EIROPAS KOPIENU KOMISIJA

Brisele, 16.6.2004
COM (2004) 429 final

KOMISIJAS PAZIŅOJUMS PADOMEI UN EIROPAS PARLAMANETAM

Par piekļuves uzlabošanu informācijai tiesībsargājošām iestādēm

SATURA RĀDĪTĀJS

KOMISIJAS PAZIŅOJUMS PADOMEI UN EIROPAS PARLAMANETAM PAR PIEKĻUVES UZLABOŠANU INFORMĀCIJAI TIESĪBSARGĀJOŠĀM IESTĀDĒM

I NODAĻA – IEVADS, RACIONĀLAIS UN POLITIKAS KONTEKSTS

Pārskats

Eiropadomes deklarācija par terorismu[1] uzdod Padomei iztirzāt likumdošanas pasākumus, lai vienkāršotu informācijas un izlūkošanas apmaiņu starp tiesībsargājošām iestādēm dalībvalstīs. Komisija ir aicināta izvirzīt priekšlikumus Jūnija Eiropadomei, attiecībā uz personiskās informācijas apmaiņu un pasažierinformācijas izmantošanu, lai apkarotu terorismu. Komisijas priekšlikumiem ir arī jāiekļauj nosacījumi, kas dod iespēju tiesībsargājošām iestādēm piekļūt Eiropas informācijas sistēmām.

Pašreizējais paziņojums ir pirmais devums no Komisijas puses kā atbilde uz Padomes lūgumu.

Šajā paziņojumā, Komisija izklāsta elementus, kas ir nozīmīgi, lai panāktu brīvu informācijas apriti starp dalībvalstu tiesībsargājošām iestādēm, daudz strukturētākā veidā, nekā tas ir bijis līdz šim. Pēdējā laikā eksistē šķēršļi brīvai informācijas apritei, kas, turklāt, liek Padomei veikt trešo piegājienu abpusējiem novērtējumiem, lai iztirzātu "informācijas un izlūkošanas apmaiņu starp Eiropolu un dalībvalstīm, un dalībvalstīm savā starpā". Informācijas sadalīšana atsevišķos nodalījumos un skaidras politikas trūkums par informācijas kanāliem, kavē informācijas apmaiņu. Izaicinājumu pārvarēt informācijas sadalīšanu starp dažādām ministrijām valsts ietvaros saasina juridiskas, tehniskas un praktiskas problēmas, kas kavē apmaiņu starp dalībvalstīm. Lai iegūtu daudz precīzāku priekšstatu par šiem šķēršļiem, Komisija ierosina uzsākt pilnīgu apstākļu uzskati, lai piekļūtu informācijai, kā arī, plašu konsultāciju ar visām ieinteresētajām pusēm, proti, Eiropas datu aizsardzības uzraugu. Paziņojums mērķē arī uz veidu paredzēšanu, lai novērstu galveno draudu īstenošanos, piemēram, terorisma, ieviešot ideju par ar prātu vadītu likuma piemērošanu ES līmenī. Tas paredz darba kārtību, kas izklāsta, kā to sasniegt, un tas deklarē likumdošanu, lai novērstu konkrētas juridiskās problēmas. Paziņojuma uzmanības centrā ir piekļuves uzlabošana nepieciešamajai svarīgajai informācijai, kā arī uz koncepciju, kas nepieciešama, lai ieviestu ar prātu vadītu likuma piemērošanu ES līmenī.

Šie divi elementi ir ES Informācijas politikas likuma piemērošanai veidojošie faktori. Kopēja darbība šajās nozarēs veicinās progresīvu brīvības, drošības un tieslietu jomu izveidi, kurās personu brīva kustība paliek nodrošināta, ņemot vērā drošības izaicinājumus, terorisms un citas organizētās noziedzības formas tiek izvirzītas Savienībai kopumā. Likuma piemērošanas aktivitāšu efektivitāti jāveido, ievērojot cilvēktiesības un pamat brīvību, ko sargā starptautiskās, Eiropas un konstitucionālās tradīcijas, kas kopīgas dalībvalstīm. Piedevām, kamēr tiek veidota šī politika, Komisija nodrošinās, lai Kopienas likumi un politikas savlaicīgi tiktu ņemtas vērā. Jo īpaši, šādai politikai nevajadzētu radīt juridisku nedrošību vai ekoomiskos apgrūtinājumus industrijām.

Komisija sasauc dalībvalstis un iesaistītās puses, lai iesaistītu sekojošās korporatīvās darbībās.

---

[1] 2004.gada 25.marta Eiropadomes deklarācija par terorisma apkarošanu.

Pirmkārt, veikt nepieciešamās darbības, lai darītu pieejamus ES tiesībsargājošām iestādēm nepieciešamos un būtiskos datus un informāciju, lai varētu novērst un apkarot terorismu un citas smagās vai organizētās noziedzības formas, kā arī draudus, ko tās izraisa. Šajā ziņā, jāpatur prātā, ka ļoti bieži kriminālā darbība, kas neietilpst kategorijā „smaga vai organizēta", var novest pie tādas vai būt saistīta ar tādu.

