Tiesībsarga viedoklis par saglabājamo datu nodošanu tiesībsargājošajām iestādēm (2007. gada septembris)

Saskaņā ar Elektronisko sakaru likumu saglabājamie dati ir likuma 1. un 2.pielikumā minētie noslodzes dati, atrašanās vietas dati un ar tiem saistīti dati, kas nepieciešami, lai identificētu abonentu vai lietotāju. Tie ietver informāciju par to, kas, kam un kad zvana, bet mobilā tālruņa lietošanas gadījumā tā var būt arī informācija par personas atrašanās vietu savienojuma sākumā. Elektronisko sakaru likuma 19.panta pirmās daļas 11.punkts un 71.1pants paredz elektronisko sakaru komersantam pienākumu nodrošināt saglabājamo datu glabāšanu 18 mēnešus, kā arī to nodošanu pirmstiesas izmeklēšanas iestādēm, operatīvās darbības subjektiem, valsts drošības iestādēm, prokuratūrai un tiesai, ja šīs institūcijas tos pieprasa. Tātad šīs iestādes no elektronisko sakaru komersanta var iegūt informāciju par to, kas, kam, kad zvana un kur persona atradās noteiktā laikā.

Latvijas Republikas Satversmes 96.pants garantē ikvienam tiesības uz privātās dzīves un korespondences neaizskaramību. Šādas tiesības ir garantētas arī Latvijai saistošās Eiropas Cilvēktiesību konvencijas 8.pantā.

Saglabājamo datu nodošana valsts iestādēm ir iejaukšanās personas tiesībās uz privātās dzīves un korespondences neaizskaramību. Tiesības uz privātās dzīves un korespondences neaizskaramību aizsargā ne tikai saziņas saturu, bet arī informāciju par saziņas apstākļiem. Šo tiesību uzdevums ir nodrošināt brīvu saziņu starp personām. Ja valsts var neierobežoti iejaukties personas saziņā, iegūstot informāciju par saziņas apstākļiem vai saturu, tas rada risku, ka personas šī iemesla dēļ var atteikties no saziņas vispār vai arī mainīt saziņas formu vai saturu. Līdz ar to personas vairs nelemj par saziņu brīvi.1
Eiropas Cilvēktiesību tiesa jau 1984.gadā lietā Malone v. The United Kingdom atzina, ka informācijas nodošana policijai bez datu subjekta piekrišanas par to, uz kādu telefona numuru zvanīts, kā arī par zvana laiku un zvana ilgumu, ir iejaukšanās personas tiesībās uz privātās dzīves un korespondences neaizskaramību.2 Paskaidrojošajā ziņojumā par Eiropas Padomes Ministru komitejas rekomendāciju Nr. R(95)4 norādīts, ka šādu datu vākšana un nodošana valsts iestādēm bez datu subjekta piekrišanas ir iejaukšanās personas tiesībās uz privātās dzīves un korespondences neaizskaramību.3 Arī Vācijas Federālā konstitucionālā tiesa savos spriedumos ir atzinusi, ka tiesības uz korespondences neaizskaramību attiecas arī uz informāciju par to, vai, kad, cik bieži un starp kādām personām ir notikusi saziņa vai mēģinājums sazināties.4

Taču tiesības uz privātās dzīves un korespondences neaizskaramību nav absolūtas. Tās var ierobežot, ja ierobežojums ir noteikts ar likumu, tas kalpo leģitīmam mērķim un ir nepieciešams demokrātiskā sabiedrībā.

Šajā gadījumā var konstatēt, ka Elektronisko sakaru likuma 19.pants un 71.1pants paredz, ka elektronisko sakaru komersantam ir pienākums nodot saglabājamos datus pirmstiesas izmeklēšanas iestādēm, operatīvās darbības subjektiem, valsts drošības iestādēm, prokuratūrai un tiesai. Tātad tiesību uz privātās dzīves neaizskaramību ierobežojums ir paredzēts likumā. Taču, lai atzītu, ka ierobežojums ir noteikts ar likumu, nepietiek ar to, ka ārējā normatīvā aktā ir norma, kas ļauj ierobežot tiesības. Likumam, kas paredz ierobežojumu, ir jāatbilst arī zināmām kvalitātes prasībām. Tam

ir jābūt pietiekami skaidram un precīzam, lai indivīds varētu prognozēt, kādos apstākļos un pie kādiem nosacījumiem iestādes šo normu piemēros.5

Ja ierobežojums izpaužas kā datu nodošana iestādēm bez datu subjekta piekrišanas, tad likums var tikt atzīts par pietiekami skaidru un precīzu, ja tas nosaka arī procedūru, kādā dati tiek nodoti.6 Elektronisko sakaru likums saglabājamo datu nodošanas procedūru nenosaka pietiekami skaidri un precīzi. Elektronisko sakaru likumā šis jautājums faktiski nav regulēts, tikai 71.1panta ceturtajā daļā Ministru kabinetam ir dots pilnvarojums noteikt saglabājamo datu pieprasīšanas un nodošanas kārtību. Taču Ministru kabinetam, realizējot šo pilnvarojumu, ir jāņem vērā arī Kriminālprocesa likumā un Operatīvās darbības likumā noteiktais. Diskusijas, kas izraisījās darba grupā, izstrādājot likumprojektu „Grozījumi Elektronisko sakaru likumā", kā arī Ministru kabineta noteikumu projektu par saglabājamo datu pieprasīšanas un nodošanas kārtību, liecina par to, ka nav vienotas izpratnes par šajos likumos noteikto saglabājamo datu nodošanas procedūru. Normu neskaidrību un neprecizitāti apliecina arī tas, ka Tieslietu ministrija, kas ir vadošā iestāde tieslietu jomā, sākotnēji sniedza vienu skaidrojumu par saglabājamo datu nodošanas procedūru, bet vēlāk – pilnīgi pretēju skaidrojumu.7

Ņemot vērā iepriekš minēto, secinu, ka šobrīd ierobežojums nav noteikts pietiekami skaidri un precīzi, tāpēc nevar atzīt, ka ierobežojums ir noteikts ar likumu. Tā kā ierobežojums nav noteikts ar likumu, tas nav arī atbilstošs Latvijas Republikas Satversmei un Eiropas Cilvēktiesību konvencijai. Lai novērstu šo neatbilstību, būtu nepieciešams vai nu Kriminālprocesa likumā un Operatīvās darbības likumā tieši un nepārprotami noregulēt saglabājamo datu nodošanas procedūru, vai arī Elektronisko sakaru likumā ietvert atsauci uz konkrētiem Kriminālprocesa likuma un Operatīvās darbības likuma pantiem, tādējādi norādot uz piemērojamo procedūru.

Pat, ja pieņemtu, ka ierobežojums ir noteikts pietiekami skaidri un precīzi, tad, lai to atzītu par atbilstošu Latvijas Republikas Satversmei un Eiropas Cilvēktiesību konvencijai, tam ir jākalpo leģitīmam mērķim un jābūt nepieciešamam demokrātiskā sabiedrībā.

Ierobežojuma mērķis ir skaidrots Elektronisko sakaru likumā. 71.1panta pirmā daļa noteic, ka saglabājamie dati tiek saglabāti un nodoti attiecīgām iestādēm, lai aizsargātu valsts un sabiedrisko drošību vai nodrošinātu noziedzīgu nodarījumu izmeklēšanu, kriminālvajāšanu un kriminālllietu iztiesāšanu. Tātad ierobežojums ir vērsts uz sabiedrības drošības aizsardzību, kas atbilstoši Latvijas Republikas Satversmes 116.pantam ir atzīstams par leģitīmu mērķi.

Izvērtējot to, vai ierobežojums ir nepieciešams demokrātiskā sabiedrībā, ir jāvērtē vai ierobežojums ir sociāli nepieciešams un samērīgs. Pieņemu, ka saglabājamo datu nodošanu iestādēm likumā paredzētajiem mērķiem var uzskatīt par sociāli nepieciešamu. Vērtējot ierobežojumu samērīgumu, ir jāņem vērā tas, ka iejaukšanās personas tiesībās uz privātās dzīves un korespondences neaizskaramību, nododot iestādēm saglabājamos datus bez personas piekrišanas, ir būtisks personas pamattiesību ierobežojums. Saglabājamie dati ļauj precīzi konstatēt personas saziņas paradumus un iegūt arī informāciju par personas attiecībām ar citām personām. Atrašanās vietas dati ļauj noteikt arī personas pārvietošanos noteiktā laikā un līdz ar to arī sadzīves paradumus. Turklāt saglabājamo datu nodošana iestādēm skar ne tikai

konkrēto personu, kas varētu būt izdarījusi noziedzīgu nodarījumu, bet gan visai plašu personu loku. Nododot iestādēm konkrētas personas saglabājamos datus, vienlaikus iestādes iegūst arī informāciju par citām personām, ar kurām šī konkrētā persona ir sazinājusies. Un tās var būt arī personas, kam nav nekādas saistības ar noziedzīgo nodarījumu. Tāpat uz ierobežojuma būtiskumu norāda arī tas, ka personas par datu nodošanu parasti uzzina tikai tad, kad tā jau ir notikusi, vai arī vispār neuzzina. Līdz ar to arī aizsardzības iespējas nepamatotas iejaukšanās gadījumā ir visai ierobežotas un parasti vairs nav iespējams pilnībā novērst iejaukšanās rezultātā radītās sekas.8

