Euroopa andmekaitseinspektori arvamus, mis käsitleb komisjoni teatist Euroopa Parlamendile ja nõukogule – „ELi sisejulgeoleku strateegia toimimine: viis sammu turvalisema Euroopa suunas”

(2011/C 101/02)

EUROOPA ANDMEKAITSEINSPEKTOR,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 16,

võttes arvesse Euroopa Liidu põhiõiguste hartat, eriti selle artikleid 7 ja 8,

võttes arvesse Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, ([1])

võttes arvesse taotlust arvamuse esitamiseks kooskõlas määrusega (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta, ([2]) eriti selle artikliga 41,

ON VASTU VÕTNUD KÄESOLEVA ARVAMUSE:

I. SISSEJUHATUS

1. 22. novembril 2010 võttis komisjon vastu teatise „ELi sisejulgeoleku strateegia toimimine: viis sammu turvalisema Euroopa suunas” ([3]) (edaspidi „teatis”). Teatis saadeti konsulteerimiseks Euroopa andmekaitseinspektorile.

2. Euroopa andmekaitseinspektor väljendab heameelt selle üle, et komisjon temaga konsulteeris. Juba enne teatise vastuvõtmist esitas Euroopa andmekaitseinspektor teksti eelnõu kohta mitteametlikud märkused, millest mõnda on teatise lõppversioonis arvesse võetud.

Teatise kontekst

3. Teatises käsitletud Euroopa Liidu sisejulgeoleku strateegia võeti vastu Hispaania eesistumise ajal 23. veebruaril 2010 ([4]). Kõnealuses strateegias on sätestatud Euroopa julgeolekumudel, mis muu hulgas hõlmab meetmeid õiguskaitse- ja kohtualase koostöö, piiride halduse ja kodanikukaitse valdkonnas ning tagab Euroopa ühisväärtuste, näiteks põhiõiguste nõuetekohase järgimise. Selle põhieesmärgid on järgmised:

— tutvustada üldsusele olemasolevaid Euroopa Liidu vahendeid, mis juba praegu aitavad tagada Euroopa Liidu kodanike julgeolekut ja vabadust, ning Euroopa Liidu meetmete lisandväärtust selles valdkonnas;

— arendada edasi ühiseid vahendeid ja poliitikaid, kasutades sealjuures terviklikumat lähenemisviisi, mis on suunatud ohtude põhjustele, mitte lihtsalt tagajärgedele;

— tugevdada õiguskaitset ja õigusalast koostööd, piirihaldust, kodanikukaitset ja suurõnnetuse likvideerimise võimekust.

4. Sisejulgeoleku strateegia eesmärk on tegeleda Euroopa Liidu olulisimate julgeolekuohtude ja –ülesannetega, nagu rasked ja organiseeritud kuriteod, terrorism ja küberkuritegevus, Euroopa Liidu välispiiri haldamine ning suurem vastupanuvõime loodusõnnetustele ja inimtegevusest tulenevatele katastroofidele. Strateegias on kehtestatud üldised suunised, põhimõtted ja suunad seoses sellega, kuidas Euroopa Liit peaks nendele küsimustele reageerima, ning selles kutsutakse komisjoni üles soovitama kindla ajakavaga meetmeid strateegia rakendamiseks.

5. Peale selle on siinkohal oluline viidata justiits- ja siseküsimuste nõukogu hiljutistele järeldustele organiseeritud ja rasket rahvusvahelist kuritegevust käsitleva Euroopa Liidu poliitikatsükli kujundamise ja rakendamise kohta, mis võeti vastu 8–9. novembril 2010 ([5]) (edaspidi „2010. aasta novembri järeldused”). See dokument on järg nõukogu 2006. aasta järeldustele sisejulgeoleku arhitektuuri kohta ([6]) ning selles kutsutakse nõukogu ja komisjoni üles määratlema kõikehõlmav sisejulgeolekustrateegia, mis põhineks Euroopa Liidu põhiõiguste hartas kinnitatud ühistel väärtustel ja põhimõtetel ([7]).

([1]) EÜT L 281, 23.11.1995, lk 31.
([2]) EÜT L 8, 12.1.2001, lk 1.
([3]) KOM(2010) 673 (lõplik).
([4]) Dokument 5842/2/10.
([5]) Justiits- ja siseküsimuste nõukogu 3043. istung Brüsselis, 8.–10. november 2010.
([6]) Dokument 7039/2/06 JAI 86 CATS 34.
([7]) 2010. aasta novembri järeldustes kajastatud organiseeritud ja rasket rahvusvahelist kuritegevust käsitlev Euroopa Liidu poliitikatsükkel koosneb neljast etapist: 1) poliitika väljatöötamine Euroopa Liidu raske ja organiseeritud kuritegevuse ohu hindamise alusel; 2) poliitika kujundamine ja otsuste tegemine nõukogu poolt kindlaks määratud piiratud arvul prioriteetidel; 3) iga-aastaste operatiivsete tegevuskavade rakendamine ja kontrollimine ja 4) poliitikatsükli lõpus põhjalik hindamine, mida muu hulgas võetakse arvesse järgmises poliitikatsüklis.

6. Nende suundade ja eesmärkide hulgas, millest sisejulgeoleku strateegia rakendamisel tuleks juhinduda, osutatakse 2010. aasta novembri järeldustes ennetava ja jälitusteabel põhineva lähenemisviisi kajastamisele, Euroopa Liidu asutuste vahelisele tõhusale koostööle, sealhulgas nende teabevahetuse täiustamisele, ning eesmärgile teavitada kodanikke sellest, kui oluline on liidu tegevus nende kaitsmisel. Peale selle kutsutakse järeldustes komisjoni üles koostama koos asjaomaste asutuste ja liikmesriikide ekspertidega iga prioriteedi kohta mitmeaastane strateegiakava, milles oleks määratletud kõige sobivam viis probleemi lahendamiseks. Ühtlasi kutsutakse selles komisjoni üles looma liikmesriikide ja Euroopa Liidu asutuste ekspertidega konsulteerides sõltumatu mehhanism, millega hinnata mitmeaastase strateegiakava rakendamist. Euroopa andmekaitseinspektor käsitleb neid küsimusi käesolevas arvamuses edaspidi üksikasjalikumalt, sest need on isikuandmete, eraelu puutumatuse ning teiste seotud põhiõiguste ja -vabaduste kaitsega tihedalt seotud ja võivad avaldada sellele suurt mõju.

