



EUROOPA ÜHENDUSTE NÕUKOGU

Brüssel, 16.6.2004
KOM (2004) 429 lõplik

KOMISJONI TEATIS NÕUKOGULE JA EUROOPA PARLAMENDILE

Õiguskaitseorganite teabe juurdepääsu parandamise kohta

SISUKORD

KOMISJONI TEATIS NÕUKOGULE JA EUROOPA PARLAMENDILE ÕIGUSKAITSEORGANITE TEABELE JUURDEPÄÄSU PARANDAMISE KOHTA	4
I PEATÜKK – SISSEJUHATUS, PÕHJENDUS JA POLIITILINE KONTEKST	4
II PEATÜKK – ANDMETELE PAREMA JUURDEPÄÄSU JA LUUREANDMETEST JUHINDUVA ÕIGUSKAITSE RAKENDAMISE SUUNAS EUROOPA LIIDU TASANDIL	5
2.1. Strateegilised eesmärgid.....	5
2.2. Andmetele ja teabele tõhusa juurdepääsu ning nende kogumise, talletamise, analüüsi ja vahetamise põhieesmärgid	6
2.2.1. Õiguskaitseorganite andmetele võrdväärse juurdepääsu printsiip	6
2.2.2. Juurdepääsutingimuste kaardistamine.....	7
2.2.3. Andmete kogumine	9
2.2.4. Andmevahetus ja -töötlus.....	9
2.2.5. Uurimistöö.....	10
2.3. Tõhusa luureandmetest juhinduva õiguskaitsevõime põhielemendid Euroopa Liidu tasandil	11
2.4. Usalduse loomine	13
III PEATÜKK – KÄESOLEVA TEATISEGA SEOTUD SEADUSANDLIKUD ALGATUSED	13

KOMISJONI TEATIS NÕUKOGULE JA EUROOPA PARLAMENDILE

ÕIGUSKAITSEORGANITE TEABELE JUURDEPÄÄSU PARANDAMISE KOHTA (ELi INFOPOLIITIKA)

I PEATÜKK – SISSEJUHATUS, PÕHJENDUS JA POLIITILINE KONTEKST

Ülevaade

Euroopa Nõukogu deklaratsioon terrorismi kohta¹ annab nõukogule korralduse läbi vaadata seadusandlikud meetmed teabevahetuse hõlbustamiseks liikmesriikide õiguskaitseorganite vahel. Komisjoni kutsutakse üles esitama juunis Euroopa Nõukogu istungil ettepanekuid isikuandmete vahetamise ja reisijate andmete kasutamise kohta terrorismivastase võitluse eesmärgil. Komisjoni ettepanekud peaksid sisaldama ka sätteid riiklikele õiguskaitseorganitele juurdepääsu võimaldamiseks Euroopa infosüsteemidele.

Käesolev teatis on komisjoni esimene panus vastuseks nõukogu üleskutsele.

Käesolevas teatises esitab komisjon senisest struktureeritumalt need tegurid, mis on äärmiselt tähtsad teabe vaba ringluse saavutamiseks liikmesriikide õiguskaitseorganite vahel. Praegu esineb teabe vabal ringlemisel takistusi, mis sunnivad muu hulgas nõukogu pühendama vastastikuste hinnangute kolmanda etapi sellele, et uurida “teabevahetust Europoli ja liikmesriikide ning erinevate liikmesriikide vahel”. Teabe killustamine ja selgepiirilise poliitika puudumine infokanalite kohta takistavad teabevahetust. Liikmesriikide vahelist teabevahetust takistavad juriidilised, tehnilised ja praktilised probleemid raskendavad teabe erinevate ministeeriumide vahel jaotumise ületamisega seotud probleemide lahendamist riigi tasandil. Nimetatud takistustest täpsema ülevaate saamiseks paneb komisjon ette viia läbi täielik teabele juurdepääsu tingimusi võrdlev analüüs, samuti kõigi huvitatud sidusrühmade, nimelt Euroopa andmekaitseinspektori, laialdane ja avatud nõupidamine. Teatis püüab ka pakkuda vahendeid suurte ohtude (nt terrorism) realiseerumise vältimiseks, tutvustades luure juhitava õiguskaitse kontseptsiooni Euroopa Liidu tasandil. Esitatud kava määratleb, kuidas seda saavutada, ja esitab õigusaktid konkreetsete juriidiliste probleemide kõrvaldamiseks. Käesolev teatis keskendub juurdepääsu parandamisele vajalikule ja asjakohasele teabele, samuti luure juhitava õiguskaitse Euroopa Liidu tasandil rakendamise laiale kontseptsioonile. See avaldab mõju ka rahvusvahelisele rollile, mida EL suudab täita.