Otrkārt, lai sagatavotu un izmantotu augstas kvalitātes ES kriminālās izlūkošanas. Zināšanas, kas tiks iegūtas šajā procesā, politiskam līmenim palīdzēs noteikt ES likuma piemērošanas prioritātes saskaņotā veidā, un tiesībsargājošām iestādēm saskarties reāli ar noziegumiem un draudiem, kas apdraud mūsu pilsoņu dzīvības, fizisko integritāti un drošību.

Treškārt, paaugstināt uzticību starp likuma ieviešanas iestādēm. Kopēju nosacījumu ieviešana, piemēram, piekļuve datu sistēmām, un dalīšanās prasmēs, veicinās vienotas informācijas politikas platformas izveidošanu, jo īpaši likvidējot reālos šķēršļus efektīvai informācijas un ziņu apmaiņai.

Virkne apsvērumu noved ES Informācijas politiku pie likuma piemērošanas. Tie ir saistīti ar pieaugošo informētību par ES vārīgumu pret draudiem, kā tiem, ko ir izvirzījušas teroristu aktivitātes, Savienības atkarību no cieši saistītiem tīklojumiem; ar nepieciešamību veicināt paaugstinātas informācijas plūsmas starp kompetentajām iestādēm, ar jauno tehnoloģiju priekšrocībām un uz zināšanām balstītām iespējām atbalstīt likuma piemērošanas darbības un, tai pašā laikā, palielināt datu aizsardzību, drošību un saistīto kontroles un uzraudzības mehānismu.

Šajā paziņojumā ir iecerēts uzlabot informācijas apmaiņu starp visām tiesībsargājošām iestādēm, t.i., ne tikai starp policijas iestādēm, bet arī starp muitas iestādēm, finansiālās informācijas daļām, mijiedarbību ar tiesnešiem un prokuratūrām, un viesām pārējām valsts ierēdņu grupām, kas piedalās procesā, sākot ar drošības draudu atklāšanu pašā sākumā un kriminālpārkāpumiem, līdz pat vainīgā notiesāšanai un sodam. Nozīmīgā loma, ko Valsts drošības un izlūkošanas iestādes spēlē šajā sakarā, ir neapspriesta. Daudzas iekšēji saistītas problēmas, ko ES Informācijas politika likuma piemērošanai ir iecerējusi risināt, ir uzskaitīti sekojošajos paragrāfos.

Visbeidzot, ir jāņem vērā ārējā dimensija, dēļ izaicinājuma terorismam un organizētās noziedzības, ko mēs mēģinām risināt, starptautiskā rakstura. Citas valstis ir ieviesušas vai nākotnē ieviesīs savas Informācijas politikas likuma piemērošanai, mēs esam jau redzējuši gadījumus, kad šīs politikas ir no svara ES pilsoņiem un uzņēmējiem. Var rasties arī jautājumi, kuri savstarpēji mijiedarbojas. Var būt jāmeklē daudzpusējus risinājumus specializētos forumos. Ir jāņem vērā arī ietekme, kāda ES politikai var būt uz trešo valstu pilsoņiem, lai nodrošinātu gan to, ka nepasliktinās sadarbība ar šīm valstīm likumu piemērošanā, gan to, ka pilsoņu tiesības tiek ievērotas, bez diskriminācijas.

Šī politika darīs pieejamus nepieciešamos un būtiskos datus un informāciju, pirmkārt, tiesībsargājošajām iestādēm, lai novērstu un cīnītos pret terorismu un citām smagās un organizētās noziedzības formām, kā arī ar draudiem, ko tie izraisa[2]. Otrkārt, tā veicinās ES līmenī augstas kvalitātes krimināLo izlūkošanu, lai palīdzētu pieņemt politiskos lēmumus un tiesībsargājošām iestādēm veiksmīgi saskarties ar šiem noziegumiem. Treškārt, atbalstīs uzticības veidošanu starp kompetentajām iestādēm. Veidojot šo politiku, Kopienas politikas

[2] Šajā paziņojumā izteikums "dati" vai "informācija" nozīmē "dati, informācija un izlūkošana", ja vien nav savādāk norādīts; termins "izlūkošana" attiecas uz "krimināLizlūkošanu'.

un Kopienas juridiskie aspekti arī tiks ņemti vērā; īsāk sakot, šī politika pilnībā respektēs pamattiesības.

Informācijas politikai ir jāņem vērā sekojošie elementi:

- **Drošības** problēmas risināšanā ir nepieciešama kopīga un saskaņota darbība, visaugstākajā līmenī; ieinteresētās puses ir tiesībsargājošās iestādes, nacionālās valdības, Eiropas izpildorgāni un likumdevēj iestādes, un citi orgāni Eiropas un starptautiskajā līmenī.

- **Cilvēktiesību** problēmas risināšana nozīmē cenšanos panākt atbilstošu līdzsvaru starp robustu datu aizsardzību un pienācīgu citu pamattiesību ievērošanu, no vienas puses, un, no otras puses, veiksmīgu tiesībsargājošās informācijas izmantošanu ar mērķi aizsargāt svarīgas valsts intereses, tādas kā valsts drošība un noziedzības apkarošana, noziegumu atklāšana un prasību ierosināšana.

