Uldis Miķelsons. Informācijas tehnoloģijas un kriminālprocess

Sākotnēji iezīmējot vispārējos aspektus šā temata izskatīšanā, autors vēlas uzsvērt, ka lasītājam gan krimināltiesisko, gan kriminālprocesuālo aspektu aplūkošanu nevajadzētu uztvert kā represīva rakstura līdzekļu un metožu slavēšanu. Krimināltiesības un kriminālprocesa tiesības attīstās un tiek piemērotas, primāri lai aizsargātu sabiedrību pret noziedzīgiem apdraudējumiem, un demokrātiskā valstī tiesībsargājošo iestāžu likumpakārtota darbība šķiet nevēlama tikai tiem cilvēkiem, kuri apdraud citu personu tiesības un intereses.

Šajā nodaļā aplūkota kriminālprocesa tiesību attīstība tajos aspektos, kas skar informācijas tehnoloģiju jomu, proti – noziedzīgu nodarījumu informācijas tehnoloģiju vidē atklāšanu un izmeklēšanu. Šie jautājumi skatīti gan starptautiskā, gan nacionālā mērogā, tajā skaitā sniegts ieskats tiesību politikas attīstībā šajā jomā, raksturota starptautisku organizāciju loma un starptautisku dokumentu pieņemšana un piemērošana, kā arī valstu sadarbība, apkarojot interneta vidē veiktus noziegumus ar pārrobežu raksturu. Tāpat raksturota Latvijas nacionālās tiesību sistēmas un juridiskās prakses attīstība šajā jomā, sniedzot ieskatu IT noziegumu atklāšanas un izmeklēšanas juridiskajos aspektos un problēmās.

Iesākumā jānorāda, ka šīs publikācijas mērķis – aplūkot kriminālprocesa attīstības un piemērošanas pamataspektus IT noziegumu jomā – to nošķir no citiem tuviem jautājumiem, tajā skaitā te netiek sniegts IT noziegumu izmeklēšanas metodikas un taktikas, kā arī elektronisko pierādījumu ieguves un izpētes tehnisko aspektu izklāsts, kas ir pārāk plašs un daudzpusīgs temats, līdz ar ko pilnvērtīgi to var izskatīt vien atsevišķā grāmatā. Arī informācijas sistēmu drošības pamataspekti, kas daļēji pārklājas ar šeit skatītiem jautājumiem, ir aplūkoti atsevišķā publikācijā.

Kriminālprocesuālās reglamentācijas attīstība IT noziegumu jomā

Uzreiz jāuzsver, ka kriminālprocesa tiesību attīstība nenotiek tikpat strauji, kā IT[1] attīstība. Tehnoloģiskais progress un dažādi veidi, kā sabiedrība izmanto informācijas tehnoloģijas, rada arī nevēlamus IT pielietojuma veidus, kas apdraud personu tiesības un intereses. Kad tādas izpausmes ir apzinātas, likumdevējs atbilstīgi vispārējiem tiesību principiem un tiesību politikas nostādnēm var tās kriminalizēt, lai ierobežotu to izpausmes sabiedrībā. Pēc tam sāk veidoties izmeklēšanas un tiesu prakse attiecībā uz šādiem nodarījumiem, kas jau var parādīt

[1] Šeit saīsinājums «IT» domāts gan informācijas tehnoloģijas, gan – kā citos avotos lieto – informācijas un komunikāciju tehnoloģijas jeb IKT. To tehniskos aspektus autors neaplūko, līdz ar to neveltot uzmanību dažādu tehnoloģiju atšķirībām, bet gan ar IT jomu saprotot visas tās tehnoloģijas, kuras balstītas uz elektronisku datu apstrādi, tajā skaitā arī elektronisku datu pārraidi utt. Ievērojot, ka saīsinājums IKT tiek lietots arī, lai nosauktu informācijas un komunikāciju tiesības, lai novērstu pārpratumus, te šis saīsinājums IKT netiks lietots vispār.

nepieciešamību izstrādāt un ieviest jaunas kriminālprocesa normas, lai nodrošinātu efektīvas iespējas izmeklēt un pierādīt attiecīgus nodarījumus. Turklāt kriminālprocesa pilnveide arī nenotiek strauji. Līdz ar to, laika posms starp jaunām tehnoloģiskām iespējām, kuras sabiedrībā var būt izmantotas arī nevēlami, un nepieciešamo kriminālprocesa normu ieviešanu, lai nodrošinātu IT noziegumu[2] izmeklēšanu, var būt diezgan ilgs.

Kaut vai tāds piemērs – lai gan bērnu pornogrāfijas izplatīšana internetā sākās jau kopš XX gs. astoņdesmito gadu otrās puses, pirmā starptautiskā policijas operācija pret to tika veikta tikai 1992.gadā, bet vien 2000.gadā tika pieņemta ANO Rezolūcija A/RES/54/263[3] par bērnu tiesību aizsardzību, kas iekļauj arī šo jautājumu. Vai cits piemērs – pirmie *hakeri* parādījās 1969.gadā, 1981.gadā izplatījās pirmais datorvīruss, internetu civilā jomā sāka lietot 1983.gadā, kopš 1984.gada aizvien biežāk notika *ielaušanās* datorsistēmās, bet tikai 2001.gadā tika pieņemta Eiropas Padomes (EP) *Konvencija par kibernoziegumiem*, kuras mērķis ir veicināt vienotu tiesību politiku šajā jomā dalībvalstīm (un vēl aizvien ne visās pat šīs konvencijas dalībvalstīs ir pietiekami efektīva šās jomas kriminālprocesuālā reglamentācija). Tajā pašā laikā informācijas tehnoloģijas un to pielietojuma veidi un jomas pastāvīgi turpina ļoti strauji attīstīties, radot aizvien jaunus izaicinājumus tiesību aizsardzībai…

Īsi raksturojot IT attīstību mūsdienās, var pieminēt šādus virzienus:

- 2010.gadā ASV superdators *Cry XT5 Jaguar* strādā ar ātrumu 1,759 petaflopi,[4] Ķīnas superdators *Tianhe 1A* sasniedza ātrumu 2,507 petaflopi, bet 2011.gadā IBM grasās pabeigt jau 20 petaflopu superdatoru. 2010.gada sākumā datu pārraides ātrums optiskajā kabelī ar *Cisco Systems* maršrutētāju CRS-3 sasniedz 322 Tbit/s.[5]
- Informācijas tehnoloģiju jomā tiek veikti zinātniski pētījumi saistībā gan ar kvantu fiziku nolūkā izstrādāt *kvantu datorus* un *kvantu sakarus sistēmas*, gan ar neirozinātni nolūkā izstrādāt *neironu tīklus* un integrēt smadzenes ar automatizētām datu apstrādes sistēmām, radot arī dažādas *kiborgu* tehnoloģijas, kas dotu iespēju veidot gan *jauktu virtuāli – reālo vidi*, gan *mākslīgo intelektu*,[6] gan ar nanotehnoloģiju un biotehnoloģiju pētījumiem nolūkā izstrādāt *datorus uz bioloģisku sistēmu, t.sk. gēnu molekulas DNS bāzes* utt.[7]

---

[2] Šeit lietots termins «IT noziegumi», vispārīgi nosaucot 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 uztverei šeit lietots īsāks apzīmējums. Juridiskajā praksē jau jāveic precīza nodarījuma kvalifikācija atbilstīgi Krimināllikuma nosacījumiem. Vēl var piebilst, ka speciālajā literatūrā dažādi autori lieto dažādus terminus, kas praktiski pārklājas, piemēram «High-Tech crimes», datornoziegumi, tehnoloģiju noziegumi utt. Taču te nav lietderīgi iedziļināties terminoloģijas niansēs, jo termins «IT noziegumi» ir pietiekami precīzs aplūkotā temata izklāstam, turklāt tādu lieto arī Interpol u.c. organizācijas.

[3] http://www.un-documents.net/a54r263.htm

[4] Salīdzināšanai – parasti rokas kalkulatori strādā ar ātrumu apt. 10 flopi, bet cilvēks skaitļošanas ātrumu dažas kalkulācijas 0,1 sekundē subjektīvi uztver kā acumirklīgu. Petaflops ir kvadriljons jeb 10^{15} kalkulācijas sekundē.

[5] Salīdzināšanai – ar tādu ātrumu datu pārraidē var nodrošināt, ka visi Ķīnas iedzīvotāji veic video zvanus vienlaikus. Tāpēc tas iezīmē jau nākamās paaudzes datortīklu («NGN» jeb «all-IP»).

[6] Mākslīgā intelekta izstrāde noris ar vairākiem pētnieciskiem projektiem, t.sk. ar ES ietvarprogrammas atbalstu veido 'robotu internetu' http://www.roboearth.org/ ; http://cordis.europa.eu/fp7/ict/cognition/home_en.html
Tā kā īsta mākslīgā intelekta izveide var satricināt sabiedrības pārvaldi pašos pamatos, autors cer, ka tāds faktiski nemaz nav iespējams. Katrā ziņā, Izaka Azimova 1942.gadā nosauktie trīs *robotu tiesību principi* ir nepietiekami apstākļiem, kad informācijas sabiedrība mijiedarbojas ar mākslīgo intelektu: http://en.wikipedia.org/wiki/Three_Laws_of_Robotics
Tomēr šis jautājums ir sabiedrības uzmanības lokā, t.sk. tiek apspriests pat starptautiskā mērogā: http://www.roboethics.org/sanremo2004/index.php
http://en.wikipedia.org/wiki/Artificial_intelligence

[7] Plašāk sk. http://cordis.europa.eu/ist/fet/areas.htm

- Tiek attīstīti līdztekus internetam pastāvoši akadēmiskie un pētniecības datortīkli GÉANT2, Abilene jeb internet2 Network, GLORIAD, JANET, CERNET u.c., dažādi Grid tīkli,[8] tajā skaitā ar semantiskā tīmekļa[9] tehnoloģiju, un arī militārām vajadzībām veidotais GIG (*Global Information Grid*) utt.