Need kaks tegurit on ELi õiguskaitse infopoliitika alusmüüriks. Ühine tegevus selles valdkonnas toetab progressiivset vabaduse, julgeoleku ja õigluse piirkonna loomist, mille raames kindlustatakse isikute vaba liikumine ka uutes, Euroopa Liitu kui tervikut ohustava terrorismi ning muu raske ja organiseeritud kuritegevuse tingimustes. Õiguskorra tagamisega seotud tegevuse efektiivsus peaks toetuma inimõiguste ja põhivabaduste järgimisele, mida kaitsevad liikmesriikidele omased rahvusvahelised, Euroopa ja konstitutsioonilised traditsioonid. Lisaks sellele kindlustab komisjon seda poliitikat luues, et ühenduse õigust ja poliitikat võetakse nõuetekohaselt arvesse. Selline poliitika ei tohiks kindlasti luua õiguslikku ebamäärasust ega põhjendamatu majanduslikku koormust ettevõtlusele.

¹ Euroopa Nõukogu 25. märtsi 2004. aasta *Deklaratsioon terrorismivastase võitluse kohta*.

Komisjon kutsub liikmesriike ja kaasatud osapooli üles osalema järgnevas jõulises koostöös.

Esiteks tuleb astuda hädavajalikke samme selleks, et teha vajalikud ja asjakohased andmed ja teave kättesaadavaks Euroopa Liidu õiguskaitseorganitele, tõkestamaks terrorismi ning muid raske ja organiseeritud kuritegevuse vorme ja nende poolt põhjustatud ohtusid ning võitlemaks nende vastu. Sellega seoses tuleb meeles pidada, et sageli võib kuritegevus, mis näiliselt ei kuulu “raske või organiseeritud kuritegevuse” kategooriasse, selleni viia või sellega seotud olla.

Teiseks tuleb luua kõrgekvaliteediline Euroopa Liidu kriminaalluure ja seda kasutada. Nimetatud protsessi käigus saadud teadmised aitavad poliitilisel tasandil kooskõlastatult määratleda ELi õiguskaitse prioriteete ning õiguskaitseorganitel võidelda efektiivselt kodanike elu, füüsilist puutumatust ja julgeolekut ohustavale kuritegevuse vastu.

Kolmandaks tuleb tugevdada usaldust õiguskaitseorganite vahel. Andmebaasidele juurdepääsu ühtsete tingimuste rakendamine ja oskusteabe jagamine aitavad kaasa ühise infopoliitikaplatformi loomisele, kõrvaldades teabe efektiivse vahetamise objektiivsed takistused.

ELi õiguskaitseorganite infopoliitikat juhivad mitmed kaalutlused. Need on seotud kasvava teadlikkusega Euroopa Liidu haavatavuse kohta, terroristide tegevusest tulenevate ohtudega, Euroopa Liidu sõltuvusega omavahel ühendatud võrgustikest, vajadusega luua tugevdatud teabevool pädevate asutuste vahel, uuel tehnoloogial ja teadmistel põhinevate võimalustega õiguskaitsetegevuse ning samal ajal andmekaitse, turvalisuse ning seonduvate järelevalve- ja kontrollimehhanismide edendamisel.

Käesoleva teatise eesmärgiks on edendada teabevahetust kõigi õiguskaitseorganite, st mitte ainult politseiasutuste, vaid ka tolliasutuste, finantsluure üksuste vahel, koostööd kohtu- ja riigiprokuratuuri ning kõigi teiste avalike asutustega, mis osalevad selles protsessis, mis ulatub julgeolekuohu ja kuritegude varajasest avastamisest kuritegude toimepanijate süüdimõistmise ja karistamiseni. Riiklikku julgeolekut tagavatel ja luureasutustel on selles vaieldamatult tähtis roll. Need paljud omavahel seotud väljakutsed, millega Euroopa Liidu õiguskaitseorganite infopoliitika kavatseb tegelda, on esitatud järgnevates punktides.

Terrorismi ja organiseeritud kuritegevuse rahvusvahelise iseloomu tõttu tuleb arvesse võtta ka väliseid mõjureid. Teised riigid on loonud või võivad tulevikus luua oma õiguskaitseorganite infopoliitikaid ning me oleme juba näinud juhtumeid, kus seesugused poliitika mõjutavad Euroopa Liidu kodanikke ja ettevõtjaid. Esile võivad kerkida ka vastastikkuse probleemid. Võimalik, et mitmepoolsete lahenduste leidmiseks tuleb korraldada spetsiaalseid foorumeid. Põhjalikult tuleb arvesse võtta ka Euroopa Liidu poliitika mõju kolmandate riikide kodanikele, kindlustamaks, et õiguskorra alane koostöö nende riikidega ei kannatataks ja et kodanike õigusi järgitakse ilma ahistamata.

Esiteks teeb see poliitika vajalikud ja asjakohased andmed ja teabe² kättesaadavaks õiguskaitseorganitele, selleks et tõkestada terrorismi ja muid raske või organiseeritud kuritegevuse vorme ja nendest tulenevaid ohte ning võidelda nende vastu. Teiseks soodustab see kõrgekvaliteediliste kriminaalluureandmete kogumist ja kasutamist

² Käesolevas teatises tähendab mõiste “andmed” või “teave” “andmeid, teavet ja luureandmeid”, kui ei ole märgitud teisiti; mõiste “luureandmed” tähistab “kriminaalluureandmeid”.