- Kas attiecas uz **tehnoloģiju**, ir nepieciešamas savienojamas informācijas sistēmas, kuras ir aizsargātas pret nelikumīgu piekļuvi, ar atbilstošu datu aizsardzību, ieskaitot datu apstrādes kontroli un pārraudzību, un izmeklēšanas audits. Informācijas tehnoloģiju noziegumu pārbaudēm ir jāatklāj vājās vietas un kriminālo darbību iespējas un ir jābūt koncentrētām uz datu analīzi, piemēram, uz riska novērtēšanu un profilēšanu.

- Lai atvieglotu efektīvo **sadarbību**, informācijas vākšanas, uzglabāšanas, analīzes un apmaiņas kopējie standarti būtiski atbalstīs uzticēšanās veidošanu starp kompetentajām iestādēm, gan valsts, gan ES līmenī.

- Multifāžu pieejas ieviešanai būs nepieciešama ilgtermiņa kooperatīvā darbība.

II NODAĻA – PRETIM LABĀKAI DATU PIEKĻUVEI UN LIKUMA PIEMĒROŠANAS IEVIEŠANAI ES LĪMENĪ, BALSTOTIES UZ IZLŪKOŠANU.

2.1. Stratēģiskie mērķi

Šī paziņojuma mērķis ir ieviest ES Informācijas politiku likuma piemērošanai, kas sekmēs LES 29.panta mērķu realizēšanu, nodrošinot labāku informāciju par drošajiem kanāliem par **pastāvošo sadarbību likuma piemērošanā** un sagatavošanas darbu veikšanu **saistībā ar likuma piemērošanu, kas balstīta uz izlūkošanu**, gan vietējā, gan Eiropas līmenī, ko apstiprina nepieciešamā **uzticības celšana**. Politikas plāns ietver juridiskās, tehniskās un organizatoriskās darbības, kas, saliktas kopā, nodrošinās tiesībsargājošām iestādēm struktūru sadarbībai, lai atvieglotu piekļuvi un datu apstrādi, kuri ir būtiski likuma piemērošanai un krimināllizlūkošanas izstrādāšanā.

Apskatot Informācijas politiku daudz sīkāk, iecerētie rezultāti ir:

- Piekļuves informācijai optimizēšana, turpmāko pamatlikumu ieviešanas pasākumiem, kā arī kriminālās izlūkošanas izstrāde;

- Nodrošināt, lai svarīgi dati, kuri nav ieviesti likuma piemērošanas nolūkiem, būtu pieejami, kamēr vien tie nav piemēroti, nepieciešami un pielāgoti specifiskiem un pamatotiem iemesliem, pēc kā tiecās[3];
- Noteikt horizontālos standartus, gadījumā, ja tie jau pastāv, veicināt efektīvu horizontālo standartu kopējo izmantošanu, lai piekļūtu datiem, novērtēšanu, informācijas konfidencionalitāti, uzticamību, datu drošību un datu aizsardzību, un savietojamības standartus valsts un starptautiskajām datubāzēm;
- Ieviest norunātos izlūkošanas veidus, lai atbalstītu politisko un operatīvo lēmumu pieņemšanu un attīstītu līdzīgu analīzes, piemēram, noziedzīgo tīklu, nozieguma draudu, riska, metožu izmantošanu;
- Nodrošināt pamatu prioritāšu noteikšanai informācijas vākšanā un analīzē ES mērogā un, līdz ar to, noteikto prioritāšu ietvaros izvēlēties vislabāko darbības kursu, lai novērstu un apkarotu terorismu un citas nopietnās vai organizētās noziedzības formas, kā arī tās izraisītos draudus;
- Sekmēt sadarbības spējīgu un saskaņotu tiesībsargājošo darbību ar mērķi efektīvi un kur nepieciešams novērst, izmeklēt un dezorganizēt teroristu aktivitātes un aktivitātes, kas saistītas ar citām nopietnās vai organizētās noziedzības formām.

Uzlabota piekļuve datiem, informācijai un izlūkošanai, veicinās likuma piemērošanu katrā dalībvalstī un Eiropas līmenī, lai novērstu un cīnītos pret terorismu un citām smagās un organizētās noziedzības formām, kā arī, ar, draudiem, ko tie izraisa. Papildus pievienotā vērtība parādīsies, kad dati tiks metodiski analizēti, lai sagatavotu augstākās klases krimināllizlūkošanu. Lai atbalstītu ES uz izlūkošanu balstītu likuma piemērošanu, ir jāapgūst valsts kriminālās izlūkošanas sistēmas minimālie standarti, kas nodrošina savienojamu draudu novērtēšanu Eiropas līmenī.

2.2. Pamatelementi efektīvai piekļuvei un datu un informācijas vākšana, glabāšana, analīze un apmaiņa

2.2.1. Līdzvērtīgās piekļuves datiem princips starp likuma pimērošanas iestādēm

Pirmajam Informācijas politikas likuma piemērošanai pamatuzdevumam ir jāveicina brīvu informācijas apriti starp tiesībsargājošajām iestādēm, tai skaitā Europol un Eurojust. Šobrīd, tiesībsargājošās iestādes var meklēt datubāzes, kas ir valstiski pieejamas. Tomēr, piekļuve informācijai, kuru pārvalda dalībvalstu tiesībsargājošās iestādes, ir praktiski neiespējama.

Informācijas politika cenšas padarīt šo informāciju praktiski pieejamu visām ES tiesībsargājošām iestādēm, tai skaitā Europol un Eurojust, lai palīdzētu tām pildīt savas funkcijas, saskaņā ar likuma varu.

Princips, ko Informācijas politika ievieš iepriekšējā nodaļā izklāstīto problēmu izlīdzināšanai, ir vienas no **'tiesībām uz līdzvērtīgu piekļuvi datiem'.** Tas sniegtu ES tiesībsargājošajām iestādēm un amatpersonām līdzvērtīgas piekļuves tiesības datiem un datubāzēm citās dalībvalstīs uz salīdzināmiem noteikumiem, kādi attiecas uz attiecīgās dalībvalsts tiesībsargājošajām iestādēm. Secinājums attiecībā uz šīm tiesībām ir pienākums citu

[3] Leģislatīvu priekšlikumu par datu saglabāšanu ir iesniegušas četras dalībvalstis 2004.gada aprīļa JHA Padomē. Komisija gaida atklātu apspriedi par šo jautājumu.

dalībvalstu tiesībsargājošo iestāžu amatpersonām sniegt piekļuvi uz tādiem pašiem noteikumiem, kādi tiek piemēroti valsts tiesībsargājošo iestāžu ierēdņiem.

Tas nozīmē dalībvalstu saistības rīkoties ES modeļa ietvaros attiecībā uz ta'diem jautājumiem kā draudu novērtēšanas sinhronizācija, pamatojoties uz kopējo metodoloģiju un sistemātisku draudu novērtēšanas pamatošanu, veuicot nozaru vājo punktu pētījumus.

Līdzvērtīgās piekļuves princips atzīst, ka:

– Savienības un tās pilsoņu drošība ir kopatbildība,

– Dalībvalstis ir atkarīgas viena no otras, lai ieviestu likumus, lai novērstu un cīnītos pret terorismu un citām smagās un organizētās noziedzības formām, un ietver to izraisītos draudus;

– Tiesībsargājošās iestādes dalībvalstīs pilda līdzīgus uzdevumus un tām ir vienāda informācijas nepieciešamība;

– Tiesībsargājošās iestādes rīkojas likumīgi, piekļūstot datiem vai pieprasījumu datubāzēm savu uzdevumu izpildei un robežās, kas noteiktas ar vispārējām normām par datu aizsardzību un datu drošību.

Principā, vienādas piekļuves tiesībām nevajadzētu samazināt esošo Savstarpējās tiesiskās palīdzības instrumentu efektivitāti. Jebkuras iespējamās tiesiskās sekas ir rūpīgi jāizanalizē.

Caurredzamie un godīgie apstākļi, lai piekļūtu nepieciešamajai un būtiskajai informācijai, visām ES tiesībsargājošajām iestādēm ir izveidoti, balstoties uz kopīgiem standartiem, iekaitot, uz datu aizsardzību un datu drošību. Dalībvalstis būs atbildīgas par šo apstākļu ieviešanu. Tiks izveidota sistēma, lai pārraudzītu ieviešanu, vadoties pēc piekļuves nosacījumu identifikācijas (skatīt 2.2.2. paragrāfu).
Informācijas apmaiņas starp tiesībsargājošajām iestādēm galvenos šķēršļus var sekmīgi risināt, tikai uzticot dalībvalstīm konkrētos pasākumus, lai izveidotu Eiropas krimināllizlūkošanas modeli (skatīt paragrāfu 2.3).
Eiropas Informācijas politika mērķē uz principa ieviešanu, kas nodrošina Eiropas tiesībsargājošajām iestādēm vienādu pieeju nepieciešamajiem un nozīmīgajiem datiem un informācijai. Komisija ar dalībvalstīm izskatīs, kuri šķēršļi eksistē, balstoties uz to, novērtēs leģislatīvā priekšlikuma iesniegšanas Padomei un Eiroparlamentam, kas ir saistīts ar tā apskatīšanu ES līmenī, atbilstību.

2.2.2. Piekļuves nosacījumu skenēšana

Komisija ierosina veikt pilnīgu apstākļu uzskati, balstoties uz pieejamo informāciju, kā arī uz informāciju, ko šai sakarā sniedz dalībvalstis, lai ieskicētu sekojošos elementus:

– Kuri dati vai datubāzes ir pieejamas *tiesībsargājošām iestādēm dalībvalstīs, un kuras ir pieejamas ārzemēs, ieskaitot indeksu datubāzes* (*saturs*);

– Kāds ir datubāzes mērķis *(mērķa definējums)*;

– Kurām *tiesībsargājošām iestādēm ir piekļuve datiem* (*lietotāji*);

– Saskaņā ar kādiem noteikumiem, šīm iestādēm ir piekļuve datiem un datubāzēm (*piekļuves protokols*);

– Kādas ir tehniskās prasības, lai piekļūtu šiem datiem un datubāzēm (*tehniskie protokoli*);

– Cik bieži piekļūst datiem un datubāzēm (*nozīmība*);

– Kuri dati vai datubāzes interesē *tiesībsargājošās iestādes,* bet nav tām pieejamas*;* kādi ir piemērojamie datu aizsardzības nosacījumi (*vajadzību apsvēršana*).