Teatise sisu ja eesmärk

7. Teatises on välja pakutud viis strateegiaeesmärki, mis kõik on seotud eraelu puutumatuse ja andmekaitsega:

— tõkestada rahvusvaheliste kuritegelike võrgustike tegevust;

— hoida ära terrorismi ning tegeleda radikaliseerumise ja terroristide värbamise probleemiga;

— tõsta kodanike ja ettevõtjate jaoks turvalisuse taset küberruumis;

— tugevdada turvalisust piiride haldamise kaudu ja

— muuta Euroopa kriisidele ja katastroofidele vastupanuvõimelisemaks.

8. Teatises välja pakutud *sisejulgeoleku strateegia toimimine* hõlmab liikmesriikide, Euroopa Parlamendi, komisjoni, nõukogu, ametite ja teiste osapoolte, sealhulgas kodanikuühiskonna ja kohalike asutuste ühist tegevuskava ning sisaldab ettepanekuid selle kohta, kuidas nad peaksid järgmise nelja aasta jooksul tegemasisejulgeoleku strateegia eesmärkide saavutamiseks koostööd.

9. Teatises lähtutakse Lissaboni lepingust ning tunnustatakse juhiseid, mis on esitatud Stockholmi programmis (ja selle tegevuskavas), mille peatükis 4.1 rõhutatakse vajadust põhiõiguste austamisele, rahvusvahelisele kaitsele ja õigusriigi põhimõttele tugineva kõikehõlmava sisejulgeoleku strateegia järele. Peale selle peaks Stockholmi programmi kohaselt olema sisejulgeoleku strateegia väljatöötamine, järelevalve ja rakendamine Euroopa Liidu toimimise lepingu artikli 71 alusel asutatud sisejulgeoleku komitee (COSI) üks põhiülesandeid. Sisejulgeoleku strateegia tõhusa jõustamise tagamiseks tuleks selles käsitleda ka integreeritud piirihalduse julgeolekuaspekte ja vajaduse korral sellise kriminaalasjades tehtava kohtualase koostöö julgeolekuaspekte, mis on seotud sisejulgeoleku alal tehtava operatiivkoostööga. Siinkohal on oluline märkida ka seda, et Stockholmi programmis rõhutatakse tervikliku lähenemise vajadust, mille kohaselt sisejulgeoleku strateegias tuleks arvesse võtta ka Euroopa Liidu koostatud välisjulgeoleku strateegiat ja muid, eelkõige Euroopa Liidu siseturuga seotud tegevuspõhimõtteid.

Arvamuse eesmärk

10. Teatises viidatakse mitmesugustele poliitikavaldkondadele, mis moodustavad osa Euroopa Liidu *sisejulgeoleku* laiemast mõistest või seda mõjutavad.

11. Käesoleva arvamuse eesmärk ei ole analüüsida kõiki teatises käsitletud poliitikavaldkondi ja konkreetseid teemasid, vaid:

— vaadelda teatises välja pakutud sisejulgeoleku strateegia eesmärke eraelu puutumatuse ja andmekaitse seisukohast ning rõhutada sellest vaatenurgast lähtudes vajalikke seoseid muude Euroopa Liidu tasandil praegu arutatavate ja vastuvõetavate strateegiatega;

— täpsustada mitut andmekaitsega seotud põhimõtet ja mõistet, mida tuleks Euroopa Liidu tasandil sisejulgeoleku strateegia kavandamisel, väljatöötamisel ja rakendamisel arvestada;

— kui see on kasulik ja asjakohane, siis soovitada viise, kuidas võtta andmekaitseküsimusi teatises välja pakutud meetmete rakendamisel kõige paremini arvesse.

12. Selleks rõhutab Euroopa andmekaitseinspektor eelkõige sisejulgeoleku strateegia ja infohaldusstrateegia ning kõikehõlmava andmekaitseraamistiku alase töö vahelisi seoseid. Peale selle viitab Euroopa andmekaitseinspektor sellistele mõistetele nagu „parim võimalik tehnika", „eraelu kavandatud puutumatus", „eraelu puutumatuse ja andmekaitse mõjuhinnang" ning „andmesubjektide õigused", millel on otsene mõju sisejulgeoleku strateegia kavandamisele ja rakendamisele. Arvamuses kommenteeritakse ka mitut valitud poliitikavaldkonda, näiteks integreeritud piirihaldust, sealhulgas Euroopa piiride valvamise süsteemi EUROSUR ning isikuandmete töötlemist Frontexis, samuti muid küsimusi, nagu küberruum ja terroristide rahastamise jälgimisprogramm.

II. ÜLDISED MÄRKUSED

Vajadus terviklikuma, kõikehõlmava ja strateegilise lähenemisviisi järele sisejulgeoleku strateegiaga seotud ELi strateegiate puhul

13. Praegu arutatakse ja pakutakse Euroopa Liidu tasandil välja mitmesuguseid Lissaboni lepingule ja Stockholmi programmile tuginevaid Euroopa Liidu strateegiaid, millel on otsene või kaudne mõju andmekaitsele. Üks neist on sisejulgeoleku strateegia, mis on tihedalt seotud teiste (komisjoni hiljutistes teatistes käsitletud või lähitulevikuks kavandatud) strateegiatega, nagu Euroopa Liidu infohaldusstrateegia ja Euroopa teabevahetusmudel, Euroopa Liidu põhiõiguste harta rakendamise strateegia, kõikehõlmav andmekaitsestrateegia ja Euroopa Liidu terrorismivastase võitluse poliitika. Oma arvamuses pöörab Euroopa andmekaitseinspektor tähelepanu eelkõige seostele infohaldusstrateegia ja Euroopa Liidu toimimise lepingu artiklil 16 põhineva kõikehõlmava andmekaitseraamistikuga, millel on andmekaitse seisukohast sisejulgeoleku strateegiaga kõige ilmsemad poliitilised seosed.

14. Nimetatud strateegiad moodustavad vastastikku seotud poliitiliste suuniste, programmide ja tegevuskavade keeruka süsteemi, mis vajab kõikehõlmavat ja terviklikku lähenemisviisi Euroopa Liidu tasandil.

15. Kui edaspidistes meetmetes hakatakse sel viisil *strateegiaid omavahel siduma*, näitab see üldisemalt, et Euroopa Liidu tasandil on *Euroopa Liidu strateegiate* osas olemas visioon ning et strateegiad ja hiljuti vastu võetud teatised, milles neid üksikasjalikult kirjeldatakse, on vastastikku tihedalt seotud, mida nad ka on, tuginedes kõik Stockholmi programmile kui ühisele lähtepunktile. Ühtlasi tooks see kaasa vabaduse, turvalisuse ja õiguse valdkonna eri tegevuspõhimõtete positiivse koostoime ning aitaks vältida töö ja jõupingutuste võimalikku dubleerimist selles valdkonnas. Sama oluline on see, et selline lähenemisviis võimaldaks kohaldada andmekaitse-eeskirju kõikide omavahel seotud strateegiate kontekstis tõhusamalt ja sidusamalt.

16. Euroopa andmekaitseinspektor rõhutab, et üks sisejulgeoleku strateegia aluspõhimõtteid on tõhus teabehaldus Euroopa Liidus, mis teabevahetuse vajalikkuse põhjendamiseks peaks tuginema vajalikkuse ja proportsionaalsuse põhimõtetele.

17. Peale selle, nagu on märgitud Euroopa andmekaitseinspektori arvamuses teabehaldust käsitleva teatise kohta, ([8]) rõhutab Euroopa andmekaitseinspektor, et uute õiguslike meetmete, millega hõlbustatakse isikuandmete säilitamist ja vahetamist, ettepanekuid tuleks teha vaid siis, kui nende vajalikkus on konkreetselt tõendatud ([9]). Sisejulgeoleku strateegia rakendamisel tuleks see õiguslik nõue kujundada ennetavaks poliitiliseks lähenemisviisiks. Vajadus sisejulgeoleku strateegiaga seotud kõikehõlmava lähenemisviisi järele tingib ka vajaduse hinnata enne uute ettepanekute tegemist kõiki sisejulgeoleku valdkonnas kehtivaid instrumente ja vahendeid.

18. Siinkohal soovitab Euroopa andmekaitseinspektor ka kasutada sagedamini olemasolevate instrumentide korrapärast hindamist sätestavaid klausleid, näiteks praegu hinnatavas andemete säilitamise direktiivis ([10]) sisalduvaid klausleid.

Andmekaitse kui sisejulgeoleku strateegia eesmärk

19. Teatises viidatakse isikuandmete kaitsele lõigus „Ühistel väärtustel põhinev julgeolekupoliitika", mille kohaselt peavad sisejulgeoleku strateegia rakendamiseks kasutatavad vahendid ja meetmed põhinema ühistel väärtustel, sealhulgas õigusriigi põhimõttel ja põhiõigustest kinnipidamisel, nagu on sätestatud Euroopa Liidu põhiõiguste hartas. Sellega seoses on kõnealuses lõigus sätestatud järgmine: „Kuna õiguskaitset hõlbustab ELis teabevahetus, peame me kaitsma ka üksikisikute eraelu puutumatust ja nende põhiõigust isikuandmete kaitsele."

20. See avaldus on tervitatav. Samas ei saa aga arvata, et andmekaitse küsimust oleks sisejulgeoleku strateegias seeläbi piisavalt käsitletud. Teatises ei täpsustata andmekaitse küsimust ([11]) ega selgitata, kuidas eraelu puutumatus ja isikuandmete kaitse sisejulgeoleku strateegia rakendamise meetmetes tegelikult tagatakse.

([8]) Euroopa andmekaitseinspektori 30. septembri 2010. aasta arvamus, mis käsitleb komisjoni teatist Euroopa Parlamendile ja nõukogule – „Ülevaade teabehaldusest vabadusel, turvalisusel ja õigusel rajaneval alal".

([9]) See on õiguslik nõue; vt eriti Euroopa Kohtu 2. novembri 2010. aasta otsus liidetud kohtuasjades C-92/09 ja C-93/09. Konkreetsemates kontekstides on Euroopa andmekaitseinspektor soovitanud sellist lähenemist ka teistes vabadusel, turvalisusel ja õigusel rajaneva alaga seotud seadusandlikke algatusi käsitlevates arvamustes, näiteks 19. oktoobri 2005. aasta arvamuses teise põlvkonna Schengeni infosüsteemi (SIS II) käsitlevate ettepanekute kohta; 20. detsembri 2007. aasta arvamuses õigusakti eelnõu kohta, mis käsitleb nõukogu raamotsust broneeringuinfo kasutamise kohta õiguskaitse eesmärkidel; 18. veebruari 2009. aasta arvamuses ettepaneku kohta võtta vastu määrus, mis käsitleb sõrmejälgede võrdlemise Eurodac-süsteemi kehtestamist, et kohaldada tõhusalt määrust (EÜ) nr (.../...) (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest); 18. veebruari 2009. aasta arvamuses ettepaneku kohta võtta vastu määrus, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest, ning 7. oktoobri 2009. aasta arvamuses ettepanekute kohta, mis käsitlevad õiguskaitseasutuste juurdepääsu Eurodac-süsteemile.