Euroopa Liidu tasemel, et toetada poliitilist otsustamisprotsessi ja õiguskaitseorganeid, võitlemaks tõhusalt nende kuritegude vastu. Kolmandaks toetab see usalduse loomist pädevate talituste vahel. Käesoleva poliitika loomisel võetakse arvesse ka ühenduse poliitikaid ja ühenduse õigusakte; eelkõige järgib käesolev poliitika täielikult põhiõigusi.

Infopoliitika peab arvesse võtma järgmisi tegureid:

- **Julgeoleku** tagamine nõuab enneolematu ulatuses ühiseid kooskõlastatud toiminguid; sidusrühmadeks on liikmesriikide õiguskaitseorganid, valitsused, Euroopa täidesaatvad ja seadusandlikud võimud ning teised asutused Euroopa ja rahvusvahelisel tasandil.
- **Inimõiguste** tagamiseks tuleb leida asjakohane tasakaal ühelt poolt tugeva andmekaitse ja põhiõiguste asjakohase järgimise ning teisalt poolt oluliste avalike huvide, nagu riiklik julgeolek ning kuritegevuse tõkestamine, avastamine ja vastutusele võtmine, kaitsmisele suunatud õiguskaitsealase teabe kõrgetasemelise kasutamise vahel.
- **Tehnoloogia** osas on vaja ühilduvaid infosüsteeme, mis on kaitstud ebaseadusliku juurdepääsu vastu asjakohase andmekaitsega, sealhulgas andmetöötluse seire ja järelevalve ning uurimise kontroll. Infotehnoloogia kuritegevuskindlaks muutmine peaks esile tooma nõrgad küljed ning kuritegeliku tegevuse võimalused ning keskenduma andmete analüüsile, nt riski hindamisele ja profileerimisele.
- Tõhusa **koostöö** võimaldamiseks toetavad teabe kogumise, talletamise, analüüsi ja vahetamise ühtsed standardid oluliselt usalduse loomist pädevate asutuste vahel nii riiklikul kui Euroopa Liidu tasemel.
- Mitmeetapilise lähenemisviisi **rakendamine** nõuab pikaajalist püsivat koostööd.

II PEATÜKK – ANDMETELE PAREMA JUURDEPÄÄSU JA LUUREANDMETEST JUHINDUVA ÕIGUSKAITSE RAKENDAMISE SUUNAS EUROOPA LIIDU TASANDIL

2.1. Strateegilised eesmärgid

Käesoleva teatise eesmärk on luua ELi õiguskaitse infopoliitika, mis toetab Euroopa Liidu lepingu artikli 29 eesmärkide elluviimist, pakkudes turvaliste kanalite kaudu pädevamat teavet **olemasolevaks õiguskaitsealaseks koostööks** ja luues aluse **tõhusa luureandmetest juhinduva õiguskaitse loomiseks** kohalikul, riiklikul ja Euroopa tasandil, tuginedes vajalikule **usalduse loomisele**. Poliitika kavatsuseks on õiguslike, tehniliste ja organisatoorsete toimingute hõlmamine, mis kõik koos loovad õiguskaitseorganitele tingimused koostööks õiguskaitsele olulistele andmetele juurdepääsu tagamisel ja nende töötlemisel ning kriminaalluureandmete saamisel.

Üksikasjalikumalt on infopoliitika kavandatud tulemused järgmised:

- optimeerida juurdepääsu andmetele õiguskaitse põhitegevuse edendamiseks ning kriminaalluureandmete saamiseks;

- kindlustada, et asjakohased andmed muuks otstarbeks kui õiguskaitse on kättesaadavad niivõrd, kui see on otstarbekas, vajalik ja kooskõlas taotletavate eriomaste ja seaduslike eesmärkidega;³
- rajada ühised horisontaalstandardid (või juba olemasolevate horisontaalstandardite korral edendada nende tõhusat kasutamist) andmetele juurdepääsu, juurdepääsuloa andmise, teabe konfidentsiaalsuse, usaldusväärsuse, andmeturbe ja andmekaitse osas ning koostalitusstandardid riiklike ja rahvusvaheliste andmebaaside jaoks;
- luua kooskõlastatud luureandmete vormid poliitiliste ja operatiivotsuste tegemise protsessi hõlbustamiseks ning edendada samaväärsete meetodite arendamist ja kasutamist näiteks kriminaalsete võrgustike, kuritegevuse ohtude, riskide ja profiilide analüüsimisel, mida lisaks sellele toetavad majandusliku kahju hinnangud;
- luua alus kogu ELi hõlmava teabe kogumise ja analüüsimise prioriteetide seadmiseks ning seejärel parima tegevuskava valimiseks, et tõkestada ja võidelda terrorismi ja muu raske või organiseeritud kuritegevuse muude vormide ning nende poolt põhjustatud ohtude vastu;
- hõlbustada koostööl rajanevat ja koordineeritud õiguskaitsealast tegevust eesmärgiga tõkestada, uurida või katkestada tõhusalt ja vastavalt vajadusele terroristlikku ja tõsise või organiseeritud kuritegevuse teiste vormidega seotud tegevust.