Komisija ir iecerējusi:

– ***uzsākt uzskaiti līdz 2004.gada beigām, lai noteiktu iespējas, vajadzības un saites, kas nepieciešamas, lai tiesībsargājošās iestādes varētu piekļūtu datiem un datubāzēm.***

– ***uzsākt tiesisko normu, nosacījumu izpēti, ietverot IT risinājumu piekļuvi (ne)likuma piemērošanas datiem, un procedūru, kas saistītas ar datu aizsardzības un datu drošības noteikumiem, izpēti.***

2.2.3. Datu vākšana

Tiesībsargājošās iestādes ES izmanto atšķirīgas pieejas informācijas vākšanā un klasifikācijā. Šobrīd nepastāv viens kopējs forums, kā klasificēt konfidencionalitāti par dažādiem informācijas avotiem.

Pirmais un galvenais informācijas avots ir datu vākšana no likuma piemērošanas pārvaldēm. Piekļuve datiem, kas nav savākti likuma piemērošanas nolūkos ir cits politikas jautājums. Tam ir nepieciešama plaša un atklāta apspriede ar ieinteresētajām pusēm,

Pirmais un galvenais informācijas avots ir datu vākšana no likuma piemērošanas pārvaldēm. Piekļuve datiem, kas nav savākti likuma piemērošanas nolūkos ir cits politikas jautājums. Tam ir nepieciešama plaša un atklāta apspriede ar ieinteresētajām pusēm, ņemot vērā iespējamo ietekmi uz Kopienas likumu un politiku patērētājiem un veidotājiem.

Sistēma, kas organizē atšķirīgo piekļūšanu privilēģijas, piemēram, *kopīgie Eiropas standarti autorizācijai un klasificētā piekļuve informācijai, patērētāju piekļuves profila* kopīgā sistēma, lai administrētu daudzās piekļuves tiesības, un autorizēto lietotāju autentiskais reģistrēšanas veids, nodrošinātu pamatu efektīvam piekļuves menedžmentam. Lietotāju profilus var izmantot arī, lai sistemātiski uzraudzītu un auditētu piekļuvi datiem.

Komisija ir paredzējusi sākt pētījumus, lai pamatotu likumdošanas un ārpus likumdošanas esošu iniciatīvu izstrādi, kas saistītas ar minimālajiem standartiem datu ieguvei, kopīgiem procesuālajiem standartiem konfidencialitātes klasificēšanai un datu uzticamībai, kopīgiem standartiem par pilnvarojumu izsniegšanu piekļuvei slepenai informācijai un lietotāju piekļuves profiliem.

Komisija turpmāk organizēs konsultācijas un daudzdisciplīnu seminārus, saskaņā ar ES Forumu par Organizētās noziedzības novēršanu, lai apspriestu publisko un privāto līdzdalību, jo sevišķi pieejamību datiem, kuri navsavākti likuma piemērošanas nolūkiem.

2.2.4. Datu apmaiņa un apstrāde

Papildus dažādiem veidiem, kā piekļūt datiem un datubāzēm saskaņā ar ekvivalentas piekļuves principu, otra alternatīva, kā uzlabot piekļuvi datiem un datubāzēm, ir savienot tos tīklā vai izveidot centrālas datubāzes. Šajā kontekstā Eiropas Padome[4] lūdza Komisiju

[4] Eiropas Padomes 2004. g. 25. marta Deklarācija par terorisma apkarošanu.

"iesniegt priekšlikumus, kā paaugstināt sadarbības iespējas starp Eiropas datubāzēm (SISH, VIS un EURODAC), lai izmantotu to pievienoto vērtību attiecīgajos tiesiskajos un tehniskajos ietvaros terorisma novēršanas un apkarošanas aspektā."[5] Paaugstinātajām sadarbības iespējām būs jāņem vērā piemērojamās tiesiskās normas par datu aizsardzību.

Komisija uzskata, ka vienīgā adekvātā alternatīva nākotnē ir savstarpēji operējamu un savstarpēji saistītu ES sistēmu izveide. Konceptuāli visaptveroša IT arhitektūra, kas ietver nacionālās, Eiropas un starptautiskās saiknes, ilgtermiņā piedāvā ievērojamu līdzekļu ietaupījumu, sinerģētikas un politikas iespējas gan kriminālajai izlūkošanai, gan plašākajā kontekstā – jaunveidojamajai Eiropas drošības stratēģijai.

Būtu jāizstrādā stadijās sadalīta pieeja, kas balstās uz saskaņotu datu šifrēšanas formātu un piekļuves noteikumu izstrādi dažādām sistēmām. Iepriekšējas konsultācijas ar iesaistītajām pusēm, ko rīkojusi Eiropas Komisija[6], jau ir norādījušas vairākus jautājumus, kas varētu radīt šķēršļus informācijas apmaiņai. Cita starpā tie it sevišķi ir:

– kopīgu standartu un datu apstrādes noteikumu trūkums;
– kopīgu datu piekļuves standartu trūkums;
– savietojamu nozieguma definīciju un noziedzības statistikas trūkums;
– savietojamu IT tehnoloģiju, ko izmanto likuma piemērošanas iestādes, trūkums;
– uz sadarbību balstītu likuma piemērošanas kultūru trūkums ārpus valstu robežām;
– sadarbības trūkums starp publisko un privāto sektoru;
– apziņas par kopīgu datu aizsardzības noteikumu nepieciešamību trūkums un kopīgu datu drošības ietvaru trūkums.

Komisija ir paredzējusi sniegt paziņojumu, lai izpētītu iedarbīgās metodes, kas likvidētu galvenos datu apmaiņai traucējošos šķēršļus un kas nepieciešamības gadījumos būtu balstītas uz attiecīgām likumdošanas iniciatīvām.

2.2.5. Pētījums

Pašreizējās Eiropas pētījumu programmas risina informācijas un komunikāciju sistēmu un infrastruktūras drošības jautājumu. Komisija jau ir izskatījusi nepieciešamību paātrināt Eiropas Drošības pētījumu programmas izstrādi, lai uzlabotu Eiropas iedzīvotāju drošību, uzsākot Sagatavošanas pasākumu par drošības pētījumu.[7] "Sagatavošanas pasākums 2004. – 2006. gadam (ar budžetu EUR 65 miljoni) atbalstītu un finansētu pasākumus esošās situācijas noskaidrošanā, ņemot vērā visaptverošo Eiropas Drošības pētījumu programmu no 2007. gada.

Eiropas iedzīvotāji terorismu un organizēto noziedzību uzskata par divām svarīgākajām problēmām (80% ES iedzīvotāju uztver terorismu un organizēto noziedzību kā galvenos draudus). Pašlaik izpētes pasākumi, kas attiecas uz kriminālās izlūkošanas sistēmām vai likuma piemērošanu, nav pietiekami iekļauti pētījumu programmās. Tāpēc ir nepieciešams definēt konkrētus pētījumu pasākumus papildus jau esošajām programmām. bez pētījumu pasākumu līdzfinansēšanas AGIS programmas ietvaros ir iespējams:

– ***sekmēt pētījumus par drošiem un konfidenciāliem saziņas kanāliem ar AGIS programmas starpniecību;***

[5] Par šo tematu tiks sagatavots atsevišķs Komisijas Paziņojums.
[6] Dublinas deklarācija un Organizētās noziedzības novēršanas foruma apspriežu slēdzieni.
[7] COM (2004) 72 fin.

– ***uzsākt standartu izstrādi drošai informācijas apmaiņai, it sevišķi starp likuma piemērošanas iestādēm;***
– ***uzsākt konkrētus pētījumus par Eiropas kriminālās izlūkošanas sistēmu izmantošanu un īstenošanu, ieskaitot ar to saistītos kopīgos standartus metadatiem, drošai informācijas apmaiņai, paaugstinātas datu aizsardzības līdzekļiem, automatizētai analīzei, draudu un risku novērtējumam un profilu izstrādes metodēm.***

2.3. Galvenie elementi efektīvai, uz kriminālās izlūkošanu balstītai likuma piemērošanas spējai ES līmenī

Otrs Informācijas politikas pamatmērķis ir ieteikt pasākumus, lai attīstītu likuma piemērošanu ES, kas balstās uz kriminālo izlūkošanu. Kriminālā izlūkošana palīdz kompetentām iestādēm īstenot to stratēģiskos vai operatīvos mērķus, lai novērstu un apkarotu terorismu un citas bīstamas organizētās noziedzības formas un radītos draudus.[8] Eiropas Kriminālās izlūkošanas modeļa ieviešana paaugstinātu uz kriminālo izlūkošanu balstītās likuma piemērošanas efektivitāti un ļautu palielināt sadarbības apmērus. Tā ietvertu tādus jautājumus kā draudu novērtējuma sinhronizēšana pēc kopīgas metodoloģijas, draudu novērtēšanas sistemātiska pamatošana ar īpašām briesmām pakļauto sektoru izpēti un nepieciešamo finanšu un cilvēku resursu piešķīrums.

ES Informācijas likuma piemērošanas politikas mērķis **ir padarīt vajadzīgo informāciju pieejamu ES kriminālās izlūkošanas tīklam,** lai radītu pirmklasīgu ES kriminālās izlūkošanas sistēmu, kuras rezultātā tiktu doti periodiski ES stratēģiskie un operatīvie novērtējumi. Eiropola Informācijas sistēmas pieejamībai arī būs nozīmīga loma šādas ES kriminālās izlūkošanas spējas attīstībā.

Turpmāk norādītie posmi veidos situāciju, kad stratēģiskie novērtējumi jau ir pieejami lēmumu pieņēmējiem, lai apsvērtu likuma piemērošanas prioritātes, cik bieži tas ir nepieciešams. Papildus tam, Padome piešķir prioritāti Policijas speciālo grupu vadītājiem (CPTF), kas sniedz vislabākās pieejamās taktiskās zināšanas, lai novērstu vai apkarotu draudus un noziedzību, ieskaitot terorismu.

Pašlaik ES likuma piemērošanas iestādes nevadās no kriminālās izlūkošanas, kuras mērķis ir ES kā veseluma drošība. Šodien pastāv aktuāla nepieciešamība aizsargāt ES iedzīvotājus pret jauniem drošības riskiem un draudiem. Tāpēc ir būtiski svarīgi, lai ES stratēģiskie un operatīvie novērtējumi kļūtu pieejami pēc iespējas ātrāk. Līdzīgā veidā izlūkošanas informācijas apmaiņai jābalstās uz likuma normām un cieņai pret cilvēku pamattiesībām.

Tāpēc ir paredzēta šāda divu fāžu pieeja:

- Īstemiņā Dalībvalstu kriminālās izlūkošanas dienestiem jārīko apspriedes katru mēnesi, iespējams, ar Eiropola atbalstu, lai apspriestu savus nacionālos stratēģiskos un operatīvos novērtējumus. Eiropolam jādod visa palīdzība ar tam pieejamo informāciju. Šādi iegūtās ziņas jāapkopo, lai izstrādātu ES stratēģiskos novērtējumus, piemēram, divas reizes gadā, un ES operatīvos novērtējumus katru mēnesi. ES stratēģiskie novērtējumi ļautu Padomei

[8] Kriminālā izlūkošana iedalās stratēģiskajā un operatīvajā (jeb taktiskajā) izlūkošanā. Stratēģiskā izlūkošana dod ieskatu jautājumā par to, kādi ir draudi un noziegumi, pret kuriem jāvēršas, bet operatīvā izlūkošana dod taktiskas vadlīnijas, kā vislabāk rīkoties pret tiem un kādas ir to prioritātes.

noteikt likuma piemērošanas prioritātes. CPTF jāiesniedz operatīvie novērtējumi līdz operatīvajam līmenim nacionālo likuma piemērošanas iestāžu ietvaros.

Pirmajā fāzē jābalstās uz informāciju, ko Dalībvalstu kriminālā izlūkošana un Eiropols var likumīgi iegūt saskaņā ar pašreizējo likumdošanu, un jāizmanto pieejamie analīzes līdzekļi.

- Ilgtermiņā nacionālās kriminālās izlūkošanas iestādes var sākt kriminālās izlūkošanas ziņu izstrādi, izmantojot standartizētus analīzes līdzekļus saskaņā ar attiecīgajiem likuma piemērošanas datiem Eiropas Savienībā.

Eiropola nozīme pieaugs, jo dati un procedūras iegūs Eiropas mērogu. Tā rezultātā veidosies teicamas kvalitātes krimināla izlūkošana, jo tā būs lielākā mērā standartizēta un plašāk saprotama. Attiecībām starp Eiropolu, Padomi un CPTF jāpieskaņojas mainīgajiem apstākļiem. Tajā laikā ES būs spējīga darboties starptautiskajā arēnā kā likuma piemērošanas partneris ar savu noteiktu raksturu un kvalitāti.

Komisija paredz izpētīt nepieciešamos soļus, lai izveidotu sistēmu savlaicīgai uzticama kriminālās izlūkošanas novērtējuma sagatavošanai un iesniegtu ziņojumu Padomei līdz 2005. gada beigām.

Padome noteiks prioritātes uz stratēģisko novērtējumu pamata, ko izstrādās Kriminālās izlūkošanas grupa. Šādi operatīvie novērtējumi piedāvās iespēju iegūt konkrētus rezultātus, piemēram, izdarīt arestus, apķīlāt vai konfiscēt noziedzīgā darbībā iegūtu mantu vai veikt mērķtiecīgus pasākumus kādas kriminālas grupas likvidēšanai.

Kopīgi izmantotas izlūkošanas metodes tiks formatizētas, lai pieskaņotu tās lietošanai ne tikai vispārējā ES līmenī, bet arī ar nolūku risināt starpreģionālus vai reģionālus jautājumus (piem., Baltijas jūras Speciālā grupa par organizētās noziedzības problēmām). Komisijai un Eiropolam jāveic pētījums par dažādām metodēm, ko izmanto Dalībvalstu kriminālās izlūkošanas iestādes, un līdz 2005. gada beigām jāiesaka Eiropas analītiskā metodoloģija kriminālajai izlūkošanai. Saistībā ar to var griezties pie CEPOL izveidot apmācības programmu, kas apmācītu kriminālanalītiķus šo metožu izmantošanā un vadošos kadrus, kā vislabāk izmantot operatīvos novērtējumus. Parasti lietotajām metodēm[9] jādod rezultāti, kurus var izmantot ES stratēģisko un operatīvo novērtējumu sagatavošanā.

–	***Šī Paziņojuma nostādnes jāapstiprina Padomei, lai varētu veikt nepieciešamos pasākumus to īstenošanā.***
–	***Ar Eiropola atbalstu Dalībvalstu kriminālās izlūkošanas orgānu pārstāvjiem jāievāc nacionālie stratēģiskie un operatīvie novērtējumi.***
–	***Padomei jāgriežas pie Dalībvalstīm ar lūgumu nodot izlūkošanas datus Eiropola rīcībā un piešķirt Eiropolam pilnvaras izstrādāt visaptverošu draudu novērtējumu. Muitas un robežu kontroles iestādēm jādod rīkojums saskaņot savu izlūkošanas ziņu sagatavošanu ar Eiropolu.***
–	***Jāizstrādā kopīgas noziedzības statistikas definīcijas un atskaišu sniegšanas standarti.***

[9] Metodes ir analīze par rezultātiem, noziegumu modeļiem, noziedzības tirgu, noziedznieku tīkliem, riskiem (kas tiek izmantots kā vadības līdzeklis), mērķu profili ("profilēšana"), noziedzīgā biznesa profili un demogrāfiskās un sociālās tendences.

– ***Jāizstrādā kopīgas analīzes metodes izlūkošanas datu sagatavošanai ES līmenī, iespējams, ar Eiropola atbalstu.***

2.4. Uzticības veidošana

Informācijas politikas trešais pamatmērķis ir veicināt uzticības veidošanu starp Eiropas tiesībsargājošām iestādēm, ierēdņiem un kompanjoniem, izveidojot kopīgu platformu no kopīgām vērtībām, standartiem, un politiskajām ievirzēm.

Kopīgu standartu ieviešana ir būtiska, lai radītu uzticības vidi informācijas, vākšanai, piekļuvei un apmaiņai (skat. 2.2. nodaļu). Kopīgi standarti datu piekļuvei un apstrādei, kā arī savietojamas metodoloģijas draudu, risku un profilu novērtēšanai kļūs par obligātu pamatu efektīvai informācijas un izlūkošanas ziņu apmaiņai stratēģiskajā un operatīvajā līmenī. Šie pasākumi būs efektīvi tikai tad. ja būs nepārtraukts politisks atbalsts **kopīgas likuma piemērošanas telpas** izveidei Eiropas Savienībā, kas balstās uz savietojamām nacionālajām kriminālās izlūkošanas sistēmām, kuras kopā veido konceptuāli integrētu Eiropas kriminālās izlūkošanas modeli.

Atbilstošā veidā formālās un neformālās darba attiecības jāattīsta, lai šī sistēma varētu funkcionēt. Likuma piemērošanas iestāžu darbinieku apmācība, lai veidotu kopīgu sapratni par krimināLo izlūkošanu, sekmēs šo aspektu attīstību. CEPOL jāspēlē būtiska loma šajā kontekstā, it sevišķi:

– izveidojot regulārus apmācības kursus potenciālajiem nākotnes politikas lēmumu pieņēmējiem un vadošajiem darbiniekiem;
– izstrādājot modeļu plānus vidējā ranga vadītāju apmācībai Eiropas kriminālās izlūkošanas jautājumos nacionālajā līmenī;
– rīkojot apmācības pasākumus, kas attiecas uz visiem ES informācijas politikas elementiem.

Citi pasākumi pastiprinās kopīga tīkla izveides pasākumus, ieskaitot pasākumus, kas balstās uz jau esošiem paņēmieniem, tādiem kā novērtējumi, mērķtiecīgi projekti AGIS programmas ietvaros vai darbības, kas tiek veiktas ar Organizētās noziedzības novēršanas foruma atbalstu.

Visbeidzot nacionālo datu uzraudzības iestāžu loma arī pienācīgi jāņem vērā, jo tās dos ieguldījumu, lai izveidotu nepieciešamās garantijas likuma varas atbalstam un nodrošinātu efektīvu demokrātisku kontroli.

Uzticības – un pārliecības – ieviešanas pasākumi un tehnikas ir ļoti svarīgi (kopējie standarti un metodoloģijas) Komisija paredz iesniegt priekšlikumus līdz 2005.gada beigām.

Paralēli Padome varētu uzaicināt CEPOL sākt kopīgas plāna izstrādi kriminālās izlūkošanas darbinieku apmācībai.

III NODAĻA – LIKUMDOŠANAS INICIATĪVAS, KAS SAISTĪTAS AR ŠO PAZIŅOJUMU

Komisija turpinās izstrādāt politiku, ieskaitot likumdošanas iniciatīvas personas datu aizsardzības jomā trešajā "stūrakmenī" un pasažierinformācijas izmantošanā likuma

piemērošanas nolūkos atbilstoši principiem, kas izklāstīti Komisijas 2-3. gada decembra Paziņojumā.[10]

Ietvaru lēmuma par datu aizsardzību priekšlikums noteiks kopīgus standartus personas datu apstrādei, kuru apmaiņa notikusi saskaņā ar Eiropas Savienības Līguma VI pantu, lai pilnvarotu policijas un tiesu orgānu piekļūšanu visiem attiecīgajiem likuma piemērošanas datiem saskaņā ar pamattiesībām. Šis Ietvara lēmums izveidos vienotu vispārēju datu aizsardzības ietvaru sadarbības nolūkos, lai novērstu, atklātu, izmeklētu noziegumus un drošības draudus un uzsāktu tiesisku vajāšanu. Tas izveidos ietvaru konkrētākiem noteikumiem, kas iekļauti dažādos ES līmenī pieņemtajos normatīvajos aktos, un turpmāk mazinās praktiskās atšķirības informācijas apmaiņā starp Dalībvalstīm, no vienas puses, un Dalībvalstīm un trešām valstīm, no otras puses, un nodrošinās mehānismu, kas garantēs pamattiesību aizsardzību.

***

[10] COM (2003) 826 final no 16.12.03. par Lidmašīnu pasažieru vārdu uzskaites (PNR) datu nodošanu. Globāla ES pieeja.