([10]) Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, (ELT L 105, 13.4.2006, lk 54).

([11]) Andmekaitset nimetatakse konkreetsemalt üksnes seoses Frontexis isikuandmete töötlemise küsimusega.

21. Euroopa andmekaitseinspektori arvamuse kohaselt peaks *sisejulgeoleku strateegia toimimise* üks eesmärk olema *kaitse* laiemas tähenduses, mis tagaks *õige* tasakaalu ühelt poolt kodanike olemasolevate ohtude eest kaitsmise ning teiselt poolt nende õiguse vahel eraelu puutumatusele ja isikuandmete kaitsele. Teisisõnu tuleb sisejulgeoleku strateegia väljatöötamisel suhtuda ühtmoodi tõsiselt nii julgeoleku kui ka eraelu puutumatusega seotud küsimustesse ning selline lähenemine on kooskõlas ka Stockholmi programmi ja nõukogu järeldustega.

22. Lühidalt peaks julgeoleku tagamine koos eraelu puutumatuse ja andmekaitse austamisega olema ära märgitud Euroopa Liidu sisejulgeoleku strateegia ühe eesmärgina. See peaks kajastuma kõikides meetmetes, mida liikmesriigid ja Euroopa Liiduinstitutsioonid võtavad strateegia rakendamiseks.

23. Sellega seoses osutab Euroopa andmekaitseinspektor teatisele (2010) 609, mis käsitleb terviklikku lähenemisviisi isikuandmete kaitsele Euroopa Liidus ([12]). Euroopa andmekaitseinspektor avaldab peatselt selle teatise kohta arvamuse, ent rõhutab siinkohal, et tõhusat sisejulgeoleku strateegiat ei ole võimalik kehtestada ilma põhjaliku andmekaitsekorrata, mis seda täiendaks ning tagaks vastastikuse usalduse ja suurema tõhususe.

III. SISEJULGEOLEKU STRATEEGIA KAVANDAMISEL JA RAKENDAMISEL KOHALDATAVAD PÕHIMÕTTED JA MÕISTED

24. On selge, et teatavad sisejulgeoleku strateegia eesmärkidest tulenevad meetmed võivad suurendada riske üksikisikute eraelu puutumatusele ja andmekaitsele. Nende riskide tasakaalustamiseks soovib Euroopa andmekaitseinspektor spetsiaalselt juhtida tähelepanu sellistele mõistetele nagu „eraelu kavandatud puutumatus", „eraelu puutumatuse ja andmekaitse mõjuhinnang", „andmesubjektide õigused" ja „parim võimalik tehnika". Kõiki neid küsimusi tuleks sisejulgeoleku strateegia rakendamisel arvesse võtta ning need võivad aidata saavutada valdkonnas eraelu puutumatust soosivamad ja andmekaitset rohkem arvestavad tegevuspõhimõtted.

Eraelu kavandatud puutumatus

25. Euroopa andmekaitseinspektor on mitmel korral ja mitmes arvamuses toetanud juba algselt tagatud eraelu puutumatuse põhimõtet (eraelu kavandatud puutumatus või vaikimisi tagatud eraelu puutumatus). Seda põhimõtet töötatakse praegu välja nii era- kui ka avaliku sektori jaoks ning seepärast peab sel olema tähtis osa ka Euroopa Liidu sisejulgeoleku ning politsei- ja õigusvaldkonna kontekstis ([13]).

26. Teatises seda mõistet ei nimetata. Euroopa andmekaitseinspektor soovitab sellele mõistele viidata sihipärastes meetmetes, mida sisejulgeoleku strateegia rakendamiseks välja pakutakse ja ellu viiakse, eelkõige 4. eesmärgi raames (tugevdada turvalisust piiride halduse kaudu), mille puhul on selgelt nimetatud uue tehnoloogia ulatuslikum kasutamine piirikontrollis ning patrull- ja vaatlustegevuses.

Eraelu puutumatuse ja andmekaitse mõjuhinnang

27. Euroopa andmekaitseinspektor kutsub komisjoni üles teatise põhjal sisejulgeoleku strateegia edasisel väljatöötamisel ja rakendamisel kaaluma, mida peaks vabadusel, turvalisusel ja õigusel rajaneval alal ning eelkõige sisejulgeoleku strateegias tegelikult tähendama *eraelu puutumatuse ja andmekaitse mõjuhinnang*.

28. Teatises viidatakse ohtude ja riskide hindamisele. See on kiiduväärt. Kordagi ei nimetata selles aga eraelu puutumatuse ja andmekaitse mõjuhinnangut. Euroopa andmekaitseinspektor usub, et sisejulgeoleku strateegia teatise rakendamisel tehtav töö annab võimaluse välja töötada selliseid eraelu puutumatuse ja andmekaitse mõjuhinnanguid sisejulgeoleku strateegia raames. Euroopa andmekaitseinspektor märgib, et ei teatises ega komisjoni mõju hindamise suunistes ([14]) ole seda aspekti täpsustatud ega poliitiliseks nõudeks muudetud.

29. Seepärast soovitab Euroopa andmekaitseinspektor koostada tulevaste vahendite rakendamisel sihipärasem ja rangem eraelu puutumatuse ja andmekaitse mõjuhinnang kas eraldi või üldise, komisjoni koostatava põhiõiguste mõjuhinnangu raames. Kõnealuses mõjuhinnangus ei tuleks nimetada üksnes üldpõhimõtteid või analüüsida võimalikke põhimõttelisi võimalusi nagu praegu, vaid tuleks soovitada ka konkreetseid kaitsemeetmeid.