- Arī entuziasti attīsta dažādas tīklu tehnoloģijas, īpaši pievērošoties vienādranga tīkliem, t.sk. Tor, Freenet, Turtle, WASTE, Entropy, anoNet, GNUnet, P-Grid, XeroBank, Skype, Ripple tīkli u.c., kuros uzmanība būtiski pievērsta drošas un konfidenciālas saziņas iespējām (šādus p2p tīklus dažkārt apzīmē *F2F* jeb *Friend-to-Friend*).[10]

- 2010.gada beigās interneta lietotāju skaits tuvojas divi miljardiem jeb apt. 29% cilvēces,[11] bet Eiropas Savienībā vairāk nekā puse iedzīvotāju regulāri lieto internetu.[12] Psihiatri uzsver aizvien pieaugošu sociālu problēmu – interneta *atkarību*. Jau mūsdienās aizvien vairāk valstis pat izvieto *virtuālās vēstniecības* virtuālo spēļu vidē, ņemot vērā, cik daudzi cilvēki tajā pavada lielu daļu laika.

- Ar IPv6 ieviešanu datortīklam iespējams pieslēgt visdažādākās tehniskās ierīces, līdz ar to tam kļūstot par "lietisko tīklu",[13] tajā skaitā arī visdažādākā sadzīves tehnika un preces ar radiofrekvenču identifikatoriem RFID var integrēt automatizēti vadāmā t.s. viedajā (*smart*) cilvēka dzīves vidē. Pat cilvēka ķermenī var ievietot miniatūru raidītāju vai pat datoru, kas savieno ķermeņa psihofizioloģiskos procesus ar tās vai citas IS funkcijām vai, nākotnē iespējams, *nanorobotiem* (programmējami nanoprocesori jau ir izstrādāti).

- Aizvien ciešāk tiek saistītas datortīklu, mobilo telekomunikāciju un satelītsakaru tehnoloģijas, kā arī alternatīvās enerģijas avotu tehnoloģijas, nodrošinot elektronisko sakaru tīklu plašu pieejamību gan ģeogrāfiski visā pasaulē, gan pielietojamo funkciju ziņā.

- Visaptverošā vienotā televīzijas sistēma CCTV, piemēram, Londonā, jau pašlaik sniedz efektīvas iespējas sabiedriskās kārtības un noziedzības kontroles jomā, bet ja tā tiktu automatizēti savienota ar citām IS, piemēram, visiem publisko reģistru datiem, personu elektroniskās identifikācijas datiem, ar ko apmaksā braucienus sabiedriskajā transportā, papildinot vēl ar pilnveidotu sejas atpazīšanas un automašīnu reģistrācijas numuru fiksēšanas tehnoloģiju, mobilo telefonu atrašanās vietas datiem, papildinot to ar GPS tehnoloģiju, priekšmetu marķēšanu ar RFID tehnoloģiju, kā arī citu tehnisko metožu izmantošanu, tad var pavērties ceļš patlaban pat neiedomājamām personu novērošanas iespējām (kas neviļus rada asociācijas ar Dž.Orvela antiutopiskā romāna «1984» attēloto ainu).

- Līdzīgi, kā decentralizētās, uz TCP/IP bāzētās interneta tehnoloģijas izspiedušas gan agrāk lietotus centralizētus tīklus, tādus kā Tymnet, ConnNet, Nabu Network, Telenet, gan cita veida datu pārraides tehnoloģijas, tajā skaitā videotex, telex, teletex, teletext, iespējams, jau netālā nākotnē aizmirstībā var nonākt vairākas mūsdienās vēl pazīstamas tehnoloģijas, tādas kā Usenet, IRC, FTP, e-pasts jeb POP / SMTP, Telnet, tāpat kā jau ir novecojuši Gopher, BBS / FidoNet u.tml. Bet WWW jau tiecas pilnveidot uz Web 3.0 vai pat WebOS.

- Aizvien plašāk tiek pielietotas tehnoloģijas, kas ļauj efektīvi pārnest *kibervidē* dažādas agrāk vien tradicionālā formā pazīstamas darbības. Piemēram, straumēšanas tehnoloģijas dod iespēju datortīkla apraidei (*webcasting* un *IP multicast*) konkurēt ar tradicionālo televīzijas un radio apraidi (*broadcasting*), turklāt gan privātā, gan komerciālā, gan izglītības jomās. VoIP tehnoloģijas un aizvien plašāk izplatītie bezvadu datortīklu brīvpiekļuves punkti rada nozīmīgu konkurenci komerciālām telekomunikāciju sistēmām. Bet *virtuālās naudas*[14] lietošana rada mulsinošus izaicinājumus finanšu sistēmām, tajā skaitā attiecībā uz cīņu pret naudas

---

[8] Grid tīkla pamatā ir savā starpā savienoti datoru klasteri (tīkla datoru vienības), kas, savukārt, sastāv no vairākiem (pat simtiem un tūkstošiem) jaudīgu, kopā savienotu datoru. Katra klastera darbību koordinē viens *virsdators*. Grid tīklos apvienotie datori veic aprēķinus un apstrādā datus ar tādu ātrumu un jaudu, kādu nespēj sasniegt neviens dators vai pat "superdators". Eiropas zinātnieku Grid tapis CERN (Eiropas centrs kodolenerģijas pētījumiem) paspārnē. Arī Latvijā darbojas jau trīs Grid klasteri (LU MII un RTU).

[9] Semantiskā tīmekļa (*semantic web*) tehnoloģijas mērķis ir padarīt tiešsaistē pieejamo decentralizēto un lielākoties nestrukturēto informāciju saprotamu ne tikai cilvēkiem, bet arī datorprogrammām, lai radītu ceļu plašai informatīvo procesu automatizācijai visdažādākajās tautsaimniecības nozarēs un sabiedrībā kopumā. Šo mērķi pilnībā sasniegt šobrīd vēl nav iespējams, tam būtu vajadzīgs pilnvērtīgs mākslīgais intelekts. Tāpēc semantiskā tīmekļa ietvaros mēģina formalizēt tās informācijas attēlošanas un apstrādes jomas, kurās zinātne jau piedāvā piemērotus risinājumus. Šī joma saistīta arī ar attēlu atpazīšanas tehnoloģiju pilnveidi.

[10] Piemēram, 2006.gadā dibinātā un 2009.gadā reģistrētā starptautiskā (22 valstu) *Pirātu partiju internacionāle* nopienti apspriež iespēju izvietot failu apmaiņas servisu ārpus valstu jurisdikcijām – neatkarīgos ūdeņos atklātā jūrā, uz aerostata vai pat satelīta Zemes orbītā.

[11] http://www.internetworldstats.com/

[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:LV:HTML

[13] Turpat

[14] Nejaukt ar *elektronisko naudu* jeb *digitālo naudu*, kas ir vien oficiālajā finanšu sistēmā lietotās naudas forma.

atmazgāšanu virtuālo spēļu vidē (tādās kā *Second Life, Entropia Universe* u.tml.)[15] un nodokļu iekasēšanu virtuālo lietu tirdzniecībā, juridiskiem aspektiem attiecībā uz *virtuālajiem noziegumiem*, piemēram, virtuālo spēļu pasaulē veiktām krāpšanām un zādzībām,[16] vai pat jautājumus par virtuālās naudas ietekmi uz valsts centrālās bankas emitētās reālās naudas vērtības izmaiņām, utt.

- Daudzas agrāk izmantotas datu pārraides tehnoloģijas vairs netiek lietotas nepietiekamas to efektivitātes un arī drošības dēļ. Tomēr aizvien pieaug IT noziegumu[17] apdraudējuma iespējamība un arī to nodarītais kaitējums.[18] 2007.gadā Interpol septītajā konferencē pat tika pausts viedoklis, ka mūsdienās ir lielāka iespēja personai kļūst par cietušo no IT nozieguma, nekā no cita veida nozieguma.[19] Var piebilst atsevišķu speciālistu izteikto prognozi – tiešsaites apdraudējumu, autortiesību pārkāpumu un mēstuļu problēmu dēļ ap 2012.gadu internets mums pazīstamā formā vispār vairs nepastāvēs, jo būs piedzīvojis principiālas strukturālas izmaiņas, tajā skaitā sadalījies dažādos korporatīvos tīklos.

Neapšaubāmi, ka no informācijas tehnoloģiju lietošanas aizvien vairāk kļūst atkarīga sabiedrības dzīve visās jomās, sākot ar vides aizsardzību, turpinot ar cilvēces kultūras mantojuma saglabāšanu un beidzot ar vienlīdzīgu tiesību nodrošināšanu visām sociālajām grupām. Pastāvīgi gan nacionālā, gan starptautiskā mērogā notiek diskusijas un tiek īstenoti projekti dažādos *informācijas sabiedrības*[20] virzienos, tajā skaitā e-pārvalde, e-vēlēšanas, e-vīzas, e-nodarbinātība, e-sociālā partnerība, e-zinātne, e-izglītība un e-bibliotēkas, e-pieejamība tiesību aktiem u.tml., e-medicīna, e-infrastruktūra, e-bizness un e-komercija, e-muita, e-nauda un e-tirgus, e-dokumenti un e-paraksti utt. Visas tehnoloģiski attīstītās valstis ir izstrādājušas vai izstrādā ilgtermiņa valsts attīstības programmas šajā jomā. Ar *informācijas sabiedrības* attīstību saistītos jautājumus skata arī ANO[21] Tūkstošgades projektā (*Millennium Project*). Eiropas Savienība 2005.gadā izskatīja «*eEurope 2005 Action Plan*» rezultātus un pieņēma jaunu piecgades iniciatīvu *i2010* «*A European Information Society for growth and*

Jāpiebilst gan, ka jēdziens *virtuālā nauda* tiek lietots arī ekonomikā, raksturojot to naudas daudzumu, kam nav seguma ekonomikā, un kas tiek emitēta, lai veicinātu patēriņa ātrumu, bet faktiski to izmanto finanšu spekulācijās. Kaut kādā ziņā virtuālās naudas jēdziens ekonomikā un spēļu vides virtuālajā ekonomikā sakrīt, jo arī reālajā ekonomikā virtuālā nauda praktiski atspoguļojas virtuālās vērtībās – akciju vērtības maiņas kursos, kredītprocentu likmēs, inflācijas procentā u.tml.

15 http://en.wikipedia.org/wiki/MMORPG ; http://en.wikipedia.org/wiki/MMO

16 Piemēram, ASV policija atteicās uzsākt izmeklēšanu 2008.gadā, kad saņēma iesniegumu no divdesmitgadīgā Geoff Luurs par to, ka *Final Fantasy XI* spēlē kāds nozadzis viņa spēles tēlam piederošo "maģisko zobenu" un citus rīkus un virtuālo naudu, ko viņš uzkrājis četru gadu spēlēšanas laikā. Policija paziņoja, ka šiem "maģiskajiem rīkiem" un virtuālajai naudai nepiemīt vērtība atbilstīgi reālās pasaules lietām, tāpēc nevar uzskatīt, ka būtu noticis noziegums. G.Luurs gan apgalvoja, ka viņam izdarīts zaudējums par 75 miljoniem šīs spēles "Gil", kas atbilst 3800 ASV dolāriem, un visas viņam nozagtās virtuālās vērtības var būt viegli pārdotas par reālu naudu – ASV dolāriem vai eiro – kādā no portāliem, kur pastāvīgi ilggadīgi notiek šāda tirdzniecība, piemēram, www.ige.com. Policijas atteikumu šajā lietā asi kritizēja ievērojami ASV juristi.
Savukārt Nīderlandē policija 2007.gada novembrī arestēja kādu 17 gadīgu jaunieti par virtuālo mēbeļu zādību spēlē *Second Life*, kuras vērtība pielīdzināma 5000 ASV dolāriem.
Bet Dienvidkorejā pat izveidota īpaša policijas struktūra, kas izmeklē virtuālo spēļu vidē veiktus noziegumus.

17 IT noziegumu kategorija aptver vairāk kā 30 Krimināllikumā iekļautus noziedzīgu nodarījumu sastāvus, kur daļa ir vienmēr saistīti ar IT jomu (kibernoziegumi), bet daļa var būt saistīta ar IT noteiktos nodarījuma apstākļos. Tomēr šai publikācijai nav mērķis aplūkot IT noziegumu krimināltiesiskos aspektus, tāpēc šo nodarījumu uzskaitījums te netiek veikts.

18 Atsevišķu lielāko IT noziegumu radītais kaitējums ir bijis vairāku miljonu ASV dolāru apjomā.

19 http://www.interpol.int/Public/ICPO/speeches/India20070912.asp

20 Jēdziens «informācijas sabiedrība» tiek lietots kā vispārējs civilizācijas attīstību raksturojošs termins, kur cilvēku suga kultūras evolūcijā ir izgājusi cauri pirmatnējai sabiedrībai, agrikulturālai sabiedrībai un industriālajai sabiedrībai, sasniedzot postindustriālās sabiedrības pakāpi, kad civilizācijas attīstību pamatā raksturo plaša IT izmantošana, «uz zināšanām balstīta ekonomika» (*knowledge economy*) utt.

21 http://www.itu.int/wsis/index.html

employment».[22]

Šāda tendence noteic arī to, ka sabiedrības interešu un cilvēku tiesību aizsardzība kļūst aizvien vairāk atkarīga no IT jomas tiesiskās reglamentācijas un tās pielietošanas efektivitātes, tajā skaitā arī IT noziegumu izmeklēšanas un novēršanas jomā.

Tomēr tas, ka IT jomas tiesiskās reglamentācijas attīstība pastāvīgi atpaliek no pašu informācijas tehnoloģiju attīstības, saistīts arī ar politiskiem faktoriem. Atliek vien atcerēties, ka vairākās valstīs ne vien ir speciālas struktūrvienības cīņai pret *kiberterorismu*, bet to bruņotajos spēkos ir arī izveidotas īpašas struktūras *kiberkara* īstenošanai,[23] turklāt 2010.gada maijā Dallasā notikušajā Pirmajā kiberdrošības sammitā tika ierosināta un 2011.gada februārī Minhenes drošības konferencē jau tika starptautiski apspriesta *kiberkara konvencija*. Proti – valstu politika iekļauj arī iespēju veikt kaitējumu citu valstu informācijas sistēmām (IS). Arī kibervidē veiktu darbību izmeklēšanā nereti ir svarīga to vai citu valstu politiskā griba un juridiskās iespējas nodrošināt tiesisko palīdzību lūdzošai valstij elektronisku informāciju no attiecīgās valsts IS vai arī tajā esošas privātas IS.

Vienlaikus nerimst arī diskusijas par cilvēka tiesībām uz vārda brīvību, par cenzūras nepieļaujamību demokrātiskā sabiedrībā, par personīgās dzīves jeb privātuma un korespondences noslēpuma neaizskaramību. Rietumvalstu sabiedrībā nereti tiek kritizētas valstis, kuras īsteno cenzūru internetā, piemēram, Ķīnu, Kubu, Ziemeļkoreju, Ēģipti, vairākas islāma valstis u.c.[24] Tomēr cilvēktiesību aizstāvji kritizē cilvēktiesību apdraudējumu arī virknē demokrātisko rietumvalstu, piemēram, ASV valdības vēlmi ieviest interneta kontroli (sevišķi pēc WikiLeaks publikācijām), kā arī papildus jau esošajām ASV iedzīvotāju saziņas totālas kontroles iespējām vēl arī bez tiesneša akcepta noklausīties ārvalstnieku telefona sarunas un kontrolēt elektronisko saziņu[25] (ASV Kongress 2008.gada jūlijā to gan noraidīja kā nekonstitucionālu), kā arī ASV 2008.gadā Muitas un Robežsardzes amatpersonām piešķirtās pilnvaras bez tiesas sankcijas un nesniedzot jebkādu pamatojumu administratīvas apskates ietvaros jebkurai valsts robežu šķērsojošai personai atsavināt datoru, mobilo telefonu vai jebkādu elektroniskas informācijas nesēju uz nenoteiktu laiku, lai pārmeklētu, kopētu un pat iesniegtu trešajām personām izpētei tajā esošo informāciju (kaut gan vairāki ASV Kongresa deputāti 2008.gadā iesniedza pat trīs likumprojektus, kas paredzēti šādas kārtības likvidēšanai attiecībā uz ASV pilsoņiem).

---

[22] http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

[23] Piemēram, ASV valdība 2011.gada sākumā ar konkursu '*Cyber Challenge*' meklē 10'000 talantīgus studentus, kuri vēlētos kļūt par kiberkareivjiem, kā arī Pentagonam atļauts veidot *botnetu* kiberuzbrukumu veikšanai – tādā pašā veidā, kā to dara kibernoziedznieki. Savukārt pēc kiberuzbrukumiem ar *botneta* palīdzību 2006.gadā Igaunijai, vēlāk Gruzijai un Lietuvai, kas tika īstenots politisku motīvu dēļ, NATO vērtēja šāda veida apdraudējumu kā līdzvērtīgu militāram raķešu triecienam.

[24] http://opennet.net/

[25] http://www.aclu.org/legislative/index.html

No vienas puses ir ļoti liela sabiedrības daļa, kas cīnās par interneta brīvību[26] jeb viedokļu[27] un informācijas plūsmas brīvību elektroniskā vidē, no otras puses ir arī ļoti spēcīgs politiskais un biznesa lobijs, kas tiecas panākt savu interešu aizsardzību arī ar elektroniskās vides kontroles metodēm. Bez tam nevar noliegt arī IT noziegumu radīto apdraudējumu un valsts pienākumu aizsargāt sabiedrību pret noziedzīgiem apdraudējumiem, tomēr novēršot varas pārmērīgu pielietojumu. Tas kopumā parāda ***dinamiska līdzsvara*** tendenci, kas kaut kādā ziņā veicina gan tehnoloģiju un to pielietojuma sabiedrībā straujāku attīstību, gan vienlaikus arī rada nenoteiktību tiesību politikas veidošanā un tiesību normu izstrādē informācijas un komunikāciju tiesību jomā, tajā skaitā arī IT noziegumu izmeklēšanas jomā.

Kā piemēru par starptautiska līmeņa diskusijām attiecībā uz elektronisko vidi te var arī minēt, ka pirms ANO samita par informācijas sabiedrību,[28] kas notika 2003.gada decembrī Ženēvā un 2005.gada novembrī Tunisā, dažu valstu, tajā skaitā Ķīnas, Brazīlijas, Dienvidāfrikas Republikas, Irānas, Saūda Arābijas, Norvēģijas, Šveices un Krievijas pārstāvji izteica ierosinājumu, par ko 2004.gada 11.novembrī ANO ģenerālsekretārs vēl izveidoja darba grupu WGIG, par juridisko pilnvaru piešķiršanu ANO kompetencei – lietās, kas saistītas ar globālā datortīkla pārvaldīšanas funkcijām (*Internet Governance*).[29] Tam iebilda ASV, kuras Tirdzniecības ministrija ir noteicēja interneta domēnu vārdu sistēmas[30] uzturēšanā, un kurai ir veto tiesības attiecībā uz starptautiskās pārvaldes organizācijas ICANN[31] lēmumiem (tas faktiski nodarbojas ar šo jautājumu risināšanu), ievērojot arī, ka vairums DNS *root* serveru vēsturiski ir ASV uzņēmumu un augstskolu pārziņā. Šādu ASV nostāju atbalstīja arī Apvienotā Karaliste. Tāpēc tad tika panākts vien kompromisa risinājums – interneta pārvaldības foruma[32] ikgadēja organizēšana ar ANO atbalstu (t.sk. 2010.gadā tas notika Lietuvā), kā arī reģionāli interneta pārvaldības forumi, tajā skaitā Eiropas mērogā.[33] Tomēr nevar izslēgt, ka nākotnē starptautiskā sabiedrība var atgriezties pie šī jautājuma, ja izmainīsies globālais politisko spēku samērs un IT jomas attīstība radīs tādus jaunus izaicinājumus, kuru risinājums būs iespējams vienīgi ciešas

[26] http://en.wikipedia.org/wiki/Internet_Freedom

[27] Eiropas Cilvēktiesību tiesa ar 1997.gada 1.jūlija spriedumu lietā *Oberschlick v. Austria* noteica, ka vārda brīvība attiecas ne vien uz informācijas saturu, bet arī uz formu, kādā šī informācija tiek izpausta.
Virknē valstu, t.sk. Latvijā cenzūra ir aizliegta gan attiecībā uz ziņām, gan uz viedokļiem jebkādā to formā.
Taču, saskaņā ar Krimināllikumu un atbilstīgi arī EP Konvencijai par kibernoziegumiem, nav pieļaujama tādas informācijas izplatīšana, kas apdraud citu personu un sabiedrības likumīgās intereses.
Te saskatāmo kolīziju atrisina cilvēktiesību princips, kas iekļauts arī LR Satversmes 116.pantā, proti – vārda brīvību un cenzūras aizliegumu var ierobežot likumā paredzētajos gadījumos, lai aizsargātu citu cilvēku tiesības, demokrātisko valsts iekārtu, sabiedrības drošību, labklājību un tikumību.
Kā piemēru nepieciešamai cenzūrai var minēt bērnu pornogrāfijas aizliegumu.

[28] http://www.itu.int/wsis/index.html

[29] http://www.wgig.org/ ; http://www.internetgovernance.org/

[30] Jāpiebilst gan, ka domēna vārdu sistēmas pārvaldība nav izšķirīgs līdzeklis interneta pārvaldīšanai. Piemēram, pēc tam, kad skandalozas informācijas nopludināšanas dēļ tika slēgts domēns WikiLeaks.org, attiecīgie elektroniskie resursi tika izplatīti vietnē bez domēna vārda, kuras URL ir tikai IP adrese: http://46.59.1.2/

[31] http://www.icann.org/

[32] http://www.intgovforum.org/

[33] http://www.eurodig.org/

starptautiskas sadarbības ceļā.

Tiesībsargājošo iestāžu pretdarbība noziedzīgiem nodarījumiem informācijas tehnoloģiju jomā vērsta gan uz to atklāšanas, gan procesuālas izmeklēšanas, gan novēršanas efektivitātes paaugstināšanu. Dažkārt gan sabiedrībā notiek diskusijas par to, ka tirgus attiecības tautsaimniecībā atsevišķos aspektos var efektīvāk atrisināt vairāku IT noziegumu radīto personu interešu apdraudējumu, nekā strikti ierobežojoša tiesiskā reglamentācija, tajā skaitā tiek atbalstīts viedoklis, ka vispiemērotākā pretdarbības stratēģija IT noziegumiem savieno – (a) tiesību aizsardzību, (b) tehnoloģiskos un (c) tirgus attiecību risinājumus. Jāpiebilst gan, ka jebkādā aspektā pretdarbība IT noziegumiem ir saistīta ar dažādiem tiesiskiem un praktiskiem šķēršļiem.

IT noziegumu pieaugošais apdraudējums, īpaši to izpausme starptautiskā mērogā rada nopietnu izaicinājumu gan nacionālām tiesību aizsardzības iestādēm, gan starptautiskām organizācijām, kas pētī tiesību politiku šajā jomā. To skaitā uzmanību šai problēmai pievērš ANO,[34] OECD,[35] G8,[36] NATO,[37] Interpol,[38] Europol,[39] Eiropas Padome,[40] ES,[41] EK,[42] Eiropas drošības un sadarbības organizācija (OSCE),[43] Baltijas jūras valstu padome (CBSS),[44] Starptautiskā tirdzniecības palāta (ICC),[45] Starptautiskā sodu tiesību asociācija (IAPL),[46] Pasaules intelektuālā īpašuma organizācija (WIPO),[47] Starptautiskā telekomunikāciju savienība

---

[34] Combating the criminal misuse of information technologies. / UN Resolution 55/63, adopted by the General Assembly, 4 December 2000. – http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
Combating the criminal misuse of information technologies. UN Resolution 56/121, adopted by the General Assembly. 19 December 2001. – www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

[35] The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. DSTI/ICCP/REG(2005)1/FINAL. 16th December 2005. – http://www.oecd.org/dataoecd/16/27/35884541.pdf

[36] Best Practices for Law Enforcement Interaction with Victim–Companies during a Cybercrime Investigation. Prepared by the G8's Subgroup on High-Tech Crime. June 17, 2005. – www.g8.utoronto.ca/justice/g8justice2005-practices.pdf

[37] http://www.nato.int/issues/cyber_defence/index.html

[38] http://www.interpol.int/Public/TechnologyCrime/default.asp

[39] http://www.europol.europa.eu/index.asp?page=news&news=pr061124.htm

[40] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp

[41] http://europa.eu/scadplus/leg/en/lvb/l33193b.htm ; http://www.enisa.europa.eu/

[42] Vispārīgā politika cīņai ar kibernoziedzību. / Eiropas Kopienu Komisijas paziņojums Eiropas Parlamentam, Padomei un Eiropas Reģionu Komitejai, Nr. COM (2007) 267, Briselē, 22.05.2007. – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LV:HTML

[43] Governing the internet : Freedom and Regulation in the OSCE Region. Organization for Security and Co-operation in Europe. The Representative on Freedom of the Media, 2007. – http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf

[44] http://www.cbss.st/baltinfo/2005/dbaFile9297.html

[45] Internet Intelligence : A three-day course at Cambridge University on How to use the internet as an Effective Investigative Research Tool : March 29 - 1 April 2009. International Chamber of Commerce. – http://www.icc-ccs.org/pdfs/II_2009_Brochure.pdf

[46] XVth International Congress of Penal Law. Rio de Janeiro, 4 – 10 September 1994. (J.L. De La Cuesta (ed.), Resolutions of the Congresses of the International Association of Penal Law (1926 – 2004). – www.penal.org/pdf/ReAIDP2007/RICPL.pdf

[47] World Intellectual Property Organization. Methods and device for increasing security during data transfer (WO/2007/035149). – http://www.wipo.int/pctdb/en/wo.jsp?IA=SE2006001044&DISPLAY=DESC

(ITU),[48] Amerikas valstu organizācija (OAS),[49] Nāciju Sadraudzība (*The Commonwealth of Nations*),[50] Āzijas – Klusā okeāna sadarbības organizācija (APEC),[51] Arābu valstu līga[52] u.c.,[53] meklējot efektīvus pretdarbības risinājumus.

Tiesību normu pilnveidošana šajā jomā sākās jau XX gadsimta astoņdesmitajos gados. Piemēram, Austrālijā jaunas kriminālprocesa tiesību normas šo jautājumu regulēšanai pieņēma 1971.gadā, Apvienotajā Karalistē – 1984., Dānijā – 1985., ASV – 1986., Kanādā – 1986. un vēl papildu 1988. un 1997., Vācijā – 1989. un 1996., Nīderlandē – 1992. un Austrijā – 1993.gadā. Tomēr vēl 1998.gadā Vācijas Vircburgas universitātes profesors Sībers (*Ulrich Sieber*) savā pētījumā[54] norādīja, ka nedz Eiropā, nedz arī ASV un Kanādā, nemaz nerunājot par citām valstīm, nav pietiekami efektīvas tiesiskās bāzes cīņai ar kibernoziegumiem. Vēl aizvien tiek turpināta tiesiskā reglamentācijas pilnveide gan tajās valstīs, kur šis darbs uzsākts pirms vairākiem gadiem, gan tajās, kur tikai mūsdienās sāk risināt šo problēmu.

1981.gada decembrī Interpol Ģenerālsekretariāts organizēja pirmo apmācības semināru par datornoziegumu atklāšanu, bet 1995.gadā notika Interpol pirmā starptautiskā konference par datornoziedzību, kurā piedalījās 49 valstu tiesību aizsardzības iestāžu un citu valstisku un privātu organizāciju speciālisti. Konferencē tika izdarīti vairāki nozīmīgi secinājumi, tajā skaitā konstatējot, ka lielākajā daļā valstu pieaug informatīvo tehnoloģiju izmantošana noziedzīgā darbībā, kas izraisa nepieciešamību pastāvīgi pētīt šo jomu līdz ar datortehnoloģiju attīstību. Lielākajā daļā valstu tiesību aizsardzības iestādēm tas ir bijis jauns noziedzības veids, kuram tās ne vienmēr ir bijušas pietiekami sagatavotas. Arvien lielāku izplatību gūst starptautiskas ar datoriem saistītas noziedzības fakti. Īpaši starp šiem noziegumiem jāpiemin krāpšana, nelikumīgi iegūtu līdzekļu legalizācija, kaitīgu programmu izplatīšana, neautorizēta piekļūšana informācijas sistēmām un informācijas neatļauta ieguve. Šīs problēmas rada nepieciešamību izstrādāt starptautiskas procedūras šīs kategorijas noziegumu izmeklēšanas atbalstīšanai. Konferencē tika uzsvērts, ka lielākajā daļā valstu nav pietiekamas normatīvās bāzes un starptautiski līgumi, lai

---

48 http://www.itu.int/cybersecurity/

49 Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. / Permanent Council of the OEA/Ser.G. Organization of American States CP/CSH-635/04 rev. 2. 13 May 2004. Committee on Hemispheric Security. – http://scm.oas.org/doc_public/ENGLISH/HIST_04/CP12893E04.doc

50 Model Law on Computer and Computer Related Crime. / Commonwealth Secretariat. Marlborough House, London. SW1Y 5HX. October 2002. - http://www.thecommonwealth.org/Internal/38061/documents/

51 Lima Declaration. / The Sixth APEC Ministerial Meeting on the Telecommunications and Information Industru (TELMIN6). 1-3 June, 2005. Lima, Peru. – http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005.html

52 Cairo Declaration against Cybercrime. 27 November 2007. - http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity %20Cairo/CairoDeclarationAgainstCC2007_EN.pdf

53 http://www.first.org/

54 Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME-Study. / Prepared for the European Commission by Prof. Dr. Ulrich Sieber, University of Würzburg. 1st January 1998., 240 p. - http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf

cīnītos ar šiem noziegumiem. Pamatiemesls ir tas, ka lielākajā daļā valstu likumdošana attīstījās, pirms radās datornoziedzības problēma, turklāt normatīvās bāzes pilnveide ir lēns process.

Te var minēt piemēru[55] – Argentīnas iedzīvotājs H.Ardita (*Julio Cesar Ardita*) bija no Argentīnas teritorijas veicis patvaļīgu piekļūšanu vairākām informācijas sistēmām ASV teritorijā, kas 1996.gadā bija pierādīts ASV veiktajā izmeklēšanā, taču ASV nespēja panākt viņa izdošanu no Argentīnas, jo abu valstu savstarpējā noziedznieku izdošanas līgumā nebija paredzēta tāda kategorija kā IT noziegumi – tā iemesla dēļ, ka Argentīnā vispār nebija kriminalizētas šāda veida darbības. (Var gan piebilst, ka 1998.gadā Ardita pats labprātīgi piekrita aizbraukt uz ASV izciest minimālu sodu par šiem noziegumiem – trīs gadus labošanas darbus un 5000 dolāru soda naudu.)
Argentīnas likumi šajā ziņā nebija mainījušies vēl 2002.gadā, kad tika attaisnoti hakeri no t.s. «X-Team» grupas, kuri 1998.gadā patvaļīgi izmainīja Argentīnas Augstākās tiesas mājaslapas saturu, protestējot pret spriedumu nogalinātā žurnālista *Jose Luis Cabezas* lietā, kurš bija publiskojis faktus par augstu amatpersonu korupciju. Tiesa konstatēja, ka Argentīnas likumi neaizsargā elektronisko vidi, tajā skaitā interneta mājaslapas.[56]
Šāda veida noziegumus Argentīnā kriminalizēja tikai 2008.gada jūlija sākumā, pēc trīs gadus ilgušām debatēm parlamentā.

1992.gadā OECD izstrādāja «Informāciju sistēmu drošības vadlīnijas»,[57] kas bija kā pamats, lai attīstītu likumdošanu cīņai pret apdraudējumiem kibertelpā. Tajā skaitā ieteikts «pieņemt un veicināt atbilstošas politikas, kā arī likumu, dekrētu, noteikumu un starptautisku līgumu pieņemšanu, tostarp nosacījumus: krimināla, administratīvai un citām sankcijām par informācijas sistēmu nepareizu lietošanu; tiesu jurisdikcijas kompetencei, ieskaitot eksteritoriālās jurisdikcijas noteikumus, un citu iestāžu administratīvajai kompetencei; savstarpējai palīdzībai, noziedznieku izdošanai un citai starptautiskai sadarbībai IS drošības jautājumos; pierādījumu iegūšanas līdzekļiem informācijas sistēmās un šādu pierādījumu atzīšanai kriminālos, civilos un administratīvos procesos. Nodrošināt un veicināt izglītību un apmācību, tajā skaitā arī tiesībsargājošām iestādēm, izmeklētājiem, advokātiem un tiesnešiem.» 2002.gadā OECD publiskoja jau pilnveidotas vadlīnijas šajā jomā,[58] bet 2005.gadā – to veicinošu programmu.[59]

1995.gadā pēc ASV Federālā Izmeklēšanas biroja Datornoziegumu izmeklēšanas nodaļas CART (*Computer Analyse and Response Team*) iniciatīvas Interpol izveidoja starptautisku darba grupu: IOCE (*International Organisation on Computer Evidence*), kas ietver dalībniekus no Eiropas, ASV, Kanādas, Dienvidāfrikas un Āzijas valstīm ar mērķi sekmēt gan informācijas apmaiņu starp tiesību aizsardzības iestādēm par IT noziegumu izmeklēšanu un elektronisko pierādījumu jautājumiem, gan piemērotas programmatūras, aparatūras un izmeklēšanas metodiku pārbaudi un apmaiņu, kā arī organizēt reģionālas darba grupas un seminārus par šo tematu, lai nodrošinātu starptautiski vienotus standartus elektronisko pierādījumu iegūšanai.

2010.gada septembrī Interpol noorganizēja pirmo starptautisko Informācijas drošības

[55] Computers and International Criminal Law: High Tech Crimes and Criminals. / By João Godoy - http://www.nesl.edu/intljournal/vol6/godoy.pdf
[56] http://news.bbc.co.uk/1/hi/world/americas/1932191.stm
[57] OECD Guidelines for the Security of Information Systems, 1992. - http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_1_1_1_1,00.html
[58] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002. - http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
[59] The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. DSTI/ICCP/REG(2005)1/FINAL. 16th December 2005. – http://www.oecd.org/dataoecd/16/27/35884541.pdf

konferenci, lai pilnveidotu starptautisko sadarbību šajā jomā, uzlabotu cīņu pret IT drošības apdraudējumiem un sekmētu kritisko infrastruktūru aizsardzību. Tajā piedalījās pārstāvji no 188 valstīm. Var piebilst, ka starp referentiem bija arī Igaunijas pārstāvis Erki Kodar, kurš izklāstīja Igaunijas pieredzi pretdarbībā 2007.gadā veiktajam kiberuzbrukumam.

1997.gada 10.decembrī tika noslēgta vienošanās starp G8 valstīm – ASV, Kanādu, Apvienoto Karalisti, Vāciju, Franciju, Itāliju, Krieviju un Japānu par ciešu sadarbību IT noziegumu izmeklēšanā. Saskaņā ar to, balstoties uz G8 Lionas – Romas Progresīvo tehnoloģiju noziedzības apkarošanas grupas rekomendācijām, dalībvalstis vienojās pilnībā atbalstīt citā valstī notikuša IT nozieguma izmeklēšanu ar savas valsts tiesībsargājošo iestāžu iespējām, izmantojot arī progresīvāko tehnoloģiju saziņai, kā arī veidot atbilstošu normatīvo bāzi un noslēgt nepieciešamos sadarbības līgumus. Minētā vienošanās arī paredzēja nodrošināt savstarpējo palīdzību IT noziegumu izmeklēšanā ar kvalificētu personālu, 24/7 kontakta centru (24 stundas diennaktī, septiņas dienas nedēļā) organizēšanu, kā arī nepieciešamo metodiku, procedūru, tehnoloģiju un standartu izmantošanu elektronisko pierādījumu iegūšanā, saglabāšanā, autentifikācijā un izpētē. 2000.gada jūlijā Okinavā, Japānā notikušajā samitā G8 valstis papildu vienojās par starpnacionālas speciālās vienības DOTF (*Digital Opportunity Task Force*) izveidi nolūkā integrēt starpvalstu sadarbību.

Par praktisku tiesībsargājošo iestāžu sadarbību tiek noslēgtas arvien jaunas reģionālas starpvalstu vienošanās, piemēram, 2000.gada decembrī Sicīlijā, Itālijā tika noslēgta starptautiska vienošanās par sadarbību organizētās noziedzības apkarošanā un IT noziegumu atklāšanas jomā, ko parakstīja arī Latvijas iekšlietu ministrs. Efektīvu tiesisko un praktisko pretdarbības līdzekļu un metožu IT noziegumiem izstrādei starptautiskā mērogā pēdējos gados organizētas vairākas ilggadīgas darba grupas, kā arī regulāri notikušas konferences un semināri par šiem jautājumiem.

Vairākas speciālas darba grupas nolūkā izpētīt un izstrādāt praktiskas metodes un līdzekļus IT noziegumu izmeklēšanai un novēršanai tika izveidotas ar ANO Ģenerālās Asamblejas 1997.gada 12.decembra rezolūciju Nr. 52/91 un 1998.gada 9.decembra rezolūciju Nr. 53/110. Šo darba grupu izstrādātās vadlīnijas izskatīja Vīnē 2000.gada 10.-17.aprīlī organizētajā ANO desmitajā kongresā par noziegumu apkarošanu un noziedznieku sodīšanu.[60] Šajā kongresā tika skatīti jautājumi: IS uzglabātu datu iegūšana un izmantošana noziegumu izmeklēšanā; pārraidītu datu un ar pārraidi saistītu datu iegūšana un izmantošana; elektronisko datu izpēte un elektroniskie pierādījumi; elektronisko komunikāciju sistēmu kontrole; meklēšana datortīklā un elektroniskas informācijas ieguve pāri valstu jurisdikciju robežām; cilvēktiesību un privātīpašuma aizsardzības nodrošināšana, izmeklējot IT noziegumus, u.c.

Eiropas Komisija pastāvīgi pievērš uzmanību šai jomai. Tajā skaitā EK 22.05.2007.

[60] http://www.un.org/events/10thcongress/2088h.htm

ziņojumā *Vispārīgā politika cīņai ar kibernoziedzību*[61] norādīti šādi apstākļi: «Mūsdienu sabiedrībai arvien nozīmīgāko informācijas sistēmu drošība aptver daudzus aspektus, kuru būtiskākā sastāvdaļa ir cīņa ar kibernoziedzību. Praksē terminu kibernoziedzība lieto attiecībā uz trīs noziedzīgu darbību kategorijām. Pirmā ietver noziedzīgo nodarījumu tradicionālās formas, kā piemēram, krāpšana vai viltošana, taču saistībā ar kibernoziedzību tā īpaši attiecas uz nodarījumiem, ko veic ar elektronisko sakaru tīklu un informācijas sistēmu (turpmāk – elektroniskie tīkli) palīdzību. Otrā attiecas uz nelegāla satura informācijas publiskošanu elektroniskajos medijos (piemēram, materiāli, kuros atspoguļota seksuāla vardarbība pret bērniem vai kūdīšana uz rasu naidu). Trešā aptver tikai elektroniskajiem tīkliem raksturīgus noziedzīgus nodarījumus, piemēram, uzbrukumi informācijas sistēmām, pakalpojumu atteikšana un nelikumīga piekļuve. Šāda veida uzbrukumi var būt vērsti arī pret ārkārtīgi būtiskām infrastruktūrām Eiropā un iespaidot pastāvošās ātrās reaģēšanas sistēmas daudzās jomās, kas var izraisīt postošas sekas visai sabiedrībai. Visu šo kategoriju noziedzīgo nodarījumu kopīga pazīme ir tā, ka tos iespējams veikt masveidā un atrodoties lielā attālumā no seku iestāšanās vietas. Tādējādi izmantotās izmeklēšanas metodes no tehniskā viedokļa ļoti bieži ir vienādas.

Ņemot vērā šo attīstību, steidzami ir nepieciešama rīcība gan valstu, gan visas Eiropas mērogā, kas būtu vērsta pret visa veida kibernoziedzību, kas rada nozīmīgus un aizvien pieaugošus draudus īpaši nozīmīgām infrastruktūrām, sabiedrībai, uzņēmējdarbībai un pilsoņiem. Indivīdu aizsardzību pret kibernoziedzību nereti sarežģī jautājumi par tiesas piekritību, piemērojamām tiesībām, pārrobežu piespiedu izpildi vai elektronisko pierādījumu atzīšanu un izmantošanu. Kibernoziedzības pārrobežu raksturs pastiprina šīs grūtības. Lai stātos pretī aprakstītajiem draudiem, Eiropas Komisija ierosina izstrādāt vispārīgu politiku, lai uzlabotu Eiropas un starptautiskā līmeņa sadarbību cīņai ar kibernoziedzību. Politika paredzēs: uzlabotu operatīvo sadarbību tiesību aizsardzības jomā, labāku politiskā līmeņa sadarbību un koordināciju starp dalībvalstīm, politisko un tiesisko sadarbību ar trešām valstīm, informētības veicināšanu, apmācību, izpēti, pastiprinātu dialogu ar ekonomikas nozaru pārstāvjiem un iespējamus likumdošanas pasākumus.

Šis paziņojums par politiku cīņai ar kibernoziedzību apkopo un papildina 2001.gada paziņojumu par „Drošākas informācijas sabiedrības izveidi, uzlabojot informācijas infrastruktūru drošību un apkarojot datornoziegumus” Ar to tika ierosināts izstrādāt atbilstošas materiālo un procesuālo tiesību normas gan pašmāju, gan pārrobežu noziedzīgo darbību apkarošanai. Tika pieņemti arī citi vispārīgāki tiesību akti, kas aptvēra cīņas ar kibernoziedzību atsevišķus aspektus, kā piemēram, Pamatlēmums 2001/413/TI “Par krāpšanas un viltošanas apkarošanu

[61] Vispārīgā politika cīņai ar kibernoziedzību. / Eiropas Kopienu Komisijas paziņojums Eiropas Parlamentam, Padomei un Eiropas Reģionu Komitejai, Nr. COM(2007) 267, Briselē, 22.05.2007. – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LV:HTML

attiecībā uz bezskaidras naudas maksāšanas līdzekļiem". Pamatlēmums 2004/68/TI "Par bērnu seksuālās izmantošanas apkarošanu" ir labs piemērs tam, cik nopietnu uzmanību Komisija pievērš bērnu aizsardzībai, jo īpaši attiecībā uz jebkāda veida materiālu par seksuālo vardarbību pret bērnu nelikumīgu publicēšanu, izmantojot informācijas sistēmas, un šī horizontālā prioritāte saglabāsies arī nākotnē.

Informācijas sabiedrības drošības problēmu risināšanai Eiropas Kopiena ir izstrādājusi trīsdaļīgu pieeju, lai nodrošinātu tīklu un informācijas drošību, kas ietver: īpašus tīklu un informācijas drošības pasākumus, elektronisko sakaru regulējumu un cīņu ar kibernoziedzību. Lai gan minētos trīs aspektus zināmā mērā var attīstīt atsevišķi, tie ir savstarpēji cieši saistīti, un tāpēc ir nepieciešama to cieša savstarpēja koordinēšana. Paralēli 2001.gada paziņojumam Eiropas Komisija 2001.gadā ar kibernoziedzību cieši saistītajā tīklu un informācijas drošības jomā pieņēma "Paziņojumu par tīklu un informācijas drošību: priekšlikums Eiropas politikas pieejai". „E-Privātuma" Direktīva 2002/58/EK paredz publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem pienākumu nodrošināt viņu sniegto pakalpojumu drošumu. Turpat ir paredzēti noteikumi pret surogātpastu un spiegprogrammatūru. Tīklu un informācijas drošības politika kopš tā laika attīstās un tās ietvaros ir īstenoti vairāki pasākumi, jaunākie no tiem ir "Paziņojums par drošas informācijas sabiedrības stratēģiju, kas paredz atjaunot stratēģiju" un piedāvā shēmu, kā turpināt un uzlabot saskaņoto pieeju tīklu un informācijas drošībai, "Paziņojums par surogātpasta, spiegprogrammatūru un ļaunprātīgu programmatūru apkarošanu" un "Paziņojums par ENISA izveidošanu 2004.gadā". ENISA galvenais mērķis ir uzkrāt īpašās zināšanas, lai uzlabotu sadarbību starp valsts un privāto sektoru un sniegtu atbalstu Komisijai un dalībvalstīm. Nozīmīgu vietu cīņā ar kibernoziedzību ieņem arī pētījumu rezultāti informācijas sistēmu drošības nodrošināšanas tehnoloģiju jomā. Tādējādi informācijas un sakaru tehnoloģijas un drošība ir iekļautas ES Septītās pētniecības pamatprogrammas (FP7) mērķu sarakstā, kas paredzēta laika periodam no 2007. līdz 2013.gadam.

Informācijas tīklu globālā rakstura dēļ kibernoziedzības apkarošanas politika nevar būt efektīva, ja to realizē tikai Eiropas Savienības robežās. Noziedznieki var uzbrukt informācijas sistēmām vai izdarīt noziedzīgus nodarījumus ne tikai no vienas dalībvalsts otrā, bet arī atrodoties ārpus Eiropas Savienības jurisdikcijas. Tāpēc Eiropas Komisija ir aktīvi piedalījusies starptautiskās diskusijās un sadarbības pasākumos, piemēram, G8 *Lionas – Romas Progresīvo tehnoloģiju noziedzības apkarošanas grupā* un Interpol vadītajos projektos. Īpaši uzmanīgi Eiropas Komisija seko *Starptautiskā progresīvo tehnoloģiju noziedzības apkarošanas diennakts informācijas apmaiņas tīkla* (24/7 tīkls) darbībai, kurā apvienojušās ievērojams skaits valstu visā pasaulē, ieskaitot lielāko daļu ES dalībvalstu. Šis tīkls ar diennakts informācijas apmaiņas punktu palīdzību nodrošina iespēju paātrināti nodibināt sakarus starp dalībvalstīm lietās, kas

saistītas ar elektroniskajiem pierādījumiem un kurās steidzami nepieciešama ārvalstu tiesību aizsardzības iestāžu palīdzība.

Galvenā vājā vieta tieslietu, brīvības un drošības jomā ir steidzamas pārrobežu operatīvās sadarbības iespēju trūkums vai to nepietiekama izmantošana. Tradicionālā savstarpējās palīdzības sistēma ir izrādījusies lēna un neefektīva, kad jārisina steidzamas kibernoziedzības lietas, tomēr jauni sadarbības līdzekļi vēl nav pietiekami attīstīti. Kaut arī valstu tiesu un tiesību aizsardzības iestādes Eiropā cieši sadarbojas ar Eiropol, Eirojust un citu struktūru starpniecību, pastāv acīmredzama nepieciešamība pastiprināt un noskaidrot pienākumus.»

Eiropas Savienība izveidotā pastāvīgi darbojošās Eiropas tīklu un informācijas drošības aģentūra ENISA[62] aptver plašu jautājumu loku cīņai pret kibernoziegumiem, to izpētei un rekomendāciju izstrādei IS drošības jomā, lai nodrošinātu efektīvas drošības politikas ieviešanu *informācijas sabiedrības* un *digitālās ekonomikas* attīstībā. ENISA veicina ciešu sadarbību starp ES institūcijām, ES dalībvalstīm, IT industrijas pārstāvjiem un privāto sektoru.

Balstoties uz 2005.gada pamatlēmumu – *Par uzbrukumiem informācijas sistēmām*[63] – Eiropas Komisija 2010.gadā sagatavoja direktīvas projektu par aizsardzību pret uzbrukumiem informācijas sistēmām, kā arī jaunus noteikumus par ENISA modernizēšanu un statusa nostiprināšanu. Tie veidoti, lai izveidotu efektīvu mehānismu reaģēšanai uz kiberuzbrukumiem, jo īpaši tādiem, kas tiek veikti ar botu tīklu palīdzību, kā tas notika, piemēram, 2009.gada martā. Tajā ir noteikta juridiskā atbildība par noziedzīgu instrumentu radīšu un izmantošanu, kā arī paredzēti stingrāki sodi likumpārkāpējiem. Direktīvas mērķis arī ir tiesas un policijas sadarbības uzlabošana, t.sk. Europol tīklā atbilde uz pieprasījumu būs jāsniedz astoņu stundu laikā. Kibernoziegumu statistikas datu vākšana būs visu ES dalībvalstu pienākums, kas sekmēs vienotu sistēmu cīņai ar kiberuzbrukumiem. Līdz ar direktīvas pieņemšanu minētais 2005.g. pamatlēmums tiks atcelts, bet dalībvalstu tiesību akti divu gadu laikā būs jāsaskaņo ar jauno direktīvu. ENISA pilnvaras, kas beidzas 2012.gadā, paredzēts pagarināt vēl uz pieciem gadiem. Saskaņā ar jaunajiem noteikumiem šai organizācijai jānodrošina aktīva pieredzes apmaiņa par cīņu ar kibernoziedzību un jāveicina valsts organizāciju, dalībvalstu tiesībaizsardzības iestāžu un datornozares pārstāvju sadarbība šajā nolūkā. Šie dokumenti iesniegti izskatīšanai Eiropas Parlamentā, lai pēc tam tos nosūtītu apstiprināšanai ES Ministru padomē.

2010.gada novembrī ENISA organizē plašas kiberaizsardzības mācības visām 27 ES dalībvalstīm. 2008.gadā ES izlēma veidot visām 27 ES dalībvalstīm kopīgu informācijas sistēmu, kurā reģistrēs nelegālas darbības internetā un informāciju par aizdomās turētajām

---

62 http://www.enisa.europa.eu/

63 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. / The Council of the European Union – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML

personām šādos noziegumos, kā arī operatīvo informāciju kibernoziegumu apkarošanas jomā. Šīs IS izveide un uzturēšana ir deleģēta Europol. Bez tam Europol veido arī vietni, kur jebkurš var ziņot par nelikumīgu saturu interneta lapās, kā arī Europol darbojas 'kiberpatruļas' šā veida apdraudējumu atklāšanai. 2010.gada jūnijā izveidotā «*European Union Cybercrime Task Force*» Europol struktūrā veido vienotu Eiropas Kibernoziegumu centru.

Šādi jautājumi tiek pētīti arī Eiropas Padomes izveidotās speciālās darba grupās nolūkā izstrādāt normatīvo regulējumu un rekomendācijas IT noziegumu izmeklēšanai un starpvalstu sadarbības veicināšanai šajā jomā. Pirmā šāda darba grupa no 1985. līdz 1989.gadam izstrādāja EP rekomendāciju R(85)S. Balstoties uz apzināto problēmu novērtējumu un iepriekšējā darba galarezultātiem, Eiropas komisija par noziedzības problēmām (CDPC)[64] 1991.gadā izveidoja ekspertu komisiju nolūkā sagatavot rekomendācijas projektu «Kriminālprocesa tiesību problēmas, kas saistītas ar informācijas tehnoloģiju», ko 1995.gada 11.septembrī pieņēma kā EP rekomendāciju R(95)13. Tās mērķis bija izveidot pamatu kriminālprocesuālās reglamentācijas pilnveidei Eiropas Padomes dalībvalstīs un kandidātvalstīs, sevišķi attiecībā uz tiesību normu saskaņošanu – specifiskos procesa tiesību strīdu jautājumos, piemēram, meklēšanas iespējamība starptautiskās IS un datu iegūšanā, telekomunikāciju noklausīšanās utt. Rekomendācija R(95)13 tika pieņemta, atsaucoties arī uz EP rekomendāciju R(81)20, kas vērsta uz tiesību saskaņošanu saistībā ar rakstisko pierādījumu prasībām un dokumentu atveidošanas pieļaujamību un datorierakstiem, EP rekomendāciju R(85)10, kas attiecas uz korespondences neaizskaramību un telekomunikāciju noklausīšanos, EP rekomendāciju R(87)15, kas regulē personas datu lietošanu policijas darbā un EP rekomendāciju R(89)9, kas attiecas uz ar datoriem saistītiem noziegumiem.

Savukārt 2001.gada 23.novembrī tika atvērta parakstīšanai EP *Konvencija par kibernoziegumiem*,[65] kas stājās spēkā 2004.gada 1.jūlijā. 2003.gadā tai tika pievienots papildus protokols par neiecietības nodarījumiem.[66] Latvija šo konvenciju un tās papildprotokolu ratificēja 2007.gada 14.februārī un tā Latvijā stājās spēkā 2007.gada 1.jūnijā. Šai konvencijai ir pievienojušās ne vien EP dalībvalstis, bet arī atsevišķas valstis, kuras nav Eiropas Padomē, tajā skaitā to ratificējusi ASV, bet parakstījušas vēl Kanāda, Japāna, Dienvidāfrikas Republika. 2010.gada beigās tā bija stājusies spēkā kopumā 30 valstīs, bet tikai parakstījušas to bija vēl 17 valstis.[67] Eiropas Padome rosina visām valstīm pievienoties šai konvencijai, lai radītu iespēju īstenot efektīvu starptautisku sadarbību kibernoziegumu izmeklēšanā, ņemot vērā to pārrobežu raksturu. Faktiski šī konvencija arī kalpo par tiesību politikas pamatdokumentu daudzām valstīm

[64] www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Steering_Committees/Cdpc/

[65] Convention on Cybercrime. / Council of Europe. Budapest, 23 November 2001. - http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm ; http://www.likumi.lv/doc.php?id=146481

[66] Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. / Council of Europe. Strasbourg, 28 January 2003. - http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm ; http://www.likumi.lv/doc.php?id=146481

[67] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

tiesiskās reglamentācijas un juridiskās prakses pilnveidei šajā jomā un uz to bieži atsaucas arī citas starptautiskas organizācijas atbilstīgos tiesību politikas dokumentos.

Jānorāda gan, ka vairākas valstis, piemēram, Krievija, tomēr nevēlas tai pievienoties, tajā skaitā dēļ šīs konvencijas 32.panta b) punktā paredzētās iespējas, ka «Puse var bez citas Puses atļaujas piekļūt vai saņemt ar tās teritorijā atrodošās datorsistēmas palīdzību uzkrātos datus, kas atrodas citā Pusē, ja Puse saņem likumīgu un brīvprātīgu tās personas piekrišanu, kurai ir likumīgas tiesības atklāt datus Pusei ar attiecīgās datorsistēmas palīdzību.» Krievija norādīja, ka šī norma aizskar valsts suverenitāti.[68]

Ja pasaulē būs valstis, kuras nesadarbosies ar citām kibernoziegumu izmeklēšanā, tad, diemžēl, netiks īstenots ANO aicinājums nepieļaut "drošas debesis" kibernoziedzniekiem, jo internetā var viegli veikt darbības pāri vairāku valstu robežām, personai pat neatrodoties attiecīgās valsts teritorijā, kā arī var viegli likvidēt nozieguma pēdas, ja tās ir elektroniskas informācijas formā.

Konvencijā par kibernoziegumiem iekļautas ietvarnormas gan noteiktu darbību kriminalizācijai, gan to izmeklēšanas metožu noteikšanai, gan starpvalstu sadarbībai – nolūkā harmonizēt valstu nacionālo tiesisko reglamentāciju šajā jomā.

Ratificējot šo konvenciju, arī Latvijas *Kriminālprocesa likumā* (KPL)[69] iekļautas virkne normu, kas nepieciešamas IT noziegumu efektīvai izmeklēšanai un pierādīšanai, vienlaikus ievērojot cilvēktiesību aizsardzības nosacījumus (kā arī noteiktos jautājumos ir pilnveidots *Krimināllikums*). Tajā skaitā detalizēti reglamentētas speciālās izmeklēšanas darbības, kas saistītas ar sakaru līdzekļu kontroli, elektroniskajā informācijas sistēmā esošo datu kontroli, pārraidīto datu satura kontroli, atsevišķi reglamentēti nosacījumi informācijas ieguvei no elektroniskās informācijas sistēmas, kā arī ir definēti elektroniskie pierādījumi. Bez tam, atsevišķā KPL sadaļās iekļautas normas attiecībā uz cilvēktiesību aizsardzību kriminālprocesā un attiecībā uz starptautisko sadarbību krimināltiesiskajā jomā. Līdz ar to pašlaik Latvijas nacionālajā tiesību sistēmā, saskaņā ar starptautiski atzītām vadlīnijām, ir izstrādāta diezgan efektīva kriminālprocesuālā reglamentācija IT noziegumu izmeklēšanai.

Tomēr tas nenozīmē, ka šīs jomas tiesiskās reglamentācijas attīstība ir pabeigta un turpmāk uzmanība jāpievērš vienīgi tiesību normu pareizai un efektīvai piemērošanai juridiskajā praksē. Ņemot vērā informācijas tehnoloģiju un to pielietojuma straujo un daudzpusīgo attīstību, arī IT noziegumu izmeklēšanas tiesiskās reglamentācijas attīstība turpinās.

IT noziegumu atklāšanas un izmeklēšanas juridiskās pamatproblēmas

[68] http://www.newsland.ru/News/Detail/id/238312/

[69] Kriminālprocesa likums. / Ar grozījumiem uz 2011.gada 1.janvāri. Latvijas Vēstnesis Nr.74, 2005.gada 11.maijā.

Viens no jautājumiem, kas vēl nav ieguvis vienotu risinājumu dažādu valstu tiesību politikā, ir par tiesībsargājošo iestāžu pilnvarām slēpti iegūt elektronisko sakaru sistēmās apstrādātu vai pārraidītu informāciju. Pamatpieeja šajā jomā ir, ka personas korespondences noslēpums (tas attiecas arī uz informācijas ieguvi datorsistēmās, ko pieļauj EP *Konvencija par kibernoziegumiem*.) var būt slēpti aizskarts tikai attiecīgas valsts jurisdikcijā un tikai ar tiesneša atļauju. Tomēr ne visas valstis strikti pieturas pie tieši šādas reglamentācijas.

Piemēram, atšķirīga nostāja ir ASV Prezidenta administrācijai un ASV Augstākajai tiesai, no kuras 2006.gada sprieduma Hamdan v. Rumsfeld lietā[70] izrietēja, ka ASV Konstitūcijai neatbilst 2002.gada saskaņā ar Patriot Act[71] izdotais ASV prezidenta Dž.Buša, Jr. rīkojums, ar ko Nacionālās drošības aģentūrai dota iespēja noklausīties telefona sarunas un iegūt elektroniski pārraidītus datus bez tiesneša akcepta tajos gadījumos, kad notika saziņa starp ārvalstnieku un ASV pilsoni, kur aizdomās turētais ir ārvalstnieks. Prezidents tomēr neatkāpās un 2007.gada 5.augustā parakstīja likumu,[72] kas reglamentēja šo jomu atbilstīgi iepriekšējam rīkojumam. Šis likums zaudēja spēku 2008.gada 17.februārī, bet 2008.gada 10.jūlijā Dž.Buša parakstīja jau cita speciālā likuma[73] grozījumus, kas turpina iepriekšējo kārtību.

Līdzīgi Zviedrijā 2008.gada jūnijā tika pieņemts likums[74] (stājās spēkā 2009.gada 1.janvārī), kas līdzinās nule aprakstītajam ASV regulējumam, un par to Zviedrijas cilvēktiesību aizstāvji jau izteikuši salīdzinājumu ne vien ar ASV, bet arī Ķīnas un Saudi Arābijas pieeju. 2008.gada septembrī Zviedrijas valdība gan paziņoja, ka varētu mīkstināt šī likuma regulējumu, ņemot vērā plašos sabiedrības protestus. Tomēr 2010.gadā Zviedrija turpināja līdzīgu tiesību politiku, pieņemot likumu par datu saglabāšanu (stāsies spēkā 2011.gadā), kur līdz ar savienojuma datiem noteikts pienākums saglabāt arī e-pasta sūtījumu saturu un telefonu īsziņas.

2008.gada 27.februārī Vācijas Konstitucionālā tiesas spriedums,[75] izskatot federālās zemes Ziemeļreinas – Vestfālenes pieņemto likumu, noteica, ka slēpti veikta informācijas meklēšana datorsistēmās (tajā skaitā instalējot tajā programmatūru, kas veic šādas funkcijas bez datora lietotāja ziņas) ir pieļaujama tikai ar tiesneša atļauju un tikai tādās lietās, kur ir apdraudētas likumīgi aizsargātas intereses, tādas kā cilvēku dzīvība vai valsts drošība. 2010.gadā Vācijas Konstitucionālā tiesa atcēla 2007.gadā pieņemto datu uzglabāšanas likumu, tomēr pēc terorisma

[70] Supreme Court of the United States. Hamdan v. Rumsfeld, Secretary of Defense, et al. Certiorari to the United States Court of Appeals for the District of Columbia Circuit. No. 05–184. Argued March 28, 2006. Decided June 29, 2006. - http://www.law.cornell.edu/supct/html/05-184.ZS.html

[71] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT). / Act of 2001. - http://epic.org/privacy/terrorism/hr3162.html

[72] Protect America Act of 2007. - http://www.govtrack.us/congress/billtext.xpd?bill=s110-1927

[73] Foreign Intelligence Surveillance Act of 1978. ("FISA" Pub.L. 95-511, 92 Stat. 1783, enacted 1978-10-25, 50 U.S.C. ch.36.) - http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_36.html

[74] http://en.wikipedia.org/wiki/FRA_law

[75] Leitsätzezum Urteil des Ersten Senats vom 27. Februar 2008. BUNDESVERFASSUNGSGERICHT. - 1 BvR 370/07. - 1 BvR 595/07. - http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

trauksmēm vairāki politiķi ierosināja atjaunot šo likumu.

Savukārt Dānijā 2010.gada rudenī Nodokļu ministrija ierosināja pieņemt likumu, lai ikviena uzņēmuma datoru cietajā diskā esošo informāciju varētu pārkopēt bez tiesneša atļaujas, nodokļu inspektoriem ierodoties negaidītā pārbaudē.[76]

Aplūkotā jautājuma būtība saistīta arī ar to, ka pastāv diezgan efektīvas tehnoloģijas,[77] kas var veikt elektronisko sakaru *monitoringu* pēc noteiktiem uzstādījumiem automatizētā režīmā, bet tas nav savienojams ar tiesneša akcepta ieguvi, jo tiesneša lēmums ir attiecināms tikai uz konkrētiem objektiem, par kuriem jau ir konstatētas ziņas, kas dod pamatu turēt tos aizdomās par noteiktu saistību ar smagu noziegumu vai valsts drošības apdraudējumu.

Tomēr, ievērojot terorisma draudu līmeni mūsdienās, var domāt, ka diskusijas par šo jautājumu turpināsies, neraugoties uz cilvēktiesību aizstāvju protestiem. Kaut vai tāpēc, ka cilvēktiesības nedrīkst būt iztulkotas vienpusēji – saskatot cilvēktiesības tikai aizdomās turētajām personām, bet ignorējot tādu fundamentālu cilvēktiesību principu, ka valstij ir pienākums aizsargāt cilvēkus pret noziedzīgiem apdraudējumiem. Proti, cilvēktiesību piemērošanā būtisks ir samērīguma princips. Tas noteikts arī *Latvijas Republikas Satversmes*[78] 116.pantā.

Latvijā šī jautājuma tiesiskā reglamentācija ir strikta, turklāt neatkarīgi no tā, vai tiek veikta noziedzīga nodarījuma izmeklēšana *Kriminālprocesa likuma* noteiktā kārtībā, vai arī tiek veikti kriminālmeklēšanas pasākumi noziedzīgu nodarījumu atklāšanai vai pretizlūkošanas pasākumi valsts drošības aizsardzībai saskaņā ar *Operatīvās darbības likuma*[79] noteikto kārtību – speciālās izmeklēšanas darbības kriminālprocesuālā vai sevišķā veidā veicamās operatīvās darbības pasākumus operatīvās darbības procesā, tajā skaitā sakaru līdzekļu kontroli, elektroniskajā informācijas sistēmā esošo datu kontroli, pārraidīto datu satura kontroli pieļaujams veikt mazāk smagu, smagu un sevišķi smagu noziegumu lietās,[80] ierobežotu laika periodu, kriminālprocesā ar izmeklēšanas tiesneša lēmumu, bet operatīvās darbības procesā ar īpaši pilnvarota Augstākās tiesas tiesneša sankcionētu lēmumu.[81]

Cits jautājums, kam vēl nav nešaubīgs risinājums nedz starptautiskos tiesību politikas dokumentos, nedz arī Latvijas un citu valstu nacionālajā tiesiskajā reglamentācijā, ir par personas privātuma aizsardzību attiecībā uz tehniska rakstura datiem elektronisko sakaru tīklā. Ja attiecībā uz personas korespondenci (t.sk. telefona saruna, īsziņas, e-pasta[82] vai cita elektroniska sūtījuma saturs) ir skaidrs pamatprincips – tās noslēpums var būt aizskarts tikai noziegumu atklāšanas vai valsts drošības aizsardzības interesēs, noteiktā kārtībā, ar tiesneša atļauju, tad

[76] http://drosiba.pudele.com/2010/10/danish-proposal-to-copy-corporate-hard-drives/

[77] Tādas kā *Echelon*, arī t.s. *Frenchelon*, *Onyx*.

[78] Latvijas Republikas Satversme. / Ar grozījumiem uz 2010.gada 2.novembri. Latvijas Vēstnesis Nr.43, 1993.gada 1.jūlijā.

[79] Operatīvās darbības likums. / Ar grozījumiem uz 2010.gada 1.janvāri. Latvijas Vēstnesis Nr.131, 1993.gada 30.decembrī.

[80] Noziedzīgu nodarījumu smagums tiek noteikts pēc Krimināllikumā attiecīgā pantā noteiktās sankcijas.

citādi ir attiecībā uz tehniskiem datiem (proti – noslodzes dati, atrašanās vietas dati un ar tiem saistīti dati, kas nepieciešami lietotāja identificēšanai), kuri paši par sevi neietver personas korespondenci, tomēr tie var pastarpināti atspoguļot fragmentāras ziņas par personas privāto dzīvi. Neapšaubāmi, privātās dzīves neaizskaramība ir tāpat cilvēktiesību aizsargāta, kā korespondences neaizskaramība – ar *Latvijas Republikas Satversmes* 96.pantu. Tomēr nav tikpat neapšaubāmi, ka privātās dzīves noslēpums tiek apdraudēts, ja iegūst elektronisko sakaru tīkla tehniskos datus, kurus rada un automatizēti apstrādā tīkla programmatūra un kas nepieciešami saziņas tehniskai nodrošināšanai.

Piemēram, telekomunikācijas tīklā tādi dati ir: telefona numurs, no kura tiek zvanīts un kuram tiek zvanīts, kā arī zvana datums, laiks, ilgums u.c. Šādi dati *per se* nesniedz nekādu informāciju par fizisko personu, jo nevar izslēgt, ka konkrēto zvanu varēja veikt ne vien konkrētā numura pastāvīgs lietotājs, bet arī cita persona, kas lietojusi attiecīgo telefona aparātu; līdzīgi arī elektroniskajā saziņā. Protams, praksē tas nav tik viennozīmīgi, jo, pirmkārt, dati, kas nepieciešami lietotāja identificēšanai, ir fizisko personu dati, kurus aizsargā speciāls likums,[83] otrkārt, no liela apjoma šādu tehnisko datu analīzes var iegūt diezgan nozīmīgu informāciju par personu, tajā skaitā viņa kontaktu loku, ja analizē telefona zvanu datus, kā arī intereses, ieradumus un citas ziņas, ja analizē interneta pārlūkošanas datus, utt.

Ņemot vērā, ka cilvēktiesību viens no pamatprincipiem ir valstij uzlikts pienākums aizsargāt personas pret noziedzīgiem apdraudējumiem, bet tas nav iespējams bez efektīvu izmeklēšanas metožu un līdzekļu pielietošanas, diskusijas par šāda veida datu izmantošanas nosacījumiem ir nepieciešamas. Sakarā ar izdarītajiem grozījumiem *Elektronisko sakaru likumā*[84] (ESL), 2007.gada jūlijā – septembrī tāda diskusija bija starp Valsts policijas, Tieslietu ministrijas, Ģenerālprokuratūras pārstāvjiem un Tiesībsargu.

---

[81] Te var piebilst, ka vairāki juristi, kuriem pievienojas arī autors, aizstāv viedokli, ka lietderīgi būtu likvidēt tiesībsargājošo iestāžu praktiskā darba sadalītību kriminālprocesā un operatīvās darbības procesā. Tā kā abi šie juridiskās prakses veidi faktiski ir vērsti uz vienu un to pašu pamatmērķi – noziedzīgu nodarījumu atklāšanu un izmeklēšanu, lai galarezultātā tiktu iegūti pierādījumi, kurus varētu vērtēt tiesa (izņēmums gan ir izlūkošana un pretizlūkošana, kam ir atšķirīga specifika), turklāt arī kriminālprocesā ir jau reglamentētas slēpti veicamas darbības (proti – speciālās izmeklēšanas darbības), kuras praktiski ir tādas pašas, kā atbilstīgie operatīvās darbības pasākumi, tad izmeklēšanas un kriminālmeklēšanas juridiska savienošana būtu vien likumsakarīga un nodrošinātu ekonomiskāku un efektīvāku tiesībsargājošo iestāžu darbu. Tāda pieeja ir vairākās rietumvalstīs (turklāt ne vien angļu – sakšu tiesību saimes valstīs, bet arī kontinentālās Eiropas tiesību tradīcijai piederošajā Vācijā u.c.), kur tā pierādījusi sevi no pozitīvās puses. Rietumvalstu tiesībsargājošo iestāžