Pierādījumu iegūšanas tiesiskie pamatprincipi informācijas tehnoloģiju noziegumu lietās

Uldis Miķelsons

Skatot jautājumu par informācijas tehnoloģiju noziegumu izmeklēšanas tehniskajām iespējām, jāizvērtē arī tiesiskie pamatprincipi izmeklēšanas darbību veikšanai un pierādījumu iegūšanai informācijas tehnoloģiju (IT) noziegumu lietās, ievērojot, ka 2005. gada 1. oktobrī stājies spēkā Kriminālprocesa likums (KPL), kas ievieš vairākas būtiskas izmaiņas izmeklēšanas procesuālajā kārtībā, kuras būtiski iespaido arī IT jomā veikto noziedzīgo nodarījumu izmeklēšanas tehniskās iespējas.

Saskaņā ar noziegumu izmeklēšanas metodikas pamatlikumsakarībām,[1] tehniskie izmeklēšanas aspekti jāpakārto juridiskajiem aspektiem, jo normatīvās reglamentācijas pārkāpumi nav pieļaujami. Īpaši svarīgi tas ir IT noziegumu[2] lietās, kur pastāv ļoti daudzveidīgas tehniskās iespējas iegūt izmeklējamai lietai būtisku informāciju, kas tiek apstrādāta, uzglabāta vai pārraidīta elektroniskā formā, vienlaikus nozīmīgi saskaroties ar fizisko vai juridisko personu tiesību un interešu aizskāruma iespēju. Piemēram, IT noziegumu lietās dažkārt jāiegūst informācija, kas tiek pārsūtīta datortīklā ar elektroniskā pasta vai cita servisa starpniecību, taču šādas informācijas noslēpums ir juridiski aizsargāts ar Latvijas Republikas Satversmē iekļautajām cilvēktiesību normām, kā arī Krimināllikumu. Tāpēc rūpīgi jāizvērtē juridiskie nosacījumi šādas informācijas ieguvei un tikai atbilstīgi tiem var būt ieteikts tāds vai citāds tehniskais risinājums.

Šā jautājuma izvērtēšana patlaban ir īpaši aktuāla, ievērojot to, cik strauji un daudzveidīgi mūsdienās attīstās IT joma un tās izmantošana visdažākajiem mērķiem visās sabiedrības grupās gan publiskā, gan privātā jomā, turklāt globālā mērogā. Var piebilst, ka jauna Kriminālprocesa likuma izstrādes nepieciešamību noteica arī tas, ka rūpīgi jāreglamentē gan cilvēktiesību ievērošanas nosacījumus kriminālprocesā, gan starptautiskās tiesiskās sadarbības jautājumus, uz ko arī norādīja ārvalstu eksperti.

Lai šos un ar tiem saistītus jautājumus risinātu starptautiskā mērogā, vairākas starptautiskas organizācijas regulāri organizē darba grupas un konferences, tajā skaitā pat

---

[1] Par to sk., piemēram: Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas metodika. – Rīga: Biznesa augstskola Turība, 2003. – 387 lpp.

[2] Šeit lietots termins «IT noziegumi», ar to apzīmējot noziedzīgus nodarījumus informācijas tehnoloģiju jomā. Saskaņā ar Krimināllikuma nosacījumiem daļa no šiem nodarījumiem ir kriminālpārkāpumi, nevis mazāk smagi, smagi vai sevišķi smagi noziegumi. Tomēr satura vieglākai uzteverei šeit lietderīgi lietot īsāku apzīmējumu. Juridiskajā praksē jau jāveic precīza nodarījuma kvalifikācija atbilstīgi Krimināllikuma attiecīgajā pantā norādītajai sankcijai.

Apvienoto Nāciju organizācija organizē sammitus, lai apspriestu jautājumus par Internet tiesisko regulējumu, kā arī ir pieņēmusi īpašu rezolūciju IT noziegumu apkarošanas jomā.[3]

Viens no nozīmīgākajiem starptautiskajiem dokumentiem šajā jomā ir arī Eiropas Padomes (EP) 2001. gada 23. novembrī pieņemtā Kibernoziegumu konvencija,[4] kas stājās spēkā 2004. gada 1. jūlijā. Patlaban[5] to parakstījušas 42 valstis, tajā skaitā arī Latvija 2004. gada 5. maijā, kā arī četras valstis, kas nav Eiropas Padomē – Japāna, Kanāda, ASV un Dienvidāfrikas Republika, taču to ratificējušas tikai 11 valstis.[6]

Latvija patlaban vēl nav ratificējusi šo konvenciju, tomēr ir paredzējusi to darīt (kaut gan nav pieņēmusi nekādu oficiālu deklarāciju sakarā ar to). Kriminālprocesa likumā tā izstrādes gaitā tika iekļautas arī vairākas normas, kas izrietēja no Kibernoziegumu konvencijas. Līdz ar to Latvijā nav objektīvu šķēršļu, lai ratificētu šo konvenciju, tāpēc, saskaņā ar autora viedokli, tās neratificēšanu var uzskatīt arī par likumdevēja neizdarību.

Ievērojot starptautisko normatīvo aktu un rekomendāciju ieteikumus, Kriminālprocesa likumā[7] jau 1. pantā uzsvērts, ka kriminālprocesa mērķis ir noteikt tādu kārtību noziedzīgu nodarījumu izmeklēšanai, kriminālvajāšanai un iztiesāšanai, kas nodrošina efektīvu Krimināllikuma normu piemērošanu un kriminālatiesisko attiecību taisnīgu noregulējumu bez neattaisnotas iejaukšanās personas dzīvē. Tas pilnībā attiecās arī uz IT noziegumu izmeklēšanu, kas nereti saistīta ar korespondences noslēpuma un privātās dzīves neaizskaramības principu aizskārumu.

Latvijas Republikas Satversmes[8] 96. un 100. panti nosaka ikvienas personas tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību, kā arī tiesības uz vārda brīvību, kas ietver tiesības brīvi iegūt, paturēt un izplatīt informāciju, paust savus uzskatus.

Arī Krimināllikumā[9] iekļauta norma, kas paredz kriminālatbildību par šāda veida pārkāpumu, proti 144. pantā noteikta atbildība par korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšanu:

«(1) Par personas korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas noslēpuma tīšu pārkāpšanu, kā arī par tādas informācijas un programmu noslēpuma tīšu

---

3 United Nations General Assembly Resolution 55-63: Combating the Criminal Misuse of Information Technologies. A/RES/55/63; Adopted by the General Assembly on 4 December, 2000.

4 Convention on Cybercrime / European Committee on Crime Problems; Committee of Experts on Crime in Cyberspace. – Budapest, 29 November, 2001.

5 Stāvoklis 2005. gada 8. oktobrī.

6 Albānija, Bulgārija, Dānija, Horvātija, Igaunija, Kipra, Lietuva, Maķedonija, Rumānija, Slovēnija, Ungārija.

7 Kriminālprocesa likums / Latvijas Republikas likums. Pieņemts Saeimā 21.04.2005.; spēkā no 01.10.2005.; publicēts Latvijas Vēstnesī 11.05.2005., Nr.74.

8 Latvijas Republikas Satversme / Latvijas Republikas pamatlikums. Pieņemta Latvijas Republikas Satversmes sapulcē 15.02.1922; spēkā no 07.11.1922.; redakcija uz 7.10.2004.; publicēta Latvijas Vēstnesī 01.07.1993., Nr.43.

9 Krimināllikums / Latvijas Republikas likums. Pieņemts Saeimā 17.06.1998.; spēkā no 1.04.1999.; redakcija uz 28.12.2004.; publicēts Latvijas Vēstnesī 08.07.1998., Nr.199/200.

pārkāpšanu, kas paredzētas lietošanai sakarā ar datu elektronisko apstrādi, soda ar brīvības atņemšanu uz laiku līdz trim gadiem vai ar piespiedu darbu, vai ar naudas sodu līdz piecdesmit minimālajām mēnešalgām, atņemot tiesības uz zināmu nodarbošanos uz laiku līdz pieciem gadiem vai bez tā.

(2) Par tādām pašām darbībām, ja tās izdarītas mantkārīgā nolūkā, soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar piespiedu darbu, vai ar naudas sodu līdz simt minimālajām mēnešalgām, atņemot tiesības uz zināmu nodarbošanos uz laiku līdz pieciem gadiem vai bez tā.»

Krimināllikumā noteikta krimināltbildība arī par cita veida darbībām, kādas var būt veiktas arī IT noziegumu izmeklēšanas gaitā, ja netiek ievērota likumā noteiktā kārtība.

Lai nodrošinātu tiesību aizsardzības iestāžu darba efektivitāti, līdz ar to nodrošinātu arī personu un sabiedrības interešu aizsardzības iespējas pret noziedzīgiem apdraudējumiem, cilvēktiesību principi paredz iespēju arī ierobežot cilvēktiesību aizsardzību, ja tas noteiktos apstākļos vajadzīgs būtisku mērķu īstenošanai. Šāda iespēja relamentēta arī nacionālajās tiesību normās, tajā skaitā Latvijas Republikas Satversmes 116. pants nosaka:

«Personas tiesības, kas noteiktas Satversmes deviņdesmit sestajā, deviņdesmit septītajā, deviņdesmit astotajā, simtajā, simt otrajā, simt trešajā, simt sestajā un simt astotajā pantā, var ierobežot likumā paredzētajos gadījumos, lai aizsargātu citu cilvēku tiesības, demokrātisko valsts iekārtu, sabiedrības drošību, labklājību un tikumību. Uz šajā pantā minēto nosacījumu pamata var ierobežot arī reliģiskās pārliecības paušanu.»

Atbilstīgi arī Kriminālprocesa likuma 12. pantā cilvēktiesību garantēšana jau sīkāk reglamentēta, tajā skaitā arī samērīguma princips, veicot izmeklēšanas darbības:

«(1) Kriminālprocesu veic, ievērojot starptautiski atzītās cilvēktiesības un nepieļaujot neattaisnotu krimināprocesuālo pienākumu uzlikšanu vai nesamērīgu iejaukšanos personas dzīvē.

(2) Cilvēktiesības var ierobežot tikai tajos gadījumos, kad to prasa sabiedrības drošības apsvērumi, un tikai šajā likumā noteiktajā kārtībā atbilstoši noziedzīgā nodarījuma raksturam un bīstamībai. […]

(4) Procesa virzītāja, īpaši pilnvarotā prokurora un izmeklēšanas tiesneša pienākums ir aizsargāt personas privātās dzīves noslēpumu un komercnoslēpumu. Ziņas par to drīkst iegūt un izmantot tikai tad, ja tas ir nepieciešams pierādāmo apstākļu noskaidrošanai.

(5) Fiziskajai personai ir tiesības pieprasīt, lai krimināllietā netiek iekļautas ziņas par šīs personas pašas vai tās saderinātā, laulātā, vecāku, vecvecāku, bērnu, mazbērnu, brāļu un māsu (turpmāk – tuvi radinieki) privāto dzīvi, komercdarbību un mantisko stāvokli, ja tas nav nepieciešams krimināltiesisko attiecību taisnīgai noregulēšanai.»

Nav gan pareizi domāt, ka līdz Kriminālprocesa likuma pieņemšanai, kriminālprocesā nebija garantēta cilvēktiesību aizsardzība. Latvijas Kriminālprocesa kodeksā tas vienkārši nebija tik detalizēti reglamentēts, tomēr nebija arī būtisku trūkumu. Piemēram, Latvijas Kriminālprocesa kodeksa[10] 176.[1] pants, kas reglamentēja telefonsarunu noklausīšanos un informācijas iegūšanu no tehniskajiem līdzekļiem (šo darbību gaitā, ja tās veic slēpti, tiek aizskartas cilvēktiesības), pieļāva šādas darbības veikšanu attiecībā uz aizdomās turētajiem un apsūdzētajiem vienīgi pamatojoties uz tiesas vai tiesneša lēmumu konkrētajā krimināllietā par noziegumiem, ja ir pietiekams pamats uzskatīt, ka sarunu noklausīšanās vai informācijas iegūšana no tehniskajiem līdzekļiem var sniegt ziņas, kam ir būtiska nozīme lietā, turklāt ne ilgāk par sešiem mēnešiem. Bez tiesas vai tiesneša lēmuma bija pieļauts veikt šādas darbības vienīgi attiecībā uz cietušo, liecinieku vai citām personām, kuras piedalās lietā, ja pret šo personu ir izteikti draudi pielietot vardarbību, izspiešanu vai izdarīt citas pretlikumīgas darbības, pēc šo personu iesnieguma un ar viņu piekrišanu.

Vēl jānorāda, ka arī Operatīvās darbības likumā[11] (ODL), tā 1. un 4. pantā noteikta cilvēktiesību aizsardzība, kas attiecās arī uz ODL 6. panta (1) daļas 10) punktā paredzēto un 17. pantā reglamentēto operatīvās darbības pasākumu – operatīvā informācijas iegūšanu no tehniskajiem līdzekļiem, proti: «informācijas noņemšana vai kopēšana no personu īpašumā vai rīcībā esošajām elektroniskajām un cita veida informācijas glabāšanas ierīcēm un informācijas kanāliem», kā arī operatīvā operatīvo korespondences kontroli un operatīvo sarunu noklausīšanos, kas arī var būt veiktas, lietojot elektroniskas informācijas sistēmas. Šos pasākumus, saskaņā ar ODL 7. panta nosacījumiem, pieļauts veikt tikai sevišķajā veidā:

«(3) Operatīvās darbības pasākumi, kuru gaitā tiek būtiski aizskartas personu konstitucionālās tiesības, veicami sevišķajā veidā.

(4) Operatīvā korespondences kontrole, operatīvā informācijas iegūšana no tehniskajiem līdzekļiem, operatīvā nepublisku sarunu slepena noklausīšanās (arī pa tālruni, ar elektroniskajiem un cita veida sakaru līdzekļiem) un operatīvā iekļūšana veicama tikai sevišķajā veidā un ar Augstākās tiesas priekšsēdētāja vai viņa īpaši pilnvarota Augstākās tiesas tiesneša akceptu. Atļauju veikt šos operatīvās darbības pasākumus var izsniegt uz laiku līdz trim mēnešiem un pamatotas nepieciešamības gadījumā to var pagarināt, taču tikai uz to laiku, kamēr attiecībā uz personu tiek veikta operatīvā izstrāde.

(5) Gadījumos, kad jārīkojas nekavējoties, lai novērstu terorismu, slepkavību, bandītismu, masu nekārtības, citu smagu vai sevišķi smagu noziegumu, kā arī tad, kad reāli ir apdraudēta

[10] Latvijas Kriminālprocesa kodekss / Latvijas Republikas likums. Pieņemts Latvijas PSR Augstākajā padomē 06.01.1961.; spēkā no 01.04.1961.; Latvijas Republikā stājies spēkā ar Latvijas Republikas Augstākās Padomes likumu 23.10.1990. (Nav spēkā) un Latvijas Republikas likumu 22.08.1991. (Latvijas Republikas Augstākās Padomes un Valdības Ziņotājs, 1991., Nr.33./34.); redakcija uz 28.01.2005. – [Oficiāli nav publicēts; sk. NAIS]

[11] Operatīvās darbības likums / Latvijas Republikas likums. Pieņemts Saeimā 16.12.1993.; spēkā no 14.01.1994.; redakcija uz 10.07.2002.; publicēts Latvijas Vēstnesī 30.12.1993., Nr.131.

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.»

Atgriežoties pie kriminālprocesuālajiem aspektiem, jānorāda, ka Kriminālprocesa likuma 9. nodaļā, kur reglamentēti pierādīšanas un pierādījumu pamatjautājumi, iekļauti virkne nosacījumu, lai kriminālprocesā iegūtās ziņas varētu uzskatīt par ticamām, attiecinām un pieļaujamām un varētu būt izmantotas pierādīšanā.

Starp šiem nosacījumiem ir arī KPL 127. panta (3) daļā iekļautā norma, ka operatīvās darbības pasākumos iegūtās ziņas par faktiem, arī ziņas, kas fiksētas ar tehnisku līdzekļu palīdzību, drīkst izmantot kā pierādījumu, tomēr ar piebildi – tikai tad, ja tās iespējams pārbaudīt Kriminālprocesa likumā noteiktajā procesuālajā kārtībā.

Pierādījumu ticamību, attiecināmību un pieļaujamību nosaka KPL 128. – 130. pantos iekļautie nosacījumi:

«128.pants. Pierādījumu ticamība

(1) Pierādījuma ticamība ir kādas ziņas patiesuma konstatēšanas pakāpe.

(2) To, cik ticamas ir pierādīšanā izmantojamās ziņas par faktiem, izvērtē, aplūkojot visus kriminālprocesa laikā iegūtos faktus vai ziņas par faktiem kopumā un savstarpējā sakarībā.

(3) Nevienam no pierādījumiem nav iepriekš noteikta augstāka ticamības pakāpe nekā pārējiem pierādījumiem.»

Šeit var piebilst, ka nevienas izmeklēšanas darbības gaitā noskaidrotajai informācijai, kā arī datortehniskās ekspertīzes galarezultātā izdarītajiem secinājumiem nevar būt augstāka ticamības pakāpe, nekā, piemēram, personas liecībām, neraugoties uz to, ka nopratināmās personas nereti melo vai maldās par kaut kādiem apstākļiem un pat maina liecības izmeklēšanas gaitā – liecības ir visnenoturīgākais pierādījumu veids, kamēr ar mūsdienu tehniskām metodēm, lietojot profesionālu programmatūru, var būt konstatēti apstākļi saistībā ar elektroniskas informācijas uzglabāšanu, apstrādi vai pārsūtīšanu nevainojami precīzi. Jāņem vērā, ka mūsdienās ir arī dažādas tehniskas metodes, ar kurām var radīt maldinošu priekšstatu par kaut kādiem apstākļiem saistībā ar elektroniskas informācijas apstrādi, kaut vai, piemēram, e-pasta vēstules sūtīšana, lietojot anonīmos starpniekserverus vai citādi ieteikmējot tās rekvizītus, lai persona pēc saņemtās e-pasta galvenes (*header*) nevarētu konstatēt īsto tās sūtītāju. Kriminālprocesa princips, ka jebkādi juridiski nolēmumi var būt pieņemti, vienīgi balstoties uz visu lietas apstākļu izvērtēšanu to kopumā un savstarpējā sakarībā, nevis tikai uz vienu kaut kādu apstākli lietā, jāievēro vienmēr arī IT noziegumu lietās.

«129.pants. Pierādījumu attiecināmība

Pierādījumi ir attiecināmi uz konkrēto kriminālprocesu, ja ziņas par faktiem tieši vai netieši apstiprina kriminālprocesā pierādāmo apstākļu esamību vai neesamību, kā arī citu pierādījumu ticamību vai neticamību, izmantošanas iespējamību vai neiespējamību.»

Šeit var piebilst – šā norma nenozīmē, ka nevar rasties juridiskas sekas tādos gadījumos, ja, piemēram, juridiskās vai fiziskās personas datora patstāvīgās atmiņas iekārtā datortehniskās ekspertīzes gaitā konstatētas pazīmes, ka persona ir izplatījusi vīrusus vai bērnu pornogrāfiju vai arī publiski aicinājusi likvidēt Latvijas Republikas valstisko neatkarību vai veikusi citas Krimināllikumā aizliegtas darbības, ja konkrētās krimināllietas ietvaros tiek izmeklēta, piemēram, ar IT līdzekļiem veikta krāpšana vai autortiesību pārkāpums vai cits noziedzīga nodarījuma veids, kam nav nekāds sakars ar minētā veida informāciju. Šādā gadījumā konstatētie pierādījumi nevar būt attiecināmi uz konkrēto kriminālprocesu, taču uz tādu ziņu pamata jau tiks uzsākts cits kriminālprocess.

«130.pants. Pierādījumu pieļaujamība

(1) Kriminālprocesa laikā iegūtās ziņas par faktiem ir pieļaujams izmantot kā pierādījumus, ja tās iegūtas un procesuāli nostiprinātas šajā likumā noteiktajā kārtībā.

(2) Par nepieļaujamām un pierādīšanā neizmantojamām atzīstamas tādas ziņas par faktiem, kuras iegūtas:

1) izmantojot vardarbību, draudus, šantāžu, viltu vai spaidus;

2) procesuālajā darbībā, ko veikusi persona, kurai saskaņā ar šo likumu nebija tiesību to veikt;

3) pieļaujot šajā likumā īpaši norādītos pārkāpumus, kas liedz konkrētā pierādījuma izmantošanu;

4) pārkāpjot kriminālprocesa pamatprincipus.

(3) Ziņas par faktiem, kuras iegūtas, pieļaujot citus procesuālos pārkāpumus, uzskatāmas par ierobežoti pieļaujamām un var tikt izmantotas pierādīšanā tikai tādā gadījumā, ja pieļautie procesuālie pārkāpumi ir nebūtiski vai var tikt novērsti, tie nevarēja ietekmēt iegūto ziņu patiesumu vai ja to ticamību apstiprina pārējās procesā iegūtās ziņas.»

Saistībā ar šo normu ļoti būtiski ir turpmāk aplūkotie juridiskie apstākļi, kas attiecās uz elektroniskās informācijas sistēmās uzglabātas, apstrādātas un pārsūtītas informācijas ieguvi krimināllietas apstākļus noskaidrošanai, jo tādas informācijas ieguves gaitā var būt tik būtiski pārkāpti Kriminālprocesa likuma nosacījumi un pat kriminālprocesa pamatprincipi, ka iegūto informāciju nav pieļaujams izmantot pierādīšanā. Tas īpaši attiecās uz speciālajām izmeklēšanas darbībām, kas aizskar cilvēktiesības, tajā skaitā arī KPL 219. un 220. pantos paredzētās speciālās izmeklēšanas darbības elektroniskas informācijas ieguvei.

Saskaņā ar Kriminālprocesa nosacījumiem, pierādījumi konkrētā kriminālprocesā var būt iegūti ar dažādiem līdzekļiem, tajā skaitā – izmeklēšanas darbībām, tostarp speciālajām

izmeklēšanas darbībām, ekspertīzēm,[12] revīzijām, kompetentu institūciju atzinumiem, ar juridisko vai fizisko personu iesniegtiem dokumentiem, kā lietiskie pierādījumi un kā elektroniskie pierādījumi,[13] kā arī – jau minētais – no operatīvās darbības pasākumos iegūtām ziņām, kā arī ziņām, kas fiksētas ar tehnisku līdzekļu palīdzību. Saskaņā ar KPL 155. panta nosacījumiem pierādījumi var būt iegūti arī personu aptaujā, tajā skaitā tās galarezultātus fiksējot šo aptauju veikušā darbinieka ziņojumā vai arī audio vai video ierakstā. Par speciālajās izmeklēšanas darbībās konstatētajiem apstākļiem informācija var būt fiksēta gan protokolā, gan pārskatā (atbilstīgi KPL 216. panta normai). Saskaņā ar KPL 189. panta normu, pierādījumi var būt iegūti arī no priekšmetiem un dokumentiem, kurus pēc savas iniciatīvas var iesniegt ikviena persona, vai arī pēc procesa virzītāja rakstveida pieprasījuma – saskaņā ar KPL 190. panta normu.

Visu juridisko aspektu izskatīšana attiecībā uz pierādījumu ieguvi IT noziegumu lietās ir ļoti plašs jautājums, kas iziet ārpus šā raksta mērķim – tiesisko pamatprincipu izvērtēšana. Šeit lietderīgi izvērtēt vienīgi juridiskos pamataspektus, kas attiecās uz tām izmeklēšanas darbībām, kuras tiek veiktas tieši saistībā ar elektroniskiem resursiem.

Izmeklēšanas darbības Kriminālprocesa likumā iedalās divos pamatveidos – tās, kuru veikšana notiek tradicionālā kārtībā (KPL 10. nodaļa) un speciālās izmeklēšanas darbības[14] (KPL 11. nodaļa).

KPL 139. pantā reglamentēti tradicionālā kārtībā veicamo izmeklēšanas darbību vispārīgie noteikumi, tajā skaitā šādi:

«(1) Iepriekš plānojamas izmeklēšanas darbības parasti veic laikā no pulksten 8.00 līdz 20.00. Gadījumos, kad izmeklēšanas darbība nav atliekama, jo tas var novest pie būtisku pierādījumu zaudēšanas un apdraud kriminālprocesa mērķa sasniegšanu, to veic nekavējoties.