Parem juurdepääs andmetele ja teabele toetab õiguskaitset igas liikmesriigis ja Euroopa tasandil, selleks et tõkestada terrorismi ja tõsise või organiseeritud kuritegevuse muid vorme ja neist tulenevaid ohte ning võidelda nende vastu. Täiendav lisandväärtus saavutatakse andmete metoodilise analüüsimise teel esmaklassilise kriminaalluure loomiseks. ELi luureandmetest juhinduva õiguskaitse toetamiseks tuleb vastu võtta riiklike kriminaalluuresüsteemide miinimumstandardid, mis võimaldavad ohu ühetaolist hindamist Euroopa tasandil.

2.2. Andmetele ja teabele tõhusa juurdepääsu ning nende kogumise, talletamise, analüüsi ja vahetamise põhieesmärgid

2.2.1. Õiguskaitseorganite andmetele võrdväärse juurdepääsu printsiip

Õiguskaitse infopoliitika esimeseks põhieesmärgiks on luua teabe vaba liikumine õiguskaitsetalituste, sh EUROPOLI ja EUROJUSTi vahel. Praegu saavad õiguskaitseorganid teostada otsinguid andmebaasides, millele on juurdepääs asjaomases riigis. Juurdepääs õiguskaitsetalituste hallatavale teabele teistest liikmesriikidest esitab aga väljakutseid, mille tõttu tehakse see praktikas võimatuks.

Infopoliitika eesmärgiks on seesuguse teabe reaalselt kättesaadavaks tegemine kõigile Euroopa Liidu õiguskaitseorganitele, sh EUROPOL ja EUROJUST, aitamaks neil täita oma funktsioone vastavalt õigusaktides ettenähtud korrale.

Eelnevas peatükis esitatud väljakutsete vältimiseks esitab infopoliitika “**andmetele võrdväärse juurdepääsu**” printsiibi. See annaks Euroopa Liidu õiguskaitseorganitele ja ametnikele õiguse juurdepääsuks andmetele ja andmebaasidele teistes Euroopa Liidu

³ Neli liikmesriiki esitasid seadusandliku ettepaneku andmete säilitamise kohta 2004. aasta aprilli JSK nõukogus. Komisjon näeb ette avatud arutelu nimetatud küsimuses.

liikmesriikides vastava liikmesriigi õiguskaitseorganitega võrreldavatel tingimustel. Nimetatud õigusega kaasneb kohustus võimaldada teiste liikmesriikide õiguskaitseametnikele juurdepääs andmetele oma riigi õiguskaitseametnikega samadel tingimustel.

Seega peavad liikmesriigid tegutsema vastavalt ELi mudelile, mis hõlmab selliseid küsimusi nagu ohu hindamise sünkroniseerimine ühise metoodika alusel ja selle süsteemikindel toetamine sektoraalse haavatavuse uuringute teel.

Võrdväärse juurdepääsu printsiibi järgi:

- on Euroopa Liidu ja selle kodanike julgeoleku tagamine ühine kohustus,
- liikmesriigid sõltuvad üksteisest õigusaktide jõustamisel terrorismi ja raske või organiseeritud kuritegevuse muude vormide ning nende poolt põhjustatud ohu tõkestamiseks ja nende vastu võitlemiseks;
- õiguskaitseorganid ühes liikmesriigis täidavad samu kohustusi ja neil on samasugused teabevajadused nagu taolistel organitel teises liikmesriigis;
- õiguskaitseorganid toimivad oma ülesannete täitmiseks andmetele ligi pääsesdes või andmebaasides otsinguid teostades vastavalt seadustele ning andmetekaitse ja andmeturbe üldistes standardites seatud piirides.

Põhimõtteliselt ei tohiks võrdväärse juurdepääsu õigus vähendada olemasolevate vastastikuse õigusabi instrumentide tõhusust. Kõiki võimalikke õiguslikke mõjusid tuleb hoolikalt analüüsida.

Läbipaistvad ja sirgjoonelised tingimused vajalikule ja asjakohasele teabele juurdepääsu tagamiseks kõigile Euroopa Liidu õiguskaitseorganitele tuleb koostada üldiste, sh andmekaitse ja andmeturbe standardite alusel. Liikmesriigid vastutavad nende tingimuste täitmise eest. Täitmise seiresüsteem luuakse pärast juurdepääsutingimuste määramist ülevaateharjutuse käigus (vt punkt 2.2.2).

Õiguskaitseorganite vahelise teabevahetuse põhitakistustega saab efektiivselt tegeleda vaid tingimusel, et kõik liikmesriigid viivad ellu konkreetseid abinõusid Euroopa kriminaalluuremudeli rajamiseks (vt punkt 2.3).

Euroopa infopoliitika eesmärgiks on kehtestada põhimõte, et Euroopa Liidu õiguskaitseorganitel on õigus võrdsele juurdepääsule vajalikele ja asjakohastele andmetele ja teabele. Komisjon uurib koos liikmesriikidega, missuguseid takistusi esineb, ning hindab selle alusel, kas on kohane esitada nõukogule ja Euroopa Parlamendile seadusandlik ettepanek selle kehtestamiseks Euroopa tasandil.

2.2.2. Juurdepääsutingimuste kaardistamine

Komisjon teeb ettepaneku olemasoleva ja liikmesriikide saadetud teabe alusel läbi viia täielik analüüs järgmiste tegurite kaardistamiseks:

- missugused andmed ja andmebaasid on juurdepääsetavad liikmesriigisiselt ja missugustele on juurdepääs välisriikides, kaasa arvatud registrid (*sisu*);
- mis on andmebaasi eesmärk (*eesmärgi defineerimine*);
- missugusel õiguskaitseorganil on juurdepääs konkreetsetele andmetele (*kasutajad*);
- millistel tingimustel on nimetatud organisatsioonidel juurdepääs andmetele ja andmebaasidele (*juurdepääsu eeskirjad*);

- millised on tehnilised nõuded juurdepääsuks andmetele ja andmebaasidele (*tehnilised protokollid*);
- kui sageli andmeid ja andmebaase kasutatakse (*asjakohasus*);
- millised andmed või andmebaasid pakuvad õiguskaitseorganitele huvi, kuid ei ole neile kättesaadavad; milliseid andmekaitsevahendeid kasutatakse (*vajaduste kaardistamine*).

Komisjon kavatseb:

- *alustada 2004. aasta lõpuks analüüsi õiguskaitseorganite andmetele ja andmebaasidele juurdepääsemise ulatuse, vajaduste ja piirangute määratlemiseks,*
- *käivitada uuringu õiguskaitsega (mitte)seotud andmetele juurdepääsu õigusnormide, tingimuste, sh IT-lahenduste ning andmekaitse ja -turbega seotud normide kohta.*

2.2.3. *Andmete kogumine*

Euroopa Liidu õiguskaitseorganid kasutavad andmete ja teabe kogumiseks ja liigitamiseks erinevaid lähenemisviise. Praegu ei ole erinevate teabeallikate konfidentsiaalsuse määramiseks ühtset foorumit.

Esimeseks ja kõige olulisemaks teabeallikaks on õiguskaitse ametkondade andmete kogumine. Juurdepääs andmetele, mis ei ole kogutud õiguskaitse eesmärgil, on täiendavaks strateegiliseks küsimuseks. See nõuab laiaulatuslikku ja avatud nõupidamist kõigi huvitatud sidusrühmadega, selgitamaks selle võimalikke mõjusid käitajatele ja kasutajatele ning ühenduse õigusele ja poliitikatele.

Erinevate juurdepääsuõiguste (nagu ühised *Euroopa standardid salastatud teabele juurdepääsu lubamiseks*, ühine *kasutajate juurdepääsuprofiilide* süsteem mitmesuguste juurdepääsuõiguste haldamiseks ja volitatud kasutajate registreerimise (*e kasutajakontode*) kinnitatud moodus) haldamise süsteem looks aluse juurdepääsu efektiivseks haldamiseks. Kasutajaprofiile saaks kasutada ka *logifailides ja kontrolljälje* süsteemides hoitavate andmete kasutamise ja töötlemise süstemaatiliseks jälgimiseks ja kontrollimiseks.

Komisjonil on kavas alustada uuringuid, et toetada seadusandlike ja mitteseadusandlike algatuste väljatöötamist, mis on seotud andmete kogumise miinimumstandardite, andmete konfidentsiaalsuse ja usaldusvääruse klassifitseerimise ühiste menetlusstandardite, salastatud teabele juurdepääsuks volituse andmise ühiste standardite ja kasutaja juurdepääsuprofiilidega.

Lisaks sellele korraldab komisjon ELi organiseeritud kuritegevuse tõkestamise foorumi raames konsultatsioone ja multidistsiplinaarseid tööseminare, et arutada avaliku ja erasektori partnerlust ja eriti juurdepääsu andmetele, mida ei ole kogutud õiguskaitse eesmärgil.

2.2.4. *Andmevahetus ja -töötlus*

Lisaks erinevatele võimalustele juurdepääsuks andmetele ja andmebaasidele võrdse juurdepääsu põhimõtte alusel on võimalik muuta olemasolevaid andmeid ja andmebaase paremini kättesaadavaks, luues neist võrgustikke või keskseid andmebaase. Selles kontekstis

kutsus Euroopa Nõukogu⁴ komisjoni üles “esitama ettepanekuid Euroopa andmebaaside (SISII, VIS ja EURODAC) koostalitlusvõime tõhustamiseks, kasutamaks nende lisandväärtust asjakohases õiguslikus ja tehnilises raamistikus terrorismi tõkestamisel ja selle vastu võitlemisel”.⁵ Tõhusam koostalitlusvõime peab arvesse võtma kehtivaid andmekaitse õigusnorme.

Komisjon on seisukohal, et ainus elujõuline võimalus tulevikuks on koostalitlusvõimeliste ja omavahel seotud Euroopa Liidu süsteemide loomine. Kontseptuaalselt kõikehõlmav IT-rajatis, mis integreerib riiklikud, Euroopa ja rahvusvahelised omavahel seotud süsteemid, võimaldab pikas perspektiivis märkimisväärset kokkuhoidu, sünergiat ja poliitikavõimalusi nii kriminaalluure kontekstis kui ka areneva Euroopa julgeolekustrateegia laiemas kontekstis.

Kavandada tuleks järk-järguline lähenemisviis, mis rajaneb andmete kodeerimise ühtlustatud formaatidele ja erinevate süsteemide juurdepääsureeglitele.

Euroopa Komisjoni läbi viidud varasemad nõupidamised sidusrühmadega⁶ on juba määratlenud terve rea küsimusi, mis võivad takistada teabevahetust, sealhulgas eriti:

- andmetöötlaste ühiste standardite ja tingimuste puudumine;
- ühiste andmetele juurdepääsustandardite puudumine;
- ühetaoliste kuriteode definitsioonide ja kuritegevusstatistika puudumine;
- õiguskaitseasutuste kasutatavate ühetaoliste IT-tehnoloogiate puudumine;
- enam kui üht asutust hõlmava õiguskaitsealase koostöö kultuuri puudumine;
- koostöö puudumine avaliku ja erasektori vahel;
- ühiste andmekaitse-eeskirjade mittetundmine ja ühise andmeturbe raamistiku puudumine.

Komisjon kavatses esitada teatise, et uurida tõhusaid viise andme jagamist tõkestavate põhitakistuste eemaldamiseks, mida vajadusel toetavad asjakohased saadusandlikud algatused.

2.2.5. Uurimistöö

Praegused Euroopa uurimisprogrammid käsitlevad teabe ning kommunikatsioonisüsteemide ja infrastruktuuride turvalisuse küsimusi. Komisjon on juba kaalunud vajadust kiirendada Euroopa turvalisusuuringute programmi ettevalmistamist Euroopa kodanike julgeoleku parandamiseks, algatades turvalisusuuringute ettevalmistustöö.⁷ See “turvalisusuuringute ettevalmistustöö” aastateks 2004–2006 (eelarve 65 miljonit eurot) toetab ja rahastab tegevusi, mis sondeerivad pinda 2007. aastast algava kõikehõlmava Euroopa turvalisusuuringute programmi jaoks.

Terrorism ja organiseeritud kuritegevus on Euroopa kodanike kaks peamist muret (80 % ELi kodanikest nimetavad terrorismi ja organiseeritud kuritegevust oma peamisteks hirmudeks). Praegu ei ole kriminaalluuresüsteemide või õiguskaitsega seotud uurimistegevus uurimisprogrammidega piisavalt kaetud. Seega on lisaks olemasolevatele programmidele vaja määratleda konkreetsed uurimistoimingud. Lisaks sellele on uurimistöid võimalik kaasfinantseerida ka programmi AGIS kaudu.

⁴ Euroopa Nõukogu 25. märtsi 2004. aasta *Deklaratsioon terrorismivastase võitluse kohta*.

⁵ Antud teema kohta valmistatakse ette eraldi komisjoni teatis.

⁶ Dublini deklaratsioon ja organiseeritud kuritegevuse tõkestamise foorumi istungite järelused.

⁷ KOM (2004) 72 lõplik.

- *Edendada uurimistööd turvaliste ja konfidentsiaalsete kommunikatsioonikanalite kohta programmi AGIS kaudu,*
- *algatada turvalise infovahetuse standardite arendamine eriti õiguskaitseorganite poolt ja nende vahel,*
- *käivitada eriuuring Euroopa kriminaalluuresüsteemide kasutamise ja rakendamise kohta, sh seonduvate ühiste standardite kohta metaandmete, turvalise andmevahetuse, täiustatud andmekaitsevahendite, automatiseeritud analüüsi, ohu- ja riskihindamise ning profileerimise meetodite jaoks.*

2.3. Tõhusa luureandmetest juhinduva õiguskaitsevõime põhielemendid Euroopa Liidu tasandil

Infopoliitika teine põhieesmärk on pakkuda välja sammud ELi luureandmetest juhinduva õiguskaitse loomiseks. Kriminaalluure aitab pädevatel asutustel täita oma strateegilisi või operatiivülesandeid terrorismi ja muu raske või organiseeritud kuritegevuse ja nende põhjustatud ohu tõkestamisel ning nende vastu võitlemisel.⁸ Euroopa kriminaalluure mudeli loomine lisab luureandmetest juhinduvale õiguskaitsele tõhusust ja võimaldab täiustatud koostööd. See hõlmaks selliseid küsimusi nagu ohu hindamise sünkroniseerimine ühise metoodika alusel, ohu hindamise süstemaatiline toetamine sektoraalsete haavatavuse uurimise kaudu ning vajalike rahaliste ja inimressursside eraldamine.

ELi õiguskaitse infopoliitika eesmärgiks on **vajaliku teabe kättesaadavaks tegemine Euroopa Liidu kriminaalluurevõrgustikule** esmaklassilise ELi kriminaalluure loomiseks, mille tulemuseks oleksid regulaarsed ELi strateegilise ja operatiivtegevuse hinnangud. Sellise ELi luurevõime arengus mängib olulist rolli ka Europoli infosüsteemi kättesaadavus.

Järgnevalt esitatud sammud peaksid viima olukorrani, kus strateegilised hinnangud on otsustajatele kergesti kättesaadavad õiguskaitse prioriteetide ülevaatamiseks nii sageli kui vaja. Lisaks sellele peaksid tegevuse hinnangud saama kättesaadavaks politseijõudude üksuste juhtidele, pakkudes parimaid kättesaadavaid taktikalisi teadmisi ohtude või kuritegevuse, sh terrorismi tõkestamiseks või selle vastu võitlemiseks vastavalt nõukogu seatud prioriteetidele.