30. Sellest tulenevalt on vaja välja töötada kindlad näitajad ja tunnused, millega tagatakse, et kõiki Euroopa Liidu sisejulgeoleku strateegia valdkonnas tehtavaid ning eraelu puutumatust ja andmekaitset mõjutavaid ettepanekuid kaalutakse põhjalikult, arvestades muu hulgas proportsionaalsust, vajalikkust ja otstarbe piiramise põhimõtet.

31. Sellega seoses on kasulik viidata veel raadiosagedustuvastuse soovituse ([15]) artiklile 4, milles komisjon kutsus liikmesriike üles tagama, et ettevõtjad töötaksid koos asjaomaste kodanikuühiskonna sidusrühmadega välja eraelu puutumatusele

([12]) Komisjoni teatis Euroopa Parlamendile, nõukogule, Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele – Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, KOM(2010) 609.

([13]) Euroopa andmekaitseinspektori arvamuses Stockholmi programmi käsitleva komisjoni teatise kohta soovitatakse kehtestada infosüsteemide loojatele ja kasutajatele juriidiline kohustus arendada ja kasutada süsteeme, mis on kooskõlas eraelu kavandatud puutumatuse põhimõttega.

([14]) SEK(2009) 92, 15.1.2009.

([15]) K(2009) 3200 (lõplik), 12.5.2009.

ja andmekaitsele avalduva mõju hindamise raamistiku. Ka Madridi resolutsioonis, mis võeti vastu eraelu puutumatuse ja andmekaitse eest vastutavate volinike rahvusvahelise konverentsi raames 2009. aasta novembris, kutsuti üles koostama enne isikuandmete töötlemiseks ette nähtud uute infosüsteemide rakendamist või olemasolevate töötlemisviiside sisulist muutmist eraelu puutumatuse ja andmekaitse mõjuhinnang.

Andmesubjektide õigused

32. Euroopa andmekaitseinspektor märgib, et teatises ei käsitleta konkreetselt andmesubjektide õigusi, mis moodustavad andmekaitse olulise osa ning peaksid mõjutama sisejulgeoleku strateegia kavandamist. Tingimata tuleb tagada, et Euroopa Liidu kõikides sisejulgeolekuga seotud süsteemides ja vahendites oleks neis käsitletud isikutel nende isikuandmete töötlemisel ühesugused õigused.

33. Paljudes teatises nimetatud süsteemides on küll andmesubjektide õiguste kohta kehtestatud konkreetsed eeskirjad (mis on suunatud ka sellistele isikute rühmadele nagu kannatanud, kahtlusalused või migrandid), kuid need on eri süsteemides ja vahendites põhjendamatult väga erinevad.

34. Seepärast kutsub Euroopa andmekaitseinspektor komisjoni üles käsitlema sisejulgeoleku strateegia ja infohaldusstrateegia raames lähitulevikus hoolikamalt Euroopa Liidu andmesubjektide õiguste ühtlustamise küsimust.

35. Eritähelepanu peab pöörama õiguskaitsemehhanismidele. Sisejulgeoleku strateegias tuleb tagada, et üksikisiku õiguste eiramise korral näeksid andmetöötlejad ette lihtsalt kasutatavad, tõhusad ja taskukohased kaebuste esitamise menetlused.

Parim võimalik tehnika

36. Sisejulgeoleku strateegia rakendamine põhineb paratamatult teatises ette nähtud meetmeid toetava IT-infrastruktuuri kasutamisel. Parim võimalik tehnika võimaldab saavutada õige tasakaalu sisejulgeoleku strateegia eesmärkide saavutamise ning üksikisikute õiguste austamise vahel. Siinkohal soovib Euroopa andmekaitseinspektor korrata varasemates arvamustes ([16]) esitatud soovitust, et komisjon peaks määratlema koos valdkonna sidusrühmadega parima võimaliku tehnika kasutamise konkreetsed meetmed ja neid edendama. Selline kasutamine tähendab kõige tõhusamat ja paremini välja arendatud tegevuse väljatöötamist ja rakendusviise, mis näitab teatava tehnika praktilist sobivust kavandatud tulemuste tõhusaks saavutamiseks, järgides eraelu puutumatuse ja andmekaitse Euroopa Liidu raamistikku. See lähenemine on täielikult kooskõlas eespool nimetatud eraelu kavandatud puutumatusest tuleneva lähenemisviisiga.

37. Kui see on asjakohane ja teostatav, tuleks välja töötada parima võimaliku tehnika viitedokumendid, et anda sisejulgeoleku strateegia raames kehtestatud meetmete tegeliku rakendamise suuniseid ja tagada selle suurem õiguskindlus. Ühtlasi võiks sellest olla abi ka meetmete ühtlustamisel eri liikmesriikides. Oluline on ka see, et eraelu puutumatust ja julgeolekut soodustava parima võimaliku tehnika määratlemine hõlbustab andmekaitseasutuste tehtavat järelevalvet, andes neile andmetöötlejate heakskiidetud tehnilise võrdlusmaterjali, mis on vastavuses eraelu puutumatuse ja andmekaitsega.

38. Samuti märgib Euroopa andmekaitseinspektor vajadust viia sisejulgeoleku strateegia tingimata nõuetekohaselt kooskõlla teadusuuringute ja tehnoloogiaarenduse seitsmenda raamprogrammi ning turvalisuse ja vabaduse kaitse raamprogrammi raames juba toimuva tegevusega. Ühtne nägemus, millega püütakse tagada parima võimaliku tehnika kasutamine, võimaldab uuendada kodanike kaitsmiseks vajalikke teadmisi ja suutlikkust, austades samas põhiõigusi.

39. Euroopa andmekaitseinspektor osutab ka Euroopa Võrguja Infoturbeameti (ENISA) võimalikule rollile suuniste väljatöötamisel ning IT-süsteemide terviklikkuse ja kättesaadavuse tagamiseks vajaliku julgeolekualase suutlikkuse hindamisel, samuti nimetatud parima võimaliku tehnika edendamisel. Sellega seoses väljendab Euroopa andmekaitseinspektor heameelt selle üle, et amet kaasati olulise osalejana küberrünnakutega toimetuleku ja küberkuritegevuse vastu võitlemise võime parandamisse ([17]).

Osalejate ja nende rollide selgitamine

40. Sellega seoses tuleb täpsustada ka need osalejad, kes moodustavad sisejulgeoleku strateegia süsteemi osa või panustavad sellesse. Teatises nimetatakse mitmesuguseid osalejaid ja sidusrühmi, nagu kodanikud, kohtud, Euroopa

([16]) Euroopa andmekaitseinspektori 2009. aasta juuli arvamus intelligentsete transpordisüsteemide kohta ning Euroopa andmekaitseinspektori 2007. aasta detsembri arvamus raadiosagedustuvastust käsitleva teatise kohta; vt ka Euroopa andmekaitseinspektori 2006. aasta aruanne, lk 48.

([17]) Euroopa andmekaitseinspektor kavatseb võtta vastu arvamuse ENISA õigusliku raamistiku kohta veel 2010. aasta detsembris.

Liidu asutused, riiklikud ametiasutused, politsei ja ettevõtjad. Nende osalejate täpseid rolle ja pädevusvaldkondi sisejulgeoleku strateegia rakendamiseks kavandatavates konkreetsetes meetmetes tuleks käsitleda üksikasjalikumalt.

IV. KONKREETSED MÄRKUSED SISEJULGEOLEKU STRATEEGIAGA SEOTUD POLIITIKAVALDKONDADE KOHTA

Integreeritud piirihaldus

41. Teatises osutatakse asjaolule, et tänu Lissaboni lepingule on Euroopa Liidus lihtsam kasutada inimeste ja kaupade liikumisega seotud piirihalduspoliitikate koostoimet. Seoses isikute liikumisega on selles märgitud, et Euroopa Liit saab „rändevoogude haldamist ja kuritegudevastast võitlust käsitada integreeritud piirihalduse strateegia kaksikeesmärkidena". Dokumendis nähakse piirhaldust potentsiaalselt mõjusa raskete ja organiseeritud kuritegude tõkestamise vahendina ([18]).

42. Samuti märgib Euroopa andmekaitseinspektor, et teatis nimetab kolm strateegilist suunda: 1) piirikontrolli uue tehnoloogia tõhusam kasutamine (SIS II, viisainfosüsteem, riiki sisenemise ja riigist lahkumise süsteem ning registreeritud reisijate programm); 2) patrull- ja vaatlustegevuse uue tehnoloogia tõhusam kasutamine (Euroopa piiride valvamise süsteem, EUROSUR) ja 3) tugevdatud koostöö liikmesriikide vahel Frontexi raames.

43. Euroopa andmekaitseinspektor soovib kasutada võimalust ja tuletada käesolevas arvamuses meelde mitmes varasemas arvamuses esitatud taotlust kehtestada Euroopa Liidu tasandil selge piirihalduspoliitika, mis järgiks täiel määral andmekaitse-eeskirju. Euroopa andmekaitseinspektor usub, et praegu sisejulgeoleku strateegias ja infohaldusstrateegias toimuv töö on suurepärane võimalus võtta konkreetsemaid meetmeid nendes valdkondades sidusama poliitilise lähenemise saavutamiseks.

44. Euroopa andmekaitseinspektor märgib, et lisaks olemasolevatele ja lähitulevikus tõenäoliselt kasutusele võetavatele suuremahulistele süsteemidele (nagu SIS, SIS II ja viisainfosüsteem) osutatakse teatises ühtlasi sellistele süsteemidele, mille osas komisjoni võib edaspidi ettepaneku teha, kuid mille kohta ei ole otsust veel vastu võetud (st registreeritud reisijate programm ning riiki sisenemise ja riigist lahkumise süsteem). Sellega seoses tuleb meelde tuletada, et nende süsteemide kehtestamise eesmärgid ja õiguspärasus vajavad veel selgitamist ja tõendamist, pidades muu hulgas silmas ka komisjoni koostatud konkreetsete mõjuhinnangute tulemusi. Vastasel korral võib leida, et teatises rutatakse otsuste tegemise protsessist ette ega võeta arvesse asjaolu, et lõplikku otsust registreeritud reisijate programmi ning riiki sisenemise ja riigist lahkumise süsteemi kehtestamise kohta Euroopa Liidus ei ole veel tehtud.

45. Seepärast soovitab Euroopa andmekaitseinspektor tulevikus sisejulgeoleku strateegia rakendamiseks tehtavas töös sellist etteruttamist vältida. Nagu eelnevalt märgitud, tuleb uute eraellu tungivate suuremahuliste süsteemide kasutuselevõtmise otsus teha alles pärast kõigi olemasolevate süsteemide piisavat hindamist, võttes nõuetekohaselt arvesse vajalikkust ja proportsionaalsust.

EUROSUR

46. Teatises on märgitud, et komisjon esitab 2011. aastal EUROSURi loomise õigusakti ettepaneku, et parandada sisejulgeolekut ning võidelda kuritegevuse vastu. Samuti on selles öeldud, et EUROSURi puhul kasutatakse Euroopa Liidu rahastatud teadusprojektide ja -töö raames välja töötatud uusi tehnoloogiaid, nagu objektide tuvastamine ja jälgimine merepiiridel satelliidifotode abil (nt Euroopa Liitu uimasteid transportivate kiirete aluste jälgimine).

47. Sellega seoses märgib Euroopa andmekaitseinspektor, et ei ole selge, kas ja mil määral nähakse komisjoni poolt 2011. aastal esitatavas EUROSURi loomist käsitlevas õigusakti ettepanekus ette ka isikuandmete töötlemine EUROSURi raames. Komisjon ei ole teatises selle kohta selget seisukohta võtnud. See küsimus on veelgi asjakohasem, kui võtta arvesse asjaolu, et teatises on välja toodud EUROSURi ja Frontexi vahelised ilmsed seosed taktikalisel, operatiivsel ja strateegilisel tasandil (vt alljärgnevad märkused Frontexi kohta) ning ette nähtud nende kahe asutuse tihe koostöö.

Isikuandmete töötlemine FRONTEXIS

48. 17. mail 2010 esitas Euroopa andmekaitseinspektor arvamuse Frontexi määruse muutmise kohta ([19]), milles ta kutsus üles pidama põhjalikku arutelu ja süvitsi kaaluma andmekaitse küsimust seoses Frontexi praeguste ülesannete tugevdamisega ning talle uute kohustuste panemisega.

49. Teatises osutatakse vajadusele suurendada 4. eesmärgi raames (tugevdada turvalisust piiride halduse kaudu) Frontexi panust välispiiridel. Selle kohta märgitakse teatises, et tuginedes kogemustele ja lähtudes Euroopa Liidu üldisest

([18]) Pressiteade „ELi sisejulgeoleku strateegia toimimine: viis sammu turvalisema Euroopa suunas", memo 10/598.

([19]) Euroopa andmekaitseinspektori 17. mai 2010. aasta arvamus ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega muudetakse nõukogu määrust (EÜ) nr 2007/2004 Euroopa Liidu liikmesriikide välispiiril tehtava operatiivkoostöö juhtimise Euroopa agentuuri (Frontex) asutamise kohta.

lähenemisviisist teabehaldusele, arvab komisjon, et kui Frontex töötleb ja kasutab nimetatud andmeid piiratud ulatuses ja isikuandmete selgelt määratletud eeskirjade kohaselt, aitab see oluliselt kaasa kuritegelike organisatsioonide likvideerimisele. Võrreldes komisjoni ettepanekuga Frontexi määruse läbivaatamise kohta, mida praegu Euroopa Parlamendis ja nõukogus arutatakse ning milles isikuandmete kaitset ei nimetatud, on selline lähenemine uudne.

50. Seda arvestades väljendab Euroopa andmekaitseinspektor heameelt asjaolu üle, et teatises on viidatud teatud olukordadele, mil võib olla vaja sellist andmete töötlemist (nt riskianalüüs, ühisoperatsioonide parem toimimine või teabevahetus Europoliga). Täpsemalt selgitatakse teatises, et teavet salakaubaveovõrgustikes osalevate kurjategijate kohta, mis Frontexi käsutusse jõuab, ei saa praegu kasutada riskianalüüsides ega tulevaste ühisoperatsioonide parema suunamise huvides. Ka ei jõua kahtlustatavaid kurjategijaid käsitlevad andmed täiendavaks uurimiseks pädevate riiklike ametiasutuste ega Europolini.

51. Sellele vaatamata märgib Euroopa andmekaitseinspektor, et teatises ei osutata toimuvale arutelule Frontexi õigusliku raamistiku muutmise kohta, mille käigus, nagu eespool märgitud, püütakse leida sellele küsimusele õigusloomelisi lahendusi. Peale selle rõhutatakse teatise sõnastuses Frontexi rolli kuritegelike võrgustike likvideerimisega seotud eesmärgi all, mida võib käsitada Frontexi volituste laiendamisena. Euroopa andmekaitseinspektor soovitab seda küsimust arvestada nii Frontexi määruse muutmisel kui ka sisejulgeoleku strateegia rakendamisel.

52. Samuti juhib Euroopa andmekaitseinspektor tähelepanu vajadusele tagada, et Europoli ja Frontexi ülesanded ei kattu. Sellega seoses väljendab Euroopa andmekaitseinspektor heameelt selle üle, et teatise kohaselt tuleb vältida Frontexi ja Europoli ülesannete kattumist. Ent ka seda küsimust tuleks selgemalt käsitleda nii muudetud Frontexi määruses kui ka sisejulgeoleku strateegia rakendamiseks võetavates meetmetes, millega nähakse ette Frontexi ja Europoli tihe koostöö. See on eriti oluline otstarbe piiramise ja andmete kvaliteedi põhimõtte järgimisel. See märkus kehtib ka edasise koostöö kohta selliste asutustega nagu Euroopa Võrgu- ja Infoturbeamet (ENISA) või Euroopa Varjupaigaküsimuste Tugiamet.

Biomeetriliste andmete kasutamine

53. Teatises ei käsitleta eraldi biomeetriliste andmete järjest sagedamat kasutamist vabadusel, turvalisusel ja õigusel rajaneval alal, sealhulgas Euroopa Liidu suuremahulistes IT-süsteemides ja teistes piirihaldusvahendites.

54. Seepärast kasutab Euroopa andmekaitseinspektor võimalust tuletada meelde oma soovitust [20] sisejulgeoleku strateegia rakendamisel ja eriti piirhalduses seda andmekaitse seiskohast ülimalt tundlikku probleemi arvesse võtta.

55. Samuti soovitab Euroopa andmekaitseinspektor töötada välja vabadusel, turvalisusel ja õigusel rajaneval alal biomeetriliste andmete kasutamise kohta selged ja ranged meetmed, mis tugineksid põhjalikule hindamisele ja biomeetriliste andmete kasutamise vajalikkuse hindamisele sisejulgeoleku strateegia raames iga üksikjuhtumi korral eraldi, võttes seejuures täielikult arvesse selliseid andmekaitse aluspõhimõtteid nagu proportsionaalsus, vajalikkus ja otstarbe piiramine.

Terroristide rahastamise jälgimisprogramm

56. Teatises on öeldud, et komisjon töötab 2011. aastal välja Euroopa Liidu poliitika finantstehinguid käsitlevate sõnumiandmete kohta, mida säilitatakse Euroopa Liidu territooriumil. Sellega seoses viitab Euroopa andmekaitseinspektor oma 22. juuni 2010. aasta arvamusele finantstehinguid käsitlevate sõnumiandmete töötlemise ja edastamise kohta Euroopa Liidust Ameerika Ühendriikidesse terroristide rahastamise jälgimise programmi raames [21]. Kõik kõnealuses arvamuses esitatud kriitilised märkused on samaväärselt kehtivad ja kohaldatavad finantstehinguid käsitlevate sõnumiandmete Euroopa Liidu raamistikuga seotud kavandatava töö suhtes. Seepärast peaks neid selle küsimuse arutamisel arvesse võtma. Tähelepanu tuleks pöörata eelkõige muid kui kahtlustatavaid isikuid käsitlevate mahukate andmete väljavõtmise ja töötlemise proportsionaalsusele ning sõltumatute asutuste ja kohtute tõhusa järelevalve küsimusele.

Kodanike ja ettevõtjate turvalisus küberruumis

57. Euroopa andmekaitseinspektor väljendab heameelt selle üle, et teatises peetakse tähtsaks Euroopa Liidu tasandi ennetusmeetmeid, ning on seisukohal, et infotehnoloogiavõrkude turvalisuse suurendamine on oluline tegur, mis aitab kaasa hästi toimiva infoühiskonna saavutamisele. Samuti toetab Euroopa andmekaitseinspektor konkreetseid meetmeid küberrünnakutega toimetuleku suutlikkuse parandamiseks, õiguskaitse- ja kohtuasutuste suutlikkuse suurendamiseks ning tööstusharuga partnerluse loomiseks, et anda kodanikele ja ettevõtjatele paremad võimalused. Tervitatav on ka ENISA abistav roll mitme selle eesmärgi raames kavandatud meetme puhul.

[20] Vt eriti joonealuses märkuses nr 8 nimetatud Euroopa andmekaitseinspektori arvamust, mis käsitleb komisjoni teatist „Ülevaade teabehaldusest vabadusel, turvalisusel ja õigusel rajaneval alal".

[21] Euroopa andmekaitseinspektori 22. juuni 2010. aasta arvamus järgmise õigusakti ettepaneku kohta: nõukogu otsus, mis käsitleb Euroopa Liidu ja Ameerika Ühendriikide vahelise lepingu (mis käsitleb finantstehinguid käsitlevate sõnumiandmete töötlemist ja edastamist Euroopa Liidust Ameerika Ühendriikidesse terroristide rahastamise jälgimise programmi raames) sõlmimist.

58. *Sisejulgeoleku strateegia toimimist* käsitlevas teatises ei täpsustata aga küberruumis ette nähtud õiguskaitsemeetmeid, kuidas need meetmed võiksid ohustada üksikuid õigusi ja milline peaks olema nõutav kaitse. Euroopa andmekaitseinspektor kutsub üles töötama välja põhjalikum lähenemine asjakohastele tagatistele; selline lähenemine tuleks kehtestada kõikide üksikisikute põhiõiguste kaitseks, sealhulgas nende, keda võivad mõjutada võimaliku kuritegevusega võitlemiseks kõnealuses valdkonnas kavandatud meetmed.

V. **JÄRELDUSED JA SOOVITUSED**

59. Euroopa andmekaitseinspektor palub sisejulgeoleku strateegia rakendamise käigus siduda omavahel mitmesugused Euroopa Liidu strateegiad ja teatised. Sellisele lähenemisele peaks järgnema konkreetne ja vajaduste tegelikul hindamisel põhinev tegevuskava, mille tulemuseks oleksid kõikehõlmavad, terviklikud ja hästi ülesehitatud Euroopa Liidu tegevuspõhimõtted seoses sisejulgeoleku strateegiaga.

60. Ühtlasi kasutab Euroopa andmekaitseinspektor võimalust rõhutada, kui oluline on õiguslik nõue kõiki sisejulgeoleku strateegia ja teabevahetuse raames kasutatavaid olemasolevaid vahendeid enne uute vahendite kohta ettepanekute tegemist tegelikult hinnata. Siinkohal on ülimalt soovitatav asjaomaste vahendite tõhususe korrapärast hindamist nõudvate sätete lisamine.

61. Euroopa andmekaitseinspektor soovitab võtta nõukogu 2010. aasta novembri järeldustes ette nähtud mitmeaastase strateegilise kava koostamisel arvesse Euroopa Liidu toimimise lepingu artikli 16 alusel kõikehõlmava andmekaitseraamistiku loomiseks tehtavat tööd, eelkõige teatist (2009) 609.

62. Euroopa andmekaitseinspektor teeb mitu soovitust seoses andmekaitse seisukohast oluliste mõistete ja põhimõtetega, mida tuleks sisejulgeoleku strateegiaga seoses arvesse võtta, nagu eraelu kavandatud puutumatus, eraelu puutumatuse ja andmekaitse mõjuhinnang ning parim võimalik tehnika.

63. Euroopa andmekaitseinspektor soovitab koostada tulevaste vahendite rakendamisel eraelu puutumatuse ja andmekaitse mõjuhinnang kas eraldi või üldise, komisjoni koostatava põhiõiguste mõjuhinnangu raames.

64. Ühtlasi kutsub ta komisjoni üles töötama välja sidusam ja järjepidevam poliitika seoses biomeetriliste andmete kasutamise võimaldamisega sisejulgeoleku strateegia valdkonnas ning tagama andmesubjektide õiguste valdkonnas Euroopa Liidu tasandil suurem kooskõla.

65. Euroopa andmekaitseinspektor esitab ka mitu märkust isikuandmete töötlemise kohta piirhalduses ja eelkõige Frontexis ning ka võimalikus EUROSURi kontekstis.

Brüssel, 17. detsember 2010

Euroopa Andmekaitseinspektor

Peter HUSTINX