(2) Izmeklēšanas darbības sākumā tās veicējs informē konkrētajā procesā iesaistīto personu par tās tiesībām un pienākumiem, kā arī brīdina par atbildību par savu pienākumu nepildīšanu. […]

(4) Aizliegts izpaust ziņas par tās personas privāto dzīvi, kura piedalās izmeklēšanas darbībā, kā arī ziņas, kas satur profesionālu noslēpumu vai komercnoslēpumu, izņemot gadījumus, kad tas nepieciešams pierādīšanā.»

---

[12] Par datortehniskās ekspertīzes juridiskajiem un metodiskajiem aspektiem, sk.:
Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas metodika. – Rīga: Biznesa augstskola Turība, 2003. – 387 lpp.
Miķelsons U. Datortehniskā ekspertīze / Tiesu ekspertīze Latvijā: Rokasgrāmata; 4. izdevums / Autoru grupa profesora A. Kavaliera vadībā. – Rīga: LPA, 2001. – 18. – 21. lpp.

[13] Par to plašāk sk.: Miķelsons U. Elektronisko pierādījumu tiesiskie aspekti // Latvijas Vēstneša izdevums «Jurista vārds», 2004., Nr. 12., 13., 14.

[14] Par speciālajām izmeklēšanas darbībām plašāk sk.: Kavalieris A. prof., Dr.hab.iur. Speciālās izmeklēšanas darbības. – Rīga: RaKa, 2003. – 128 lpp.

No šiem nosacījumiem redzams, ka KPL 10. nodaļā reglamentētās darbības nevar būt veiktas slēpti no tās personas, tieši uz kuru attiecās šī darbība. Tas attiecās arī uz KPL 191. un 192. pantos reglamentētajām darbībām, kas tiek veiktas saistībā ar elektroniskām informācijas sistēmām:

«191.pants. Elektroniskās informācijas sistēmā esošo datu saglabāšana

(1) Procesa virzītājs ar savu lēmumu var uzdot elektroniskās informācijas sistēmas īpašniekam vai likumīgajam valdītājam (tas ir, personai, kura nodrošina personu sazināšanos ar informācijas sistēmas palīdzību vai kura šā pakalpojuma ietvaros pārstrādā vai uzkrāj datus) nekavējoties nodrošināt tā valdījumā vai kontrolē esošo noteiktu, izmeklēšanas vajadzībām nepieciešamu datu veseluma saglabāšanu neizmainītā stāvoklī un to nepieejamību citiem sistēmas lietotājiem.

(2) Datu saglabāšanas pienākumu var noteikt uz laiku līdz trīsdesmit dienām, bet šo termiņu, ja nepieciešams, vēl uz laiku līdz trīsdesmit dienām var pagarināt izmeklēšanas tiesnesis.

192.pants. Elektroniskajā informācijas sistēmā saglabāto datu atklāšana

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.»

Šādas darbības var būt veiktas, piemēram, attiecībā uz Internet pakalpojuma sniedzēju (tajā skaitā Internet mājaslapas uzglabāšanas jeb *web hostinga* pakalpojumu vai plaša informācijas sistēmas ārpakalpojuma spektra jeb *outsourcing* sniedzēju), publiskas datu bāzes uzturētāju u.tml. Tomēr būtiski ir tas, kādi tieši kritēriji atšķir minētās izmeklēšanas darbības no KPL 219. un 220. pantos reglamentētajām speciālajām izmeklēšanas darbībām:

«219.pants. Elektroniskajā informācijas sistēmā esošo datu kontrole

(1) Informācijas sistēmas (tās daļas), tajā uzkrāto datu, datu vides meklēšanu un piekļuvi tai, kā arī iegūšanu (turpmāk – informācijas sistēmas datu kontrole) bez šīs sistēmas vai datu īpašnieka, valdītāja vai turētāja ziņas kriminālprocesā veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka konkrētajā informācijas sistēmā esošā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem.

(2) Ja ir pamats uzskatīt, ka meklētie dati (informācija) tiek uzglabāti citā Latvijas teritorijā esošā sistēmā, kurai var piekļūt autorizēti, izmantojot izmeklēšanas tiesneša lēmumā minēto sistēmu, jauns lēmums nav nepieciešams.

(3) Izmeklēšanas darbības uzsākšanai procesa virzītājs var pieprasīt, lai persona, kura pārzina sistēmas funkcionēšanu vai veic ar datu apstrādi, uzglabāšanu vai pārraides nodrošināšanu saistītus pienākumus (turpmāk – sistēmas atbildīgais darbinieks), sniedz nepieciešamo informāciju, kā arī brīdina šo personu par izmeklēšanas noslēpuma neizpaušanu.

(4) Procesa virzītāja uzdevumā veicot informācijas sistēmas datu kontroli, sistēmas atbildīgā darbinieka pienākums ir pārņemt vai citādi nodrošināt sistēmu (tās daļu, datu uzkrāšanas vidi), izgatavot datu kopijas, saglabāt būtiskos uzglabātos datus nemainītus, nodrošināt sistēmā esošo informācijas resursu veselumu, padarīt kontrolējamos datus nepieejamus citiem lietotājiem vai aizliegt citu darbību veikšanu ar tiem.

220.pants. Pārraidīto datu satura kontrole

Tādu datu pārtveršanu, vākšanu un ierakstīšanu, kuri pārraidīti ar informācijas sistēmas palīdzību, izmantojot Latvijas teritorijā esošās sakaru ierīces (turpmāk – pārraidīto datu kontrole), bez šīs sistēmas īpašnieka, valdītāja vai turētāja ziņas veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka no datu pārraides iegūtā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem.»

Ievērojot vispārējos nosacījumus attiecībā uz speciālajām izmeklēšanas darbībām, kas reglamentēti KPL 210. – 216. pantos, jāapzinās, ka tās veic, ja kriminālprocesā pierādāmo apstākļu noskaidrošanai ziņas par faktiem nepieciešams iegūt, neinformējot kriminālprocesā iesaistītās personas un tās personas, kuras varētu šīs ziņas sniegt.

Taču rodas jautājums, vai KPL 191. un 192. pantos norādītās darbības var un vajag veikt, vienmēr informējot par to personu, kuras izveidoto informāciju uzglabā, apstrādā vai pārsūta tas pakalpojumu sniedzējs, pie kā vēršas procesa virzītājs, tas ir, «persona, kura nodrošina personu sazināšanos ar informācijas sistēmas palīdzību vai kura šā pakalpojuma ietvaros pārstrādā vai uzkrāj datus»? Proti – vai gadījumos, ja kriminālprocesa virzītājs vēršas, piemēram, pie Internet pakalpojumu sniedzēja (angl.: *Internet service provider* jeb «*provaidera*»), lai KPL 191. panta kārtībā uzdotu tam saglabāt datus, kurus ar *provaidera* servera starpniecību pārsūta noteikts tā klients, un pēc tam KPL 192. panta kārtībā uzdotu tam atklāt šos datus, kriminālprocesa virzītājam vajag tūlīt informēt par šo darbību arī atbilstīgo klientu, t.i. personu, kuras pārsūtītā informācija jāsaglabā un jāatklāj uz *provaidera* servera, un vai to vienmēr arī var izdarīt?

Atbilde šim jautājumam ir nešaubīga – saskaņā ar Kriminālprocesa likuma nosacījumiem vienmēr persona ir jāinformē par to, ka tās pārsūtītā informācija tiek saglabāta un atklāta, un ja šāda informēšana nav iespējama, tad KPL 191. un 192. pantu kārtībā šādu informācijas iegūšanu nedrīkst veikt! Tas ir tāpēc, ka jebkādas slēptas darbības ar personas izveidoto, apstrādāto un uz *provaidera* servera uzglabāto vai pārsūtīto informāciju aizskar cilvēktiesību normu aizsargāto korespondences neaizskaramību, un var veidot apstākļus, kādi paredzēti Krimināllikuma 144. panta dispozīcijā. Šādas darbības pieļaujams veikt tikai KPL 219. vai 220. pantu kārtībā – kā speciālās izmeklēšanas darbības!