Käesoleval ajal ei juhindu Euroopa Liidu õiguskaitse kriminaalluure andmetest, mis oleks suunatud Euroopa Liidu kui terviku julgeolekule. Praegu on pakiline vajadus kaitsta ELi kodanikke uute julgeolekuriskide ja ohtude eest. Seetõttu on äärmiselt vajalik ELi strateegilised ja tegevushinnangud kiiresti kättesaadavaks muuta. Samuti peaks luureandmete vahetamine olema seadusega määratletud ja austama indiviidi põhiõigusi.

Seetõttu nähakse järgnevat kaheetapilist lähenemist:

- Lühiajalises perspektiivis peaksid liikmesriikide kriminaalluuretalitused iga kuu kohtuma näiteks Europoli egiidi all, arutamaks riiklikke strateegilisi ja tegevushinnanguid. Europoli peaks toetama kõigi luureandmetega, mida ta saab kasutada. Selle tulemusena saadud luureandmed tuleks kokku võtta, et koostada Euroopa Liidu strateegilisi hinnanguid näiteks kaks korda aastas ja ELi tegevushinnanguid üks kord kuus. Euroopa Liidu strateegilised hinnangud võimaldaksid nõukogul seada õiguskaitse prioriteete.

⁸ *Kriminaalluure jaguneb strateegiliseks ja operatiiv- (või taktikaliseks) luureks. Strateegiline luure pakub vastuseid küsimusele, millised on ohud ja kuriteod, millele tuleb tähelepanu pöörata, ja operatiivluure pakub taktikalisi juhendeid, kuidas on kõige parem nendega tegelda ja prioriteete seada.*

Politseijõudude üksuste juhid peaksid tegevushinnangud edasi andma riigi õiguskaitseorganite operatiivtasanditele.

See peaks esimesel etapil esile tooma teabe, millele liikmesriikide kriminaalluurel ja Europolil on seaduslik juurdepääs vastavalt kehtivatele õigusaktidele, ja ära kasutama olemasolevaid analüütilisi vahendeid.

- Pikemas perspektiivis saavad riikide kriminaalluureorganid hakata standardiseeritud analüütilisi töövahendeid kasutades andma kriminaalluureandmeid Euroopa Liidus kättesaadavate asjakohaste õiguskaitseandmete alusel.

Europoli tähtsus kasvaks, kuna andmed ja nende esitajad oleksid Euroopast. Tulemuseks oleks ülimusliku kvaliteediga kriminaalluure, kuna see oleks enam standardiseeritud ja seega laiemalt mõistetav. Europoli, nõukogu ja politseijõudude üksuste juhtide vahelised suhted peavad kohanduma muutuvate tingimustega. Sel hetkel on Euroopa Liidul võimalik esineda rahvusvahelisel tasandil selgelt määratletud iseloomu ja omadustega õiguskorda kaitsva partnerina.

Komisjon näeb ette usaldusväärsete kriminaalluurehinnangute õigeaegse esitamise süsteemi loomiseks vajalike etappide uurimise ja raporti esitamise nõukogule 2005. aasta lõpuks.

Nõukogu seab prioriteedid kriminaalluurerühma arendatud strateegiliste hinnangute põhjal. Selline tegevushinnang peaks pakkuma võimalust konkreetsete tulemuste saavutamiseks, näiteks arreteerimisteks, kriminaalse tegevusega saadud varade arestimiseks või konfiskeerimiseks või jõupingutuste tegemiseks kriminaalse rühmituse lõhkumisel.

Üldkasutatavaid luuremeetodeid tuleks kohandada nii, et need sobiks kasutamiseks nii üldisel Euroopa Liidu tasandil kui spetsiaalsete rahvusvaheliste või piirkondlike küsimuste puhul (nt Läänemere maade organiseeritud kuritegevuse tööühm). Komisjon ja Europol peaksid läbi viima uurimuse erinevate meetodite kohta, mida liikmesriikide kriminaalluureorganid kasutavad, ja esitama 2005. aasta lõpuks ettepaneku Euroopa kriminaalluure analüütilise metoodika kohta. Sellega seoses võiks CEPOLile anda ülesande luua õppekava, et õpetada kriminaalanalüütikuid neid meetodeid ja tippjuhtkonda tegevushinnanguid parimal viisil kasutama. Üldiselt kasutatavad analüütilised meetodid⁹ peaksid andma tulemusi, mida saab kasutada Euroopa Liidu strateegiliste ja tegevushinnangute loomiseks.

- *Nõukogu võiks käesolevas teatises esitatud ideed heaks kiita, võimaldades nii vajalike sammude astumist nende elluviimiseks.*
- *Liikmesriikide kriminaalluureühenduste esindajad peaksid Europoli egiidi all kokku panema riiklikud strateegilised ja tegevushinnangud.*
- *Nõukogu võiks liikmesriike üles kutsuda luureandmeid Europolile kättesaadavaks tegema ning andma Europolile õigust kõikehõlmava ohuhinnangu koostamiseks. Tulli- ja piirikontrolliorganitele võiks anda ülesande koordineerida oma luureandmete kogumist Europoliga.*

⁹ Meetoditeks on tulemuste, kuritegevuse mudelite, kriminaalturgude, kriminaalvõrgustike, riskide (mida samuti kasutatakse juhtimisvahendina), sihtprofiilide (mida sageli nimetatakse "profileerimiseks"), kriminaaläri profiilide ning demograafiliste ja sotsiaalsete suundumuste analüüs.

- *Tuleks välja töötada ühised kuritegevuse statistika mõisted ja aruandestandardid.*
- *Tuleks välja töötada ühised analüüsimeetodid luureandmete koostamiseks Euroopa Liidu tasandil näiteks Europol'i egiidi all.*

2.4. Usalduse loomine

Infopoliitika kolmas põhieesmärk on kaasa aidata usalduse loomisele Euroopa õiguskaitseorganite, ametnike ja partnerite vahel, luues väärtushinnangute, standardite ja strateegilise suunitluse ühise platvormi.

Ühiste standardite juurutamine on ülioluline teabe kogumiseks, hindamiseks ja vahetamiseks usaldusliku keskkonna loomisel (punkt 2.2). Ühised standardid andmete kasutamisel ja töötlemisel, samuti ühitavad meetodid ohu, riski ja profiili hindamisel saavad möödapääsmatuks aluseks teabe efektiivsel vahetamisel strateegilisel ja operatiivtasandil. Nimetatud vahendid on efektiivsed vaid juhul, kui on pidev poliitiline toetus **ühise õiguskaitseruumi** rakendamisele Euroopa Liidus kokkusobivate riiklike kriminaalluuresüsteemide alusel, mis moodustavad koos kontseptuaalselt integreeritud Euroopa kriminaalluuremudel.

Vastavalt eeltoodule tuleb süsteemi toimimiseks luua ametlikud ja mitteametlikud töösuhted. Nimetatud aspektide arendamisele aitab kaasa kriminaalluuret ühetaoliselt mõistva õiguskaitse personali väljaõpetamine. Selles kontekstis peaks suur roll olema CEPOLil, eriti:

- regulaarsete väljaõppekursuste korraldamine võimalikele tulevastele strateegiliste otsuste tegijatele ja tippjuhtidele,
- mudelõppekava koostamine Euroopa kriminaalluureorganite kesktaseme juhtide väljaõpetamiseks riigi tasandil,
- kõigi ELi infopoliitika elementidega seotud õppemeetmete läbiviimine.

Muud meetmed, sh juba olemasolevad vahendid, näiteks vastastikune hindamine, konkreetsele eesmärgile pühendatud projektid programmi AGIS raames või teised organiseeritud kuritegevuse tõkestamise foorumi egiidi all läbi viidavad tegevused, tugevdaksid võrkkoostööalaseid jõupingutusi.

Viimaks tuleks arvesse võtta riiklike andmete järelevalveorganite rolli, kuna need aitavad luua seadusi toetavaid ja efektiivset demokraatlikku kontrolli pakkuvad ettevaatusabinõusid.

Usaldust ja konfidentsiaalsust loovad meetmed ja meetodid on fundamentaalse tähtsusega (ühised standardid ja metodoloogia), komisjoni visiooni järgi esitatakse vastavad ettepanekud 2005. aasta lõpuks.

Paralleelselt võiks nõukogu teha CEPOLile ettepaneku alustada luureametnike ühtse väljaõppekava väljatöötamist.

III PEATÜKK – KÄESOLEVA TEATISEGA SEOTUD SEADUSANDLIKUD ALGATUSED

Komisjon jätkab poliitika arendamist, sh seadusandlikud algatused seoses isikuandmete kaitsmisega kolmandas sambas ja reisijate andmete kasutamise õiguskaitse eesmärgil, viimane kooskõlas komisjoni 2003. aasta detsembri teatises¹⁰ esitatud põhimõtetega.

Ettepanek andmekaitse raamotsuse kohta rajab ühised standardid Euroopa Liidu lepingu VI jaotise alusel vahetatavate isikuandmete töötlemiseks eesmärgiga parandada politsei ja kohtuorganite juurdepääsu kõigile asjakohastele õiguskaitse andmetele kooskõlas põhiõigustega. Nimetatud raamotsus peaks looma ühe andmekaitseraamistiku kuritegevuse ja julgeolekuohtude tõkestamise, avastamise, uurimise ja vastutusele võtmise tarvis. See loob raamistiku spetsiifilisematele sätetele, mis sisalduvad teistes Euroopa Liidu tasandil vastuvõetud õigusaktides, ja vähendab veelgi tegelikke erinevusi teabevahetuses ühelt poolt liikmesriikide ja teiselt poolt liikmesriikide ja kolmandate riikide vahel ning sellesse on kätketud põhiõiguste kaitset kindlustav mehhanism.

¹⁰ KOM (2003) 826 lõplik, 16.12.2003, õhureisijate nimeregistri (PNR) andmete ülekandmise kohta. ELi üldine lähenemisviis.