Lai šādu būtisku pamattiesību ierobežojumu atzītu par samērīgu, ir jānodrošina, ka tas tiek izmantots tikai tad, kad sabiedrības drošība ir pietiekami nopietni apdraudēta. Tāpat samērīgums prasa, lai pastāvētu mehānismi pret saglabājamo datu patvaļīgu izmantošanu. To var nodrošināt, ja pastāv pienācīga kontrole pār saglabājamo datu nodošanu iestādēm.

Lai noteiktu, kādi kontroles mehānismi ir nepieciešami, ir jāizvērtē attiecīgā pasākuma raksturs. Elektronisko sakaru likuma 71.1pants paredz saglabājamo datu nodošanu bez attiecīgās personas piekrišanas. Šā panta sestajā daļā pat īpaši uzsvērts, ka elektronisko sakaru komersantam nav tiesību izpaust informāciju par faktu, ka saglabājamie dati pieprasīti vai nodoti šā panta pirmajā daļā minētajām institūcijām, kā arī informāciju par lietotājiem vai abonentiem, attiecībā uz kuriem saglabājamie dati pieprasīti vai nodoti. Tas nozīmē, ka saglabājamo datu nodošana ir slepens pasākums attiecībā pret konkrēto personu. Kā vairākos spriedumos ir norādījusi Eiropas Cilvēktiesību tiesa, tad dažādi slepeni pasākumi var būt nepieciešami, lai aizsargātu valsts un sabiedrības drošību, tādējādi aizsargājot arī demokrātiju. Taču pastāv risks, ka šie slepenie pasākumi tiek izmantoti tā, ka, atsaucoties uz nepieciešamību aizsargāt demokrātiju, tie patiesībā grauj vai pat iznīcina to. Tāpēc valstu rīcības brīvība, ieviešot slepenus pasākumus, nav absolūta un ir jābūt mehānismiem, kas mazinātu slepeno pasākumu nepareizas vai patvaļīgas izmantošanas risku.9

Dažādu slepenu pasākumu izmantošanu pret indivīdu var izvērtēt trīs šo pasākumu stadijās – uzsākot, veikšanas laikā un pēc pabeigšanas. Ja pasākums ir slepens, tad loģiski ir tas, ka persona par to netiek informēta, uzsākot šo slepeno pasākumu, vai pasākuma veikšanas laikā. Ja persona nav informēta par pasākumu, tad tā nevar arī pati izmantot nekādus aizsardzības līdzekļus. Tāpēc šādās situācijās ir jānodrošina tādas procedūras slepenu pasākumu uzsākšanai un veikšanai, kas nodrošinātu pienācīgu un atbilstošu indivīda tiesību aizsardzību. To prasa arī tiesiskuma princips. No tiesiskuma principa izriet prasība, lai iejaukšanās personas tiesībās tiktu pakļauta efektīvai kontrolei, ko parasti vismaz pēdējā līmenī veic tiesas, jo tiesu kontrole nodrošina vislabākās neatkarības, objektivitātes un taisnīgu procedūru garantijas.10 Arī Eiropas Savienības datu aizsardzības uzraugs ir norādījis, ka tiesībsargājošo iestāžu pieeja personas datiem ir pieļaujama tikai, pieprasot informāciju par konkrētu gadījumu, skaidri definētos apstākļos un skaidri definētiem mērķiem, un šādos gadījumos ir jānodrošina arī tiesas kontrole.11 Savukārt Lietuvas Republikas konstitūcijas 22.pantā ir tieši noteikts, ka personas datu pieprasīšanai ir nepieciešama tiesas atļauja.

Vācijas Federālā konstitucionālā tiesa ir atzinusi, ka tiesas atļauja datu nodošanai ir vislabākais mehānisms personas tiesību uz korespondences neaizskaramību

aizsardzībai. Lai nodrošinātu samērīgumu, tiesnesim patstāvīgi ir jāizvērtē visi konkrētās lietas apstākļi. Nav pieļaujama tikai formāla attiecīgās amatpersonas lūgumu izvērtēšana, dodot piekrišanu datu nodošanai.12
Tas nozīmē, lai saglabājamo datu nodošanu pirmstiesas izmeklēšanas iestādēm, operatīvās darbības subjektiem, valsts drošības iestādēm, prokuratūrai un tiesai atzītu par nepieciešamu demokrātiskā sabiedrībā, pār to ir jānodrošina tiesas kontrole.

Izvērtējot Elektronisko sakaru likuma 71.1pantā paredzēto saglabājamo datu nodošanu, ir jākonstatē, ka Elektronisko sakaru likums neregulē jautājumu par tiesas atļaujas nepieciešamību datu nodošanai. Taču Kriminālprocesa likuma 192.pants paredz: „Procesa virzītājs, pamatojoties uz izmeklēšanas tiesneša lēmumu vai ar datu subjekta piekrišanu var pieprasīt, lai elektroniskās informācijas sistēmas īpašnieks vai likumīgais valdītājs atklāj informācijas sistēmā saglabātos datus.” Manuprāt, šīs normas formulējums liek domāt, ka tā attiecas uz saglabājamiem datiem. Arī viens no šīs normas izstrādātājiem tiesību zinātņu doktors Uldis Ķinis norādījis, ka šo normu bija paredzēts attiecināt arī uz tādu datu nodošanu kā saglabājamie dati.13 Savukārt Operatīvās darbības likuma 7.panta ceturtā daļa paredz, ka operatīvā informācijas iegūšana no tehniskajiem līdzekļiem veicama tikai sevišķā veidā un ar Augstākās tiesas priekšsēdētāja vai viņa īpaši pilnvarota Augstākās tiesas tiesneša akceptu. Uzskatu, ka šo normu var interpretēt tādā veidā, ka tā attiecas arī uz saglabājamo datu nodošanu. To apstiprina arī Tieslietu ministrija un Ģenerālprokuratūra.14

Taču praksē šīs normas netiek piemērotas, pieprasot saglabājamos datus. Iestādes šobrīd saglabājamos datus pieprasa saskaņā ar Kriminālprocesa likuma 190.pantu un Operatīvās darbības likuma 9.pantu. Šie panti regulē attiecīgi dokumentu pieprasīšanu kriminālprocesā un operatīvo izzināšanu un atbilstoši tiem tiesas atļauja nav nepieciešama. Tieslietu ministrija un Ģenerālprokuratūra skaidro, ka Kriminālprocesa likuma 192.pants ir jāinterpretē saistībā ar 191.pantu. Tāpēc 192.pantā paredzētais attiecoties tikai uz 191.panta kārtībā saglabātajiem datiem. Savukārt Operatīvās darbības likuma 7.panta ceturtā daļa atbilstoši Tieslietu ministrijas skaidrojumam attiecoties tikai uz personas paustās informācijas saturu.15 Tāpat attiecīgās iestādes norāda, ka tiesas atļaujas nepieciešamība liegtu izmantot šos datus gadījumos, kad jārīkojas nekavējoties, lai novērstu draudus personu dzīvībai, terorisma draudus u.tml.

Šādam skaidrojumam nevar piekrist. Vēlos uzsvērt, ka tiesiskā valstī normatīvajos aktos ietvertās tiesību normas ir jāinterpretē pēc iespējas atbilstoši konstitūcijai. Kā jau norādīju, tad no Latvijas Republikas Satversmes izriet prasība pēc tiesas atļaujas saglabājamo datu nodošanas gadījumā. Ne Kriminālprocesa likuma 192.panta, ne Operatīvās darbības likuma 7.panta ceturtās daļas vārdiskā jēga neizslēdz šādu interpretāciju. Tāpēc šīs normas būtu jāinterpretē tā, ka tās attiecas uz Elektronisko sakaru likuma 71.1pantā paredzēto saglabājamo datu nodošanu. Nav pieļaujama arī tāda interpretācija, ka Elektronisko sakaru likumā Ministru kabinets ir pilnvarots noteikt atšķirīgu kārtību. Ministru kabineta noteikumos var regulēt tikai saglabājamo datu pieprasīšanas un nodošanas tehnisko kārtību, un šie noteikumi nedrīkst būt pretrunā ar Kriminālprocesa likumu un Operatīvās darbības likumu.

Kas attiecas uz gadījumiem, kad jārīkojas nekavējoties, tad vēlos vērst uzmanību uz šādiem apstākļiem. Pirmkārt, vēlos norādīt, ka šajā atzinumā ietvertās prasības neattiecas uz Elektronisko sakaru likuma 71.panta septītajā daļā ietvertajām glābšanas dienestu tiesībām pieprasīt atrašanās vietas datus. Šajā gadījumā nav runa par datu

nodošanu kā slepenu pasākumu, turklāt personai pašai nemaz nav iespējams dot piekrišanu datu nodošanai. Atbilstoši personas datu aizsardzības principiem, kas ietverti gan Fizisko personu datu aizsardzības likumā, gan dažādos starptautiskos dokumentos, datu apstrāde bez personas piekrišanas ir pieļaujama, ja tā nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, arī dzīvību un veselību.16 Tāpēc atrašanās vietas datu nodošanai glābšanas dienestiem nav jāsaņem tiesas atļauja.

Otrkārt, runājot par pazudušu bērnu meklēšanu, attiecīgajām iestādēm nevajadzētu aizmirst, ka vecākiem kā bērna likumiskajiem pārstāvjiem un bērna aizbildņiem ir tiesības bērna vietā dot piekrišanu saglabājamo datu nodošanai. Ja ir saņemta piekrišana, tad nenotiek iejaukšanās personas tiesībās uz privātās dzīves un korespondences neaizskaramību, tāpēc tiesas atļauja nav nepieciešama.
Treškārt, ir jānorāda, ka likumos ir iespējams paredzēt arī tādu kārtību, kad neatliekamos gadījumos iestādes ir tiesīgas pieprasīt saglabājamos datus, bet tiesas kontrole pār šo pieprasījumu notiek dažu dienu laikā pēc datu pieprasīšanas. Tāda kārtība jau ir paredzēta Operatīvās darbības likuma 7.panta piektajā daļā: „Gadījumos, kad jārīkojas nekavējoties, lai novērstu terorismu, slepkavību, bandītismu, masu nekārtības, citu smagu vai sevišķi smagu noziegumu, kā arī tad, kad reāli ir apdraudēta personas dzīvība, veselība vai īpašums, šā panta ceturtajā daļā minētos operatīvās darbības pasākumus var veikt bez tiesneša akcepta. Par to 24 stundu laikā jāpaziņo prokuroram un 72 stundu laikā jāsaņem tiesneša akcepts. Pretējā gadījumā operatīvās darbības pasākumu veikšana ir jāpārtrauc.” Šādu izņēmuma kārtību būtu iespējams ietvert arī Kriminālprocesa likumā.

Ņemot vērā iepriekš minēto, uzskatu, ka Elektronisko sakaru likuma 71.1pantā paredzētajai saglabājamo datu nodošanai ir jāsaņem tiesas atļauja. Tāpēc aicinu šobrīd Kriminālprocesa likuma 192.pantu un Operatīvās darbības likuma 7.panta ceturto daļu interpretēt atbilstoši Latvijas Republikas Satversmei un piemērot šīs normas saglabājamo datu nodošanai.

Taču, ņemot vērā pastāvošo praksi un asās diskusijas par šo jautājumu, manuprāt, ir pamats uzskatīt, ka normatīvajos aktos šis jautājums tomēr nav noregulēts pietiekami skaidri. Tāpēc būtu nepieciešams izdarīt grozījumus likumos, tieši un precīzi nosakot, ka saglabājamo datu nodošanai ir nepieciešams saņemt tiesas atļauju. Lai to nodrošinātu, tad būtu nepieciešams, piemēram, Kriminālprocesa likuma 191.pantu papildināt ar jaunu trešo daļu, kas paredzētu, ka datu saglabāšanas pienākumu var noteikt arī ar likumu. Savukārt Kriminālprocesa likuma 192.pantu varētu grozīt, nosakot, ka procesa virzītājs, pamatojoties uz izmeklēšanas tiesneša lēmumu vai ar datu subjekta piekrišanu, var pieprasīt atklāt datus, kas informācijas sistēmā saglabāti saskaņā ar procesa virzītāja lēmumu vai saskaņā ar Elektronisko sakaru likuma 19.panta pirmās daļas 11.punktu. Savukārt Operatīvās darbības likumā varētu, piemēram, papildināt 17.panta 2.punktā ietverto skaidrojumu par operatīvās informācijas iegūšanu no tehniskajiem līdzekļiem, norādot, ka tā ietver arī saglabājamo datu nodošanu. Uzskatu, ka arī Elektronisko sakaru likuma 71.1panta trešajā daļā varētu ietvert atsauci uz Kriminālprocesa likuma 192.pantu un Operatīvās darbības likuma 7.panta ceturto daļu. Tādējādi tiktu nodrošināta saglabājamo datu nodošanas regulējuma atbilstība Latvijas Republikas Satversmei, tiesiskuma ievērošana un demokrātiskai iekārtai atbilstoša cīņa ar valsts un sabiedrības drošības apdraudējumiem.

1. Vācijas Federālās konstitucionālās tiesas 1999.gada 14.jūlija spriedums lietā 1 BvR 2226/94, 2003.gada 12.marta spriedums lietā 1 BvR 330/96. http://www.bverfg.de/entscheidungen.html

2. Eiropas Cilvēktiesību tiesas 1984.gada 2.augusta spriedums lietā Malone v. The United Kingdom, para.84

3. Explanatory Memorandum. Recommendation No.R (95) 4 of the Committee of Ministers to Member States on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, para. 53. http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/ international_legal_instruments/EM_R(95)4_EN.pdf

4. Skatīt, piemēram, Vācijas Federālās konstitucionālās tiesas 1999.gada 14.jūlija spriedums lietā 1 BvR 2226/94, 2003.gada 12.marta spriedums lietā 1 BvR 330/96, 2005.gada 27.jūlija spriedumu lietā 1 BvR 668/04. http://www.bverfg.de/entscheidungen.html

5. Skatīt, piemēram, Eiropas Cilvēktiesību tiesas 2006.gada 8.jūnija spriedumu lietā Lupsa v.Romania, para. 32., 1987.gada 26.marta spriedumu lietā Leander v. Sweden, para. 50 u.c.

6. Eiropas Cilvēktiesību tiesas 2000.gada 4.maija spriedums lietā Rotaru v.Romania, paras. 55-57; 1987.gada 26.marta spriedums lietā Leander v. Sweden, paras. 55-56. u.c.

7. Tieslietu ministrija 2007.gada 20.jūnija vēstulē Nr.1-7.5.5/2668 norādīja, ka uz sagalabājamo datu nodošanu ir attiecināma Kriminālprocesa likuma 192.pantā un Operatīvās darbības likuma 7.panta trešajā daļā paredzētā procedūra un ir nepieciešama tiesas atļauja. Savukārt 2007.gada 17.jūlija vēstulē Nr.1-7.1/3050 Tieslietu ministrija kopā ar Ģenerālprokuratūru skaidro, ka tiesas atļauja nav nepieciešama.

8. Vācijas Federālās konstitucionālās tiesas 2005.gada 27.jūlija spriedums lietā 1 BvR 668/04, paras. 137-143, kā arī 2003.gada 12.marta spriedums lietā 1 BvR 330/96, paras. 70-74. http://www.bverfg.de/entscheidungen.html

9. Eiropas Cilvēktiesību tiesas 1978.gada 6.septembra spriedums lietā Klass and others v. Germany, paras. 48-50, 2006.gada 2.novembra spriedums lietā Volokhy v. Ukraine, para. 52, 2000.gada 4.maija spriedums lietā Rotaru v.Romania, para. 59 u.c.

10. Eiropas Cilvēktiesību tiesas 1978.gada 6.septembra spriedums lietā Klass and others v. Germany, para.55., 2006.gada 2.novembra spriedums lietā Volokhy v. Ukraine, para. 52, 2000.gada 4.maija spriedums lietā Rotaru v.Romania, para. 59 u.c.

11. Third opinion of 27 April 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, para. 35.

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-04-27_3dpillar_3_EN.pdf

12. Vācijas Federālās konstitucionālās tiesas 2003.gada 12.marta spriedums lietā 1 BvR 330/96, paras. 87-88. http://www.bverfg.de/entscheidungen.html

13 Ķinis U. Datordati Krimināprocesā: tiesiskās problēmas. Jurista Vārds, 2006.gada 6.jūnijs, Nr.22

14. Tieslietu ministrijas 2007.gada 17.jūlija vēstule Nr.1-7.1/3050

15. Ģenerālprokuratūras 2007.gada 23.jūlija vēstule Nr.8/4-776-07, Tieslietu ministrijas 2007.gada 17.jūlija vēstule Nr.1-7.1/3050

16. Fizisko personu datu aizsardzības likuma 7.panta 4.punkts, Eiropas Padomes Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi 9.pants u.c