Tas tomēr nenozīmē, ka Kriminālprocesa likuma 191. un 192. pantā norādītās izmeklēšanas darbības vispār nekad nevar veikt. Cilvēktiesības aizsargā vienīgi to

informāciju, kuru apzināti izveidojis cilvēks. Taču elektroniskās informācijas sistēmās tiek saglabāta un apstrādāta arī daudz tāda informācija, kuru cilvēks apzināti nav veidojis (tāpēc tā nav uzskatāma par korespondenci cilvēktiesību izpratnē), bet ko izveido programmatūra informācijas apstrādes procesā, tajā skaitā dati par savienojumiem datortīklā, to laiku, lietotajiem Internet protokoliem, pārraidīto datu formātu un apjomu u.tml. Šāda informācija Eiropas Padomes Kibernoziegumu konvencijas 16. un 17. pantos tiek saukta *traffic data* jeb tehniskie pārraides dati.

Tehnisko datu (*traffic data*) noslēpums vispārējos gadījumos juridiski nav reglamentēts, atšķirībā no cita veida informācijas – fizisko personu datiem (to aizsargā Fizisko personu datu aizsardzības likums) un korespondenci (to aizsargā cilvēktiesību akti, kā arī Satversmes 96. pants). Tehniskos datus arī nav iespējams turēt noslēpumā, jo tie paredzēti sekmīgai elektroniskās informācijas apstrādei un pārsūtīšanai datortīklā, tāpēc ar tiem patstāvīgi vairāk vai mazāk var iepazīties ikviens Internet pakalpojumu sniedzējs vai persona, kuras serveris tiek lietots datu pārraides laikā.

Tajā pašā laikā minēto tehnisko datu nozīme izmeklējamā krimināllietā var būt ļoti būtiska, jo atsevišķos gadījumos ar tiem var pierādīt personas veiktās darbības IT noziegumu īstenošanā Internet tīklā. Piemēram var aplūkot jau iepriekš iezīmēto situāciju, kad persona nosūtījusi citam cilvēkam e-pasta vēstuli ar draudiem izspiešanas nolūkā, pārsūtīšanu veicot ar vairāku starpniekserveru starpniecību, lai pēc e-pasta vēstules galvenē (*header*) esošās informācijas nevarētu atklāt, no kurienes šā vēstule nosūtīta. Pašu e-pasta vēstuli elektroniskā formā KPL 189. panta kārtībā kriminālprocesa virzītājam var iesniegt tās saņēmējs, lūdzot veikt izmeklēšanu šo draudu sakarā. Pēc tam kriminālprocesa virzītājs jau var vērsties pie Internet pakalpojumu sniedzēja, kurš nodrošina attiecīgajam vēstules saņēmējam šo pakalpojumu (sniedz Internet piekļuvi vai uztur publisku e-pasta serveri ar POP3 vai IMAP protokolu), lai tas serverī programmatūras izveidotajos žurnālu (*.log) failos nekavējoties saglabātu (KPL 191. panta kārtībā) un pēc tam atklātu kriminālprocesa virzītājam (KPL 192. panta kārtībā) tos datus, kas saistīti ar e-pasta servisa nodrošinājumu atbilstīgajam klientam noteiktā laika periodā. Šo tehnisko datu izpēte jau var dot iespēju noteikt nākamo serveri, ar kura starpniecību noticis attiecīgais e-pasta sūtījums, pie kura kriminālprocesa virzītājs var tieši tāpat vērsties, tādā veidā cenšoties noskaidrot sākotnējo avotu šim sūtījumam, lai konstatētu lietotāju, no kura datora nosūtīta šā draudu vēstule. Visā šo darbību veikšanas laikā netiek veiktas jebkādas darbības ar personas izveidoto informāciju, bet tikai ar tehniskajiem pārraides datiem, tāpēc cilvēktiesības ar šo darbību netiek aizskartas un nav vajadzības to veikt speciālās izmeklēšanas darbības kārtībā.

Savukārt KPL 219. un 220. pantos reglamentētās darbības jau attiecās uz tādas informācijas ieguvi, kuru radījusi persona apzināti. Tas aizskar cilvēktiesību principus, tāpēc

tādas darbības pieļauts veikt vienīgi ar izmeklēšanas tiesneša lēmumu un vienīgi izmeklējot smagus vai sevišķi smagus noziegumus (noziedzīgu nodarījumu klasifikācijas nosacījumi reglamentēti Krimināllikuma 7. pantā).

Šeit jānorāda uz vēl vienu speciālo izmeklēšanas darbību, kas reglamentēta KPL 218. pantā – sakaru līdzekļu kontroli:

«(1) Telefonu un citu sakaru līdzekļu kontroli bez sarunas dalībnieku vai informācijas nosūtītāja un saņēmēja ziņas veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka sarunas vai nodotā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem, un ja bez šīs darbības nepieciešamo ziņu iegūšana nav iespējama.

(2) Telefonu un citu sakaru līdzekļu kontroli ar sarunas dalībnieka, informācijas nosūtītāja vai saņēmēja rakstveida piekrišanu veic, ja ir pamats uzskatīt, ka pret šo personu vai tās tuviniekiem var tikt vērsts noziedzīgs nodarījums vai arī šī persona ir vai var tikt iesaistīta noziedzīga nodarījuma izdarīšanā.»

Mūsdienās strauji attīstās *Internet telefonijas* servisi, kad verbālas sarunas tiek veiktas ar Internet protokolu (galvenokārt VoIP vai XMPP) pielietošanu, jo tiek pat par brīvu plaši piedāvāta speciāla programmatūra tādiem mērķiem, tajā skaitā *ICQ, Skype, Google Talk* u.c., kuras lietošana ļauj būtiski ietaupīt finanšu resursus, īpaši ja saruna notiek ar personu citā valstī. Tāpat arī faksimila sakari, videokonferences un cita veida sakari var būt īstenoti ar Internet starpniecību.

Pamatnosacījumi speciālo izmeklēšanas darbību veikšanai ir šādi:

«210.pants. Speciālo izmeklēšanas darbību veikšanas noteikumi

(1) Šajā nodaļā paredzētās speciālās izmeklēšanas darbības veic, ja kriminālprocesā pierādāmo apstākļu noskaidrošanai ziņas par faktiem nepieciešams iegūt, neinformējot kriminālprocesā iesaistītās personas un tās personas, kuras varētu šīs ziņas sniegt.

(2) Speciālās izmeklēšanas darbības, pamatojoties uz izmeklēšanas tiesneša lēmumu, veic procesa virzītājs vai iestādes un personas viņa uzdevumā. Ja šādas darbības realizācijai nepieciešams izmantot operatīvās darbības līdzekļus un metodes, to uzdod veikt tikai ar likumu īpaši pilnvarotām valsts iestādēm (turpmāk šajā nodaļā – specializētā valsts iestāde).

(3) Speciālās izmeklēšanas darbības drīkst veikt, vienīgi izmeklējot smagus vai sevišķi smagus noziegumus.

211.pants. Speciālo izmeklēšanas darbību rezultātā iegūtā informācija

(1) Speciālās izmeklēšanas darbības gaitā fiksē tikai saistībā ar smagiem vai sevišķi smagiem noziegumiem iegūto informāciju, kura:

1) nepieciešama kriminālprocesā pierādāmo apstākļu noskaidrošanai;

2) norāda uz cita noziedzīga nodarījuma izdarīšanu vai tā izdarīšanas apstākļiem;

3) nepieciešama tūlītēja būtiska sabiedriskās drošības apdraudējuma novēršanai.

(2) Procesa virzītājam, viņa iesaistītajām personām, kā arī prokuroram un izmeklēšanas tiesnesim, kas uzrauga speciālās izmeklēšanas darbības, jāveic visi nepieciešamie pasākumi, lai nepieļautu informācijas vākšanu un izmantošanu neatbilstoši šā panta pirmajā daļā noteiktajiem mērķiem.

212.pants. Atļauja speciālo izmeklēšanas darbību veikšanai

(1) Speciālās izmeklēšanas darbības veic, pamatojoties uz izmeklēšanas tiesneša lēmumu.

(2) Izmeklēšanas tiesneša lēmums nav nepieciešams, ja speciālās izmeklēšanas darbības veikšanai piekrīt visas publiski nepieejamā vietā šīs darbības veikšanas laikā strādājošās vai dzīvojošās personas.

(3) Šīs nodaļas izpratnē publiski nepieejamas ir vietas, kurās nevar ieiet vai uzturēties bez īpašnieka, valdītāja vai lietotāja piekrišanas.

(4) Neatliekamos gadījumos procesa virzītājs var uzsākt speciālās izmeklēšanas darbības, saņemot prokurora piekrišanu un ne vēlāk kā nākamajā darba dienā – izmeklēšanas tiesneša lēmumu.

213.pants. Lēmums par speciālās izmeklēšanas darbības veikšanu

(1) Izmeklēšanas tiesnesis lēmumu par speciālās izmeklēšanas darbības veikšanu pieņem pēc tam, kad ir izskatīts procesa virzītāja motivēts ierosinājums un krimināllietas materiāli.

(2) Lēmumā norāda speciālo izmeklēšanas darbību, iestādes vai personas, kurām uzdota šīs darbības veikšana, tās veikšanas mērķi un atļauto ilgumu, kā arī visus citus apstākļus, kuriem ir nozīme veicamās darbības nodrošināšanā.

(3) Publiski nepieejamā vietā veicamās speciālās izmeklēšanas darbības ilgums nedrīkst pārsniegt 30 dienas. Šo termiņu izmeklēšanas tiesnesis var pagarināt, ja tam ir pamats.

214.pants. Atļaujas saņemšanas kārtības pārkāpšanas sekas

(1) Ja procesa virzītājs nav ievērojis šajā nodaļā noteikto atļaujas saņemšanas kārtību, speciālās izmeklēšanas darbības rezultātā iegūtie pierādījumi nav izmantojami pierādīšanas procesā.

(2) Ja speciālā izmeklēšanas darbība uzsākta šā likuma 212.panta ceturtajā daļā paredzētajā kārtībā, izmeklēšanas tiesnesis lemj par šīs izmeklēšanas darbības uzsākšanas pamatotību, kā arī par tās turpināšanas nepieciešamību, ja tā nav pabeigta. Ja izmeklēšanas darbība nebija pamatota vai tika veikta prettiesiski, tiesnesis lemj par iegūto pierādījumu pieļaujamību un par rīcību ar izņemtajiem priekšmetiem.

233.pants. Pasākumi informācijas aizsardzībai kriminālprocesā

(1) Ziņas par speciālās izmeklēšanas darbības veikšanas faktu līdz tās pabeigšanai ir neizpaužami izmeklēšanas dati, par kuru izpaušanu amatpersonas vai personas, kuras iesaistītas tās veikšanā, atbild saskaņā ar likumu. Aizstāvi, kuram ir tiesības iepazīties ar

visiem kriminālllietas materiāliem no apsūdzības izsniegšanas brīža, ar tiem dokumentiem, kuri attiecas uz speciālo izmeklēšanas darbību, neiepazīstina līdz šīs izmeklēšanas darbības pabeigšanai.

(2) Procesa virzītājs lieto visus likumā paredzētos līdzekļus, lai ierobežotu speciālās izmeklēšanas darbības rezultātā iegūto tādu ziņu izplatīšanu, kurām ir pierādījuma nozīme kriminālprocesā, ja tās aizskar personu privātās dzīves noslēpumu vai skar citu ar likumu aizsargātu ierobežotas pieejamības informāciju.

(3) Speciālo izmeklēšanas darbību rezultātā iegūto materiālu kopiju izgatavošana pieļaujama vienīgi likumā paredzētajos gadījumos, izdarot par to atzīmi attiecīgās darbības protokolā.

234.pants. Kriminālllietai nepievienotajos materiālos ietvertās informācijas aizsardzības pasākumi

(1) Speciālās izmeklēšanas darbības veikšanas metodes, paņēmieni un līdzekļi, kā arī tās rezultātā iegūtās ziņas, kurām nav pierādījumu nozīmes kriminālprocesā, kurā šī darbība veikta, vai kuru izmantošana citā kriminālprocesā nav atļauta, vai kuras nav nepieciešamas sabiedrības drošības tūlītēja būtiska apdraudējuma novēršanai, ir valsts vai izmeklēšanas noslēpums, un personas par to izpaušanu atbild Krimināllikumā noteiktajā kārtībā.

(2) Procesa virzītājs brīdina personas, kuras iesaistītas speciālo izmeklēšanas darbību veikšanā, par šā panta pirmajā daļā paredzēto atbildību. Ja speciālo izmeklēšanas darbību veikšana ir personas profesionāls pienākums, brīdināšanu nodrošina darba devējs.

(3) Prokurors vai izmeklēšanas tiesnesis brīdina par atbildību personas, kuras tiek iepazīstinātas ar kriminālllietai nepievienotajiem materiāliem.

(4) Lemjot par rīcību ar kriminālllietai nepievienotajiem materiāliem, prokurors un izmeklēšanas tiesnesis pārbauda, vai ir brīdinātas visas personas un vai veikti nepieciešamie pasākumi, lai novērstu neattaisnotu informācijas izplatīšanu, un dod uzdevumus trūkumu novēršanai.»

Kriminālprocesa likumā reglamentētas dažāda veida speciālās izmeklēšanas darbības, tajā skaitā minētās divas, kā arī – legālās korespondences kontrole, sakaru līdzekļu kontrole, vietas vai personas audiokontrole, vietas videokontrole, personas novērošana un izsekošana, objekta novērošana, speciālais izmeklēšanas eksperiments, salīdzinošajai izpētei nepieciešamo paraugu iegūšana speciālā veidā un noziedzīgās darbības kontrole.

«227.pants. Noziedzīgas darbības kontrole

(1) Ja konstatēts vienota noziedzīga nodarījuma vai savstarpēji saistītu noziedzīgu nodarījumu atsevišķs posms, bet, to nekavējoties pārtraucot, zudīs iespēja novērst citu noziedzīgu nodarījumu vai noskaidrot visas iesaistītās personas, it īpaši tā organizētājus un pasūtītājus, vai visus noziedzīgas darbības mērķus, pamatojoties uz izmeklēšanas tiesneša lēmumu, var veikt noziedzīgas darbības kontroli.

(2) Noziedzīga nodarījuma pārtraukšanas atlikšana kontroles nolūkā nav pieļaujama, ja nav iespējams pilnīgi novērst:

1) cilvēku dzīvības un veselības apdraudējumus;

2) daudzu cilvēku dzīvībai bīstamu vielu izplatīšanos;

3) bīstamu noziedznieku bēgšanu;

4) ekoloģisku katastrofu vai neatgriezenisku mantisku zaudējumu.

(3) Ja noziedzīgās darbības kontroles nolūkā jāveic citas speciālās izmeklēšanas darbības, atļauja to veikšanai jāsaņem vispārējā kārtībā.

(4) Kontroles veicēji iesniedz procesa virzītājam pārskatus atbilstoši speciālās izmeklēšanas darbības gaitai, bet ne retāk, kā noteikts lēmumā.»

Noziedzīgas darbības kontrole arī var būt veikta IT noziegumu izmeklēšanas gaitā, proti – ja tiek izmeklēti personas vai personu grupas turpināti vai atkārtoti veikti noziedzīgi nodarījumi, lietojot IT resursus, piemēram, krāpšana Internet vidē (piemēram, pielietojot *phishing* vai *pharming* metodes vai izveidojot fiktīvu Internet veikalu vai kazino portālus u.tml.) vai finanšu norēķinos izmantotas informācijas nelikumīga ieguve, veicot patvaļīgu piekļūšanu kredītiestāžu informācijas sistēmai vai citām datu bāzēm, pēc tam šo informāciju jau pārdodot citām personām, kuras veic naudas izņemšanu no šiem kontiem, vai arī bērnu pornogrāfijas izplatīšana, sākot ar šādu pornogrāfijas attēlu vai videoierakstu izgatavošanu un beidzot ar to komerciālu piedāvāšanu ar Internet resursu starpniecību, vai pat narkotiku tirdzniecība Internet vidē, teroristisko organizāciju darbība, apmainoties ar informāciju elektroniskā formā utt.

Noziedzīgu darbību kontrole var būt veikta nacionālā mērogā. Taču, ievērojot Internet vidē veiktu noziegumu (saskaņā ar Kibernoziegumu konvencijas terminoloģiju – kibernoziegumu) pārrobežu raksturu, visos šādos un līdzīgos bīstamu noziegumu gadījumos nereti var būt lietderīgi organizēt ilgstošu tiesisku sadarbību vairāku valstu tiesībsargājošo iestādēm, atsevišķiem uzdevumiem iesaistot arī kredītiestāžu vai citu institūciju pārstāvjus, lai iegūtu informāciju nevis par tikai vienu atsevišķu personu, kas iesaistīta tādu noziegumu īstenošanas kaut kādā posmā, bet gan atklātu pēc iespējas visas personas, kas tajā iesaistītas, to lomas un veiktās darbības noziegumu sagatavošanā, īstenošanā un slēpšanā, to lietotos IT tehniskos un informācijas resursus, metodes un nodarījuma pēdas, tajā skaitā arī elektronisko pierādījumu avotus, nolūkā nodrošināt iespēju tiesāt visus nozieguma izdarītājus, organizatorus un atbalstītājus, un likvidēt nozieguma veikšanai izveidoto informācijas tehnoloģiju resursu, finanšu līdzekļu un citu resursu nodrošinājumu.

Noziedzīgas darbības kontrole var būt īstenota, izveidojot apvienotās izmeklēšanas grupas, saskaņā ar Kriminālprocesa likuma 75. nodaļā iekļautajām normām.

Taču noziedzīgas darbības kontroles nolūkā var būt veikts arī tā sauktais *Internet monitorings*, proti – pastāvīga (tomēr nepārkāpjot tiesiskos nosacījumus) noziedzīgas darbības apzināšana un kontrole Internet vidē, tajā skaitā noziedzīgu aktivitāšu atklāšanai, pārlūkojot elektroniskās saziņu grupas (dažāda veida forumus, *IRC* jeb čatus, vēstkopas u.c.), dažāda veida Internet mājaslapas, tajā skaitā privātās Internet dienasgrāmatas (t.s. *blogus*), turklāt gan tiesībsargājošo iestāžu darbiniekiem vai to uzdevumā citām personām patstāvīgi, gan arī lietojot specializētu programmatūru, kas pārskata serveros indeksētos elektroniskos resursus pēc noteiktiem atslēgvārdiem, kādi tiek lietoti noteikta veida noziedzīgās aktivitātēs.[15]

Kā noprotams no minētā, noziedzīgas darbības kontroles ietvaros var būt veiktas arī KPL 218., 219. un 220. pantos paredzētās darbības.

Veicot noziedzīgās darbības kontroli Internet vidē, vēl jānorāda vairāki aspekti.

Vispirms jau jāuzsver KPL nosacījums, ka speciālās izmeklēšanas darbības var būt veiktas vienīgi smagu un sevišķi smagu noziegumu izmeklēšanā. Tāpēc, piemēram, Krimināllikuma 241., 242. un 243. pantos paredzēto noziedzīgo nodarījumu (t.s. informācijas sistēmu *hakings*, *DDoS* uzbrukumi, web lapu *deface* u.tml.)[16] izmeklēšanas gaitā speciālās izmeklēšanas darbības veikt nedrīkst. Tāpat arī tās nedrīkst veikt, ja tiek izmeklēta Krimināllikuma 244. panta (1) daļā paredzētā datora vīrusa izplatīšana.

Vienīgi tādā gadījumā, ja tiek konstatēts, ka datora vīrusa, tas ir, tāda programmas līdzekļa apzināta izplatīšana, kas izraisa datortehnikas programmatūras vai informācijas nesankcionētu iznīcināšanu vai grozīšanu vai kas sabojā informējošo iekārtu vai sagrauj aizsardzības sistēmu, vai jauna veida vīrusa ievadīšana datortehnikas programmatūras vidē radījusi būtisku kaitējumu (līdz ar to ir Krimināllikuma 244. panta jau (2) daļas dispozīcijā norādītais kvalificējošais apstāklis), pieļauts veikt speciālās izmeklēšanas darbības, jo par šādu noziegumu paredzēta sankcija jau vairāk par pieciem gadiem brīvības atņemšana.

Minētā ierobežojuma lietderība, saskaņā ar autora viedokli, ir strīdīga. No vienas puses, KPL 218., 219., 220. un 227. pantos paredzētās darbības – sakaru līdzekļa kontrole, elektroniskajā informācijas sistēmā esošo datu kontrole, pārraidīto datu satura kontrole un noziedzīgas darbības kontrole, būtiski aizskar cilvēktiesības tām personām, pret kurām tās tiek vērstas, vienlaikus arī būtiski samazinot informācijas aprites un darbību brīvību Internet vidē, kas tradicionāli ir visai brīva šajā aspektā. No otras puses, šāds ierobežojums atņem iespējas tiesībsargājošām iestādēm aizsargāt personas pret noziedzīgiem apdraudējumiem, kādi ir ļoti izplatīti Internet vidē un kas visai būtiski apdraud arī e-biznesa, elektronisko

---

[15] Ievērojot šās publikācijas atklāto raksturu, plašāka informācija par to šeit netiek sniegta.

[16] Par šiem un citiem praktiskiem aspektiem sk., piemēram: Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas metodika. – Rīga: Biznesa augstskola Turība, 2003. – 387 lpp.

finanšu norēķinu drošību un attīstību, kā arī personu privātuma aizsardzību kibervidē, jo to var apdraudēt ne jau tikai tiesībsargājošās iestādes, bet arī noziedzīgu nodarījumu veicēji.

Jānorāda gan, ka šis jautājums jau ir ļoti plašs, jo tas saistīts ar valsts un pat starptautiska mēroga tiesību politiku, kas mūsdienās tiek diskutēts visdažādākajā līmenī – vai Internet videi vajadzētu arī nākotnē palikt iespēji maz tiesiski regulētai, pieļaujot tajā gan maksimālu brīvību, gan vienlaikus arī maksimālu patvaļu un apdraudējumus, vai arī Internet vidi būtu vēlams tiesiski regulēt un vairāk kontrolēt, lai nodrošinātu tajā veikto darbību drošību un, līdz ar to, arī Internet vides komerciālas lietošanas attīstību utt. Kā sākumā norādīts, par to diskusijas notiek pat ANO sammitu līmenī. Turklāt viedoklis par šo jautājumu dažādām sabiedrības grupām un personām ir ļoti atšķirīgs, pat diametrāli pretējs, ko parasti ietekmē katra personīgā pieredze Internet resursu lietošanā un personīgās nostādnes. Tās personas, kuras vēlas attīstīt komercdarbību Internet vidē vai arī droši iepirktis Internet veikalos, izsolēs, spēlēt Internet kazino utt., nosverās uz viedokli par papildus kontroles lietderību. Savukārt, personas, kuras vēlas iegūt materiālas vērtības (piemēram, pirātiskus mūzikas un filmu ierakstus, pirātisku programmatūru utt.) vai pat noziedzīgā ceļā pelnīt naudu, kategoriski nosverās uz viedokli pret Internet vides tiesisku kontroli. Jāpiebilst, ka šis jautājums būtiski aizskar arī politiskos un ideoloģiskos aspektus, tajā skaitā valstīs, kur valdošā vara ierobežo demokrātiskās brīvības (piemēram, valstis, kur dominē ortodoksāls islams, arī Ķīna u.c.), tiek ierobežota arī Internet lietošanas brīvība, bet personas un organizācijas, kas cīnās pret kaut kādiem politiskajiem vai ideoloģiskajiem režīmiem, cīnās arī pret Internet vides tiesisku kontroli.

Līdz ar to, šis jautājums ir pārāk nozīmīgs, lai autors šeit aizstāvētu tikai vienu pozīciju. Attiecībā uz Latviju jāņem vērā spēkā esošā tiesiskā reglamentācija, tās turpmāku attīstību jau atstājot juridiskās zinātnes pārstāvju, nevalstisko organizāciju, politiķu un likumdevēju darbības jomai.

Var vienīgi piebilst, ka teleoloģiski iztulkojot Kibernoziegumu konvencijas 13. panta normu, saskaņā ar autora viedokli, izriet, ka par noziedzīgām darbībām, kas saistītas ar patvaļīgu piekļūšanu informācijas sistēmai, patvaļīgu informācijas iegūšanu u.c., jābūt paredzētai tādai sankcijai, lai novērstu personu vēlmi veikt šādus noziedzīgus nodarījumus («*Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty*.»). Taču ja faktiski ar nacionālajām tiesību normām Latvijā tiesībsargājošām iestādēm tiek būtiski ierobežotas iespējas veikt šādu nodarījumu izmeklēšana, vispār nepieļaujot nepieciešamo izmeklēšanas darbību veikšanu šādās lietās, tādā gadījumā šie nodarījumi var būt ar augstu latentuma pakāpi, līdz ar ko likumpārkāpēji var justies nesodīti un tāpēc pat

iegūt noturīgu nostādni uz šādu darbību recidīvu. Arī Kibernoziegumu konvencijas 2. daļā, kur iekļautas rekomendācijas procesuālo tiesību normu izstrādei, neapšaubāmi norādīts, ka arī minētā veida noziedzīgu nodarījumu izmeklēšanas gaitā jābūt nodrošinātai iespējai veikt nepieciešamās izmeklēšanas darbības (var piebilst, ka KPL 219. un 220. pantos iekļautās speciālās izmeklēšanas darbības tika pārņemtas tieši no Kibernoziegumu konvencijas). Kibernoziegumu konvencijas 21. pantā gan norādīts, ka pārsūtītu satura datu (personas korespondences) iegūšana (*Interception of content data*) var būt veikta vienīgi bīstamu noziegumu (*serious offences*) lietās, norādot, ka atbilstīga klasifikācija jau atkarīga no nacionālās tiesību reglamentācijas.

Līdz ar to, saskaņā ar autora viedokli, likumdevējs Latvijā nav nodrošinājis pietiekami efektīvu normatīvo reglamentāciju, nenosakot Krimināllikuma 241., 242., 243., 244. un arī citos pantos pietiekami smagu sankciju, lai būtu nodrošināta šo nodarījumu sekmīga izmeklēšana, proti – lai būtu iespēja to izmeklēšanas gaitā veikt arī speciālās izmeklēšanas darbības, bez kurām to atklāšana ir maz ticama. Šādu nepilnību lietderīgi novērst, ievērojot gan arī valsts tiesību politikas nostādnes šajā jomā.

Cits aspekts, kas ir būtisks gan KPL 227. pantā reglamentētajai noziedzīgas darbības kontrolei, gan arī citām izmeklēšanas darbībām, ir starptautiskas sadarbības nosacījumu ievērošanas nosacījumi un kārtība, jo noziedzīgu nodarījumu izmeklēšanā būtisks ir valsts jurisdikcijas aspekts. Šie nosacījumi reglamentēti Kriminālprocesa likuma C daļā, tajā skaitā 18. sadaļā reglamentēta palīdzība procesuālās darbības veikšanā.

Kriminālprocesa likumā starptautiskās sadarbības jautājumi ir pietiekami detalizēti atrunāti. Šeit lietderīgi vien pievērst uzmanību arī Kriminālprocesa likuma 2. panta (3) daļā ieļauto normu:

«Citas valsts kriminālprocesa normas var piemērot tikai starptautiskajā sadarbībā uz ārvalsts motivēta lūguma pamata, ja tas nav pretrunā ar Latvijas kriminālprocesa pamatprincipiem.»

un KPL 674. panta (2) un (3) daļas normas:

«(2) Citas valsts kriminālprocesuālo kārtību var piemērot, ja tāda nepieciešamība pamatota krimināltiesiskās sadarbības lūgumā un ja tā nav pretrunā ar Latvijas kriminālprocesa pamatprincipiem.

(3) Latvija var lūgt ārvalsti, izpildot krimināltiesiskās palīdzības lūgumu, piemērot Latvijā noteikto kriminālprocesuālo kārtību vai atsevišķus tās principus.»

ievērojot arī KPL 676. panta normu:

«Pierādījumi, kas iegūti krimināltiesiskās sadarbības rezultātā atbilstoši ārvalstī noteiktajai kriminālprocesuālajai kārtībai, pielīdzināmi šajā likumā paredzētajā kārtībā iegūtiem pierādījumiem.»

No tā izriet, ka veicot, piemēram, kibernoziegumu izmeklēšanu saskaņā ar ārvalsts tiesībsargājošas iestādes lūgumu, var būt īstenoti tāda procesuālā kārtība, kas atšķirās no Kriminālprocesa likuma nosacījumiem. Tomēr tas nenozīmē, ka nav jāievēro augstāk minētie ierobežojumi speciālo izmeklēšanas darbību veikšanai – tāds ierobežojums ir īpaši atrunāts Kriminālprocesa likuma 819. pantā:

«Speciālo izmeklēšanas darbību pēc ārvalsts lūguma veic tikai tad, ja tā būtu pieļaujama Latvijā notiekošā kriminālprocesā par tādu pašu nodarījumu.»

Līdz ar to nepārprotami skaidrs, ka IT noziegumu izmeklēšanas procesuālajā kārtībā svarīgākais tiesiskais princips ir cilvēktiesību aizsardzība, kas rūpīgi jāizvērtē, izstrādājot praktiskas metodes šādu noziedzīgu nodarījumu izmeklēšanai. Vienlaikus nedrīkst aizmirst par to, ka rūpes par nozieguma izdarītāju cilvēktiesību aizsardzību nedrīkst padarīt tiesībsargājošās iestādes bezpalīdzīgas, viņu darbu neefektīvu – vienlīdz svarīga ir arī to personu cilvēktiesību aizsardzība, kuri var kļūt vai ir kļuvuši par cietušajiem noziedzīgos nodarījumos. Gan tiesiskajā reglamentācijā, gan juridiskajā praksē pamataspekts ikvienam tiesiskajam principam ir līdzsvara nodrošināšana, tajā skaitā līdzsvars tiesībsargājošo iestāžu pilnvaru pielietošanā, lai nebūtu nedz pārmērīga varas pielietošana, nedz arī nespēja sekmīgi izpildīt savas funkcijas personu, sabiedrības un valsts interešu aizsardzībā.

Vēl jāpiebilst, ka Kibernoziegumu konvencijas 35. pants paredz, ka katrā valstī, kas to ratificē, jānodrošina tā sauktais 24 / 7 kontaktpunkts, proti – dienests tiesībsargājošā iestādē, kas vienmēr, bez brīvdienām visu diennakti nodrošinātu sazināšanos ar citu valstu atbilstīgiem dienestiem un nacionālajām tiesībsargājošām iestādēm gadījumos, kad IT noziegumu izmeklēšanai jāveic nekavējošas darbības elektroniskas informācijas saglabāšanai nolūkā iegūt elektroniskos pierādījumus. Šis dienests nodrošinātu arī citu neatliekamu sazināšanās uzdevumu īstenošanu, tajā skaitā terorisma draudu gadījumiem. Šādus dienestus sākotnēji izveidoja G8 valstis 1997. gadā un turpmāk tās jau cenšas maksimāli paplašināt valstu skaitu, kur tādi izveidoti un iekļauti kopējā sazināšanās tīklā jeb «24/7 *Network*» (patlaban jau vairāk nekā 20 valstis). Saskaņa ar Kibernoziegumu konvencijas 35. pantu, šajā dienestā jānodarbina darbībām datortīklā apmācīti un pienācīgi tehniski nodrošināti darbinieki, kuriem ir dotas pietiekamas pilnvaras patstāvīgi veikt darbības, lai saglabātu elektroniskos pierādījumus. Turklāt šie darbinieki vai nu jābūt pilnvaroti patstāvīgi nodrošināt sadarbību arī ar citu 24/7 *Network* tīklā esošo valstu atbilstīgiem dienestiem, vai arī viņiem jābūt iespējai nekavējoši vērsties pie kompetentām personām tādas sadarbības nodrošināšanai.

Noslēgumā jānorāda, ka IT noziegumu jomā, līdz ar tās straujo attīstību, gan praktiskie aspekti noziedzīgu nodarījumu izdarīšanā, gan juridiskie aspekti to kvalificēšanai, izmeklēšanai, cilvēktiesību un citu interešu aizsardzībai un starptautiskai tiesībsargājošo

iestāžu sadarbībai ir ļoti daudzpusīgi un ļoti strauji attīstās, tāpēc šajā jomā pastāvīgi jāturpina pētījumi, lai pietiekami rūpīgi izvērtētu visus svarīgos jautājumus un uz tā pamata izstrādātu efektīvus līdzekļus un metodes tiesībsargājošo iestāžu darbam.