podatkov in namen, za katerega so se zbirali⁽²⁰⁾. Ko njihova hramba ne bi bila več potrebna za doseganje namenov, za katere so bili zbrani ali nadalje obdelani, bi jih bilo treba spremeniti v anonimne podatke, t. j. spremeniti tako, da se ne bi več nanašali na določene ali določljive posameznike.
36. Načrtovanje strukture sistemov in postopki izmenjave podatkov bi morali podpirati obdelavo kar najmanjše količine osebnih podatkov. Zato bi bilo treba v zvezi s tem upoštevati vse faze obdelave in vse akterje v verigi zagotavljanja storitev ITS. Nekatero podatke je sicer mogoče izmenjati in obdelati anonimno, druge podatke pa je kljub izmenjavi, pri kateri ostanejo neprepoznavni, možno povezati s podatki, ki se nanašajo na določene posameznike in se zato opredelijo kot osebni podatki v

⁽¹⁸⁾ Predvsem člen 3(3)(c) Direktive 1999/5/ES Evropskega parlamenta in Sveta z dne 9. marca 1999 o radijski opremi in telekomunikacijski terminalni opremi ter medsebojnem priznavanju skladnosti te opreme.

⁽¹⁹⁾ Najboljše razpoložljive tehnologije pomenijo najučinkovitejše in najbolj razvite dejavnosti ter njihove metode delovanja, ki kažejo praktično ustreznost posameznih tehnologij, s katerimi se načeloma lahko zagotovi, da bodo sistemi in aplikacije ITS skladni z načeli varstva zasebnosti in podatkov ter z varnostnimi zahtevami, določenimi v regulativnem okviru EU.

⁽²⁰⁾ Hramba podatkov o prometu in lokaciji, obdelanih v zvezi z zagotavljanjem javnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih je na primer urejena v Direktivi 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES.

smislu člena 2(a) Direktive 95/46/ES ⁽²¹⁾. Glede na namene, za katere se bodo uporabljali ITS, se zdi skorajda nemogoče zagotoviti, da se bo velika količina podatkov, zbrana z ITS, obdelala anonimno, saj bodo podatki o identiteti posameznika potrebni za posebne namene, kot je izdaja računov. Zato bi bili za zagotovitev anonimnosti na nekaterih področjih potrebni vsaj posebni – tehnični, organizacijski in pravni – ukrepi.

III.1(b) Medobratovalnost, kakovost podatkov in omejitve namena

37. Medobratovalnost aplikacij in sistemov je ključni element za uspešno uvajanje ITS. Opravljeno bo usklajevalno delo, prek katerega bodo opredeljene tehnične specifikacije vmesnikov, ki bodo vključeni v aplikacije in sisteme, da bi se jim omogočila medobratovalnost z drugimi aplikacijami, vgrajenimi v druge vrste in/ali sisteme prevoza. Medobratovalnost sistemov bo sicer pomagala olajšati izvajanje številnih storitev in prispevala k zagotavljanju njihove kontinuitete po vsej Evropi, po drugi strani pa predstavlja določeno tveganje z vidika varstva podatkov, kot so tveganja nepravilne uporabe ali zlorabe podatkov ⁽²²⁾ praktičnih zaščitnih ukrepov o varnosti (glej tudi del III.1(c)).
38. Načelo kakovosti podatkov iz člena 6(d) Direktive 95/46/ES je še zlasti pomembno v okviru medobratovalnosti aplikacij in sistemov. Tehnične specifikacije, ki jih bo treba opredeliti za načrtovanje vmesnikov, bi morale zagotoviti točnost podatkov, ki bodo pridobljeni kot rezultat povezovanja aplikacij in sistemov.
39. Glede na to, da bo medobratovalnost sistemov olajšala povezovanje zbirk podatkov in ujemanje podatkov za dodatne namene, ENVP poudarja, da bi bilo treba vsako povezovanje izvesti ob skrbnem upoštevanju načela omejitve namena iz člena 6(1)(b) Direktive 95/46/ES. Še zlasti je pomembno, da načrtovanje strukture sistemov ITS preprečuje vsakršno nadaljnjo uporabo podatkov za drugačne namene od tistih, za katere so bili zbrani. Ustrezna varnostna zaščita mora biti vgrajena v sistem zaradi preprečevanja nepravilne uporabe, nepooblaščenega razkritja ali dostopa ter stranskih učinkov naprav. Treba bi bilo na primer izvesti zadostno zaščito, tako da nepooblaščen tretje strani ne dostopajo do nomadskih naprav in se te ne uporabljajo za identifikacijo in sledenje ljudem, ki presegajo namene sistema.

⁽²¹⁾ Glej opombo 15.

⁽²²⁾ Glej tudi pripombe ENVP glede sporočila Komisije o interoperabilnosti evropskih zbirk podatkov, 10. marec 2006. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

40. Kar zadeva zakonitost samega povezovanja, bo treba to oceniti za vsak primer posebej, ob upoštevanju narave podatkov, ki se dajo na razpolago in ki se izmenjajo prek sistemov, ter namenov, za katere so se prvotno namepravali uporabiti.

III.1(c) Varnost podatkov

41. Varnost osebnih podatkov je glavni element uvajanja ITS. ENVP pozdravlja dejstvo, da je varnost izrecno omenjena v akcijskem načrtu in predlogu direktive. Varnost bi bilo treba predvideti ne samo med delovanjem naprave ITS (pri sistemih v vozilu in pri protokolu prenosa sporočil), temveč tudi izven delovanja naprave – v zbirkah podatkov, kjer se podatki obdelujejo in/ali hranijo. Treba bi bilo opredeliti ustrezne tehnične, upravne in organizacijske zahteve za vse faze obdelave, ki zagotavljajo ustrezno raven varnosti v skladu s členoma 16 in 17 Direktive 95/46/ES (pa tudi členoma 4 in 5 Direktive 2002/58/ES, kjer je to ustrezno).
42. Ustrezne varnostne ukrepe bi bilo treba opredeliti šele po temeljiti oceni konkretnih namenov, za katere se bodo ITS uporabljali, in načinov izvedene obdelave. V tej zvezi ENVP priporoča, da se opravijo ocene učinkov glede zasebnosti in varstva podatkov za določene sektorje in/ali namene uporabe (npr. za sisteme ITS, ki omogočajo večjo varnost, za sisteme upravljanja tovora itd.). Izvedba ocene učinkov glede zasebnosti in varstva podatkov ter uporaba najboljših razpoložljivih tehnologij za zasebnost in varstvo podatkov bosta prispevali k opredelitvi najustreznejših varnostnih ukrepov, ki zadevajo določeno izvedeno obdelavo.

III.2 Nadaljnji razmisleki o varstvu podatkov in zasebnosti za izvajanje storitev ITS

43. Na ravni EU je potrebno nadaljnje usklajevanje načinov uvajanja storitev ITS, da bi se preprečile razlike pri uvajanju ITS. V tej zvezi bi želel ENVP izpostaviti dve vprašanji, ki bosta zlasti zahtevali nadaljnji razmislek z vidika zasebnosti in varstva podatkov:
- uporaba lokacijskih orodij za zagotavljanje javnih in komercialnih storitev, vezanih na lokacijo, zahteva, da se izvedejo dodatni zaščitni ukrepi. V tej zvezi je treba posebno pozornost posvetiti temu, ali in kdaj se storitve ITS, vezane na lokacijo, uporabljajo v zasebne ali službene namene in kako bi lahko uporaba tega sistema vplivala na posameznike, ki uporabljajo vozilo v okviru službe,

— v integriranih sistemih je še zlasti pomembno, da se razjasnijo vloge in pristojnosti različnih strani, vključenih v uvajanje ITS.

III.2(a) *Zaščitni ukrepi za uporabo lokacijskih orodij za zagotavljanje storitev ITS, vezanih na lokacijo*

44. Uvajanje ITS bo podprlo razvoj aplikacij za sledenje in spremljanje blaga ter omogočilo uvajanje komercialnih in javnih storitev, vezanih na lokacijo. Te storitve bodo oprte na uporabo tehnologij, kot so satelitsko določanje položaja in oznake RFID ⁽²³⁾. Sistemi za navigacijo, sledenje in spremljanje so namenjeni uporabi za številne namene, kot so nadzor vozil in tovorov na daljavo (npr. za prevoz nevarnega blaga ali živih živali), zaračunavanje vozilom glede na različne parametre, vključno s prepotovano razdaljo in časom dneva (npr. cestnine, elektronski cestninski sistemi) in nadzor voznikov zaradi izpolnjevanja obveznosti, kot so preverjanje časa za vožnjo (z digitalnimi tahografi) in nalaganje sankcij (z elektronsko identifikacijo vozila).
45. Uporaba lokacijskih tehnologij je še zlasti vsiljiva z vidika zasebnosti, saj omogoča sledenje voznikov in zbiranje najrazličnejših podatkov v zvezi z njihovimi voznimi navadami. Kot je poudarila Delovna skupina iz člena 29 ⁽²⁴⁾, je obdelava lokacijskih podatkov še zlasti občutljiva zadeva, ki zajema ključno vprašanje svobode anonimnega gibanja, ter zahteva izvajanje posebnih zaščitnih ukrepov, da se preprečita nadzor posameznikov in nepravilna uporaba podatkov.
46. ENVP poudarja, da mora biti uporaba lokacijskih orodij zakonita, tj. temeljiti na ustrezni pravni podlagi, za izrecne in legitimne namene, ter sorazmerna z nameni, ki naj se dosežejo. Zakonitost opravljene obdelave podatkov bo v veliki meri odvisna od načina, na katerega se bodo uporabila lokacijska orodja, in od namenov, za katere se bodo uporabila. Delovna skupina iz člena 29 je v mnenju o klicu v sili (eCall) poudarila, da „s stališča varstva podatkov ne bi bilo sprejemljivo, da so takšne naprave stalno priključene in so vozila tako stalno izsledljiva, glede na morebitno aktivacijo naprav za klic v sili (eCall)“ ⁽²⁵⁾. Zato je pomembno, da se podrobneje pojasnijo konkretne okoliščine, v katerih se bo vozilu sledilo, in vpliv na uporabnika. V vsakem primeru bi bilo treba uporabo

lokacijskih naprav upravičiti z legitimno potrebo (npr. nadzor prevoza blaga) in strogo omejiti na to, kar je potrebno za ta namen. Zato je pomembno natančno opredeliti, kateri podatki o lokaciji se zbirajo, kje se hranijo in kako dolgo se hranijo, s kom in za katere namene se izmenjajo, ter sprejeti vse potrebne ukrepe, da se izogne nepravilni uporabi ali zlorabi podatkov.

47. Poleg tega je obdelava podatkov o lokaciji v zvezi z uporabniki javnih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev strogo urejena v členu 9 Direktive 2002/58/ES. Predvsem zahteva, da se obdelava podatkov o lokaciji opravi anonimno oziroma po prostovoljni privolitvi uporabnika. To pomeni, da morajo uporabniki pred dogovorom o uporabi lokacijskega orodja prejeti ustrezne informacije, vključno o vrsti obdelanih podatkov o lokaciji, namenih in trajanju obdelave ter ali se bodo podatki posredovali tretji strani za namen izvajanja storitve z dodano vrednostjo. Uporabniki morajo imeti na voljo enostavna in brezplačna sredstva, da začasno zavrnejo obdelavo podatkov o lokaciji za vsako povezavo na omrežje ali za vsak prenos sporočila. Obdelava podatkov o lokaciji bi morala biti strogo omejena na osebe, ki delujejo pod vodstvom ponudnika javnega komunikacijskega omrežja ali javno razpoložljive komunikacijske storitve ali tretje strani, ki izvaja storitev z dodano vrednostjo.
48. Treba je sprejeti dodatne zaščitne ukrepe v primeru zbiranja podatkov o lokaciji pri vozilih, ki se uporabljajo za opravljanje poklicne dejavnosti, da se prepreči uporaba lokacijske tehnologije za neupravičen nadzor uslužbencev. V vsakem primeru bi bilo treba obdelavo omejiti na podatke o lokaciji, ki se zbirajo med delovnim časom – zato bi morali imeti uslužbenci možnost izklopiti lokacijsko funkcijo izven delovnega časa in/ali ko uporabljajo vozila za zasebne namene.
49. Obstaja tveganje, da tretje strani (kot so zavarovalnice, delodajalci in organi kazenskega pregona) zahtevajo dostop do podatkov, zbranih s sistemi za navigacijo in sledenje, za legitimne in konkretne namene (kot je sledenje blaga, elektronsko cestninjenje itd.), da bi jih nato uporabile za sekundarne namene, kot so preverjanje časa za vožnjo in počitek ali preverjanje upoštevanja cestnih predpisov in nalaganje sankcij. Načeloma dostop do podatkov za sekundarne namene ni dovoljen, če ta dostop služi namenom, ki so nezdržljivi z nameni, za katere so bili zbrani. Dostop se dovoli le z odstopanjem od tega načela, če pogoji za ta dostop izpolnjujejo stroge zahteve člena 13 Direktive 95/46/ES. Posledično bi bilo treba vsak dostop tretjih strani do podatkov o lokaciji zagotoviti le v skladu z zakonodajo in na pregleden način, na podlagi pravnega

⁽²³⁾ Glej vprašanja o zasebnosti in varstvu podatkov, ki se odpirajo z uporabo RFID, v mnenju evropskega nadzornika za varstvo podatkov o sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom „Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki k okviru politike“ COM(2007), UL C 101, 23.4.2008, str. 1. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf

⁽²⁴⁾ Delovna skupina iz člena 29, mnenje o uporabi podatkov o lokaciji, da se zagotovijo storitve z dodano vrednostjo, DS 115, november 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

⁽²⁵⁾ Glej WP 125 o klicu v sili (eCall), str. 5, naveden v opombi 10.

ukrepa, ki določa ustrezne postopke in načine za dostop do podatkov za konkretne namene, ter ki zagotavlja ustrezne zaščitne ukrepe za posameznike v skladu z nadaljnimi nameni, za katere bi se lahko njihovi podatki uporabili.

III.2(b) Vloge in pristojnosti akterjev ITS

50. Ni še jasno, kdo bo upravljavec podatkov za vsak del obdelave. V številnih primerih bodo upravljavci podatkov po vsej verjetnosti ponudniki storitev ITS, bodisi sami glede osebnih podatkov, obdelanih za zagotavljanje svojih lastnih storitev ITS, bodisi skupaj v primerih, ko se obdelava izvede skupaj z drugimi upravljavci podatkov. Operaterji, ki so na različne načine vključeni v ITS, bi morali imeti svojo vlogo in pristojnosti kot upravljavci podatkov in obdelovalci podatkov jasno opredeljene, in sicer za vsak del obdelave (npr. telekomunikacijski operaterji, ki izvajajo komunikacijske storitve in storitve ITS).
51. Te osebe v vlogi upravljavcev podatkov bodo pristojne ⁽²⁶⁾ za zagotavljanje skladnosti sistemov in storitev z vsemi obveznostmi glede varstva podatkov ter zlasti za izvedbene sisteme, ki vključujejo načelo spoštovanja zasebnosti pri načrtovanju, ki spoštujejo načeli kakovosti podatkov in omejitve namena ter ki jamčijo ustrezne ravni varnosti podatkov, kot je opisano v III.1).
52. Upravljavci podatkov bodo morali zagotoviti, da se sprejmejo ustrezni zaščitni ukrepi na vseh ravneh verige akterjev, vključenih v uvajanje ITS. To bo zlasti zahtevalo, da vzpostavijo ustrezne pogodbene sheme z vsemi interesnimi skupinami, vključenimi v izmenjavo in obdelavo podatkov, ki bi morale zagotoviti ustrezne zaščitne ukrepe za varstvo podatkov (zlasti glede členov 16 in 17 Direktive 95/46/ES in členov 4 in 5 Direktive 2002/58/ES). Pomebno je opozoriti, da so upravljavci podatkov tisti, ki morajo zagotoviti, da se v vseh fazah obdelave zagotovi varstvo podatkov, a so z vidika varstva podatkov še naprej pristojni za obdelavo in ne morejo pogodbeno izključiti svoje pristojnosti.

IV. SKLEPNE UGOTOVITVE

53. ENVP pozdravlja predlagani načrt za uvajanje ITS, ki ga je predložila Komisija in je namenjen uskladitvi postopkov v zvezi s podatki po Evropi, da bi se olajšalo izvajanje storitev ITS, ter v katerem je varstvo podatkov ključni pogoj za ustrezno uvajanje ITS po Evropi.
54. ENVP ugotavlja, da predlagana direktiva določa splošni okvir, ki odpira številna vprašanja glede zasebnosti in varstva podatkov, ki jih je treba podrobneje obravnavati na ravni EU in nacionalni ravni:

- Obstaja tveganje, da bo nejasnost predlaganega pravnega okvira povzročila različne načine izvajanja ITS v Evropi, posledica tega pa bodo različne ravni varstva podatkov v Evropi. ENVP poudarja, da je treba dodatno uskladiti ta vprašanja na ravni EU zaradi razjasnitve odprtih vprašanj (kot je opredelitev vlog in pristojnosti akterjev ITS, katere posebne aplikacije in sisteme ITS je treba vgraditi v vozila, oblikovanje usklajenih pogodb za izvajanje storitev ITS, posebni nameni in načini uporabe ITS itd.). Zlasti je ključno opredeliti, kdo bodo upravljavci podatkov glede opravljene obdelave podatkov, saj bodo odgovorni za zagotovitev, da se bodo razmislili glede zasebnosti in varstva podatkov izvajali na vseh ravneh obdelave.
- Odločitve o nekaterih načinih obdelave, ki bi lahko resno vplivali na pravice posameznikov glede zasebnosti in varstva podatkov, bi morala sprejeti Evropski parlament in Svet; za njihovo sprejemanje se ne bi smelo uporabiti postopka komitologije.
- Bistveno je, da se zasebnost in varstvo podatkov upoštevata od zgodnje faze obdelave in v vseh fazah obdelave; za načrtovanje aplikacij in sistemov ITS bi bilo treba spodbujati izvajanje načela spoštovanja zasebnosti pri načrtovanju ter ga vključiti v standarde, najboljše prakse, tehnične specifikacije in sisteme.
- Vsako povezovanje aplikacij in sistemov bi bilo treba izvesti ob ustreznem spoštovanju načel o varstvu podatkov in praktičnih zaščitnih ukrepov o varnosti.
- Kar zadeva negotovosti v tej fazi, ki se nanašajo na načine uvajanja ITS, ENVP zlasti pozdravlja pobudo Komisije iz sporočila, da naj se v letu 2011 izvede ocena zasebnosti. Poleg tega močno priporoča, da se ocene učinkov glede zasebnosti in varstva podatkov izvedejo za določene sektorje in/ali namene uporabe, da se tako opredelijo ustrezni zaščitni ukrepi ter razvijejo najboljše razpoložljive tehnologije za zasebnost, varstvo podatkov in varnost ITS.
- ENVP poleg tega poudarja, da bodo države članice odgovorne za izvajanje direktive na ustrezen način, tako da bodo upravljavci ITS izvajali sisteme in storitve, ki nudijo ustrezno raven varstva podatkov v Evropi.

⁽²⁶⁾ Glej opombo 13.

- Upravljalci podatkov, ki izvajajo storitve ITS, bi morali izvesti ustrezne zaščitne ukrepe, tako da uporaba lokacijskih tehnologij, kot so satelitsko določanje položaja in oznake RFID, ne vdira v zasebnost posameznikov, ki uporabljajo vozila v izključno zasebnem ali službenem okviru. To bo zahtevalo predvsem omejitev obdelave na podatke, ki so potrebni izključno za ta namen, da se zagotovi, da se v sisteme vgradijo ustrezni varnostni ukrepi, tako da se podatki o lokaciji ne razkrijejo nepooblaščenim prejemnikom, in da imajo uporabniki na voljo učinkovita sredstva za deaktivacijo lokacijske naprave/funkcije
55. ENVP priporoča, da se spremeni člen 6 predloga v skladu z Direktivo 95/46/ES:
- V zvezi z obdelavo podatkov, ki se izvede prek ITS, bi bilo treba spodbujati zmanjšanje količine podatkov. S tega stališča se priporoča, da se spremeni člen 6(1)(b) predloga: „Osební podatki se obdelajo le, če je obdelava potrebna za konkreten namen, za katerega se ITS uporablja, in v skladu z ustrezno pravno podlago“.
- Pomembno je, da se osebni podatki, obdelani prek medobratovalnih sistemov, ne uporabljajo za nadaljnje namene, ki so nezdružljivi s tistimi, za katere so bili zbrani. Zato se priporoča, da se spremeni člen 6(2): „in da se jih ne sme uporabiti za namene, ki niso nameni, za katere so bili zbrani, na način, ki je nezdružljiv s temi nameni.“
- Priporoča, da se v člen 6 predloga doda izrecen sklic na pojem „spoštovanje zasebnosti pri načrtovanju“ za načrtovanje aplikacij in sistemov ITS. Poleg tega priporoča, da sta Delovna skupina iz člena 29 in ENVP obveščena o nadaljnjih ukrepih, sprejetih glede tega vprašanja po postopku komitologije, ter se z njima o njih posvetuje.
56. ENVP še priporoča, da se v uvodnih izjavah predloga navede sklicevanje na to posvetovanje.
57. Ob upoštevanju zgoraj navedenega ENVP priporoča, da so organi za varstvo podatkov, zlasti prek Delovne skupine iz člena 29, in ENVP tesno vključeni v pobude, povezane z uvajanjem ITS, in sicer prek posvetovanja v dovolj zgodnji fazi pred oblikovanjem zadevnih ukrepov.

V Bruslju, 22. julija 2009

Peter HUSTINX

Evropski nadzornik za varstvo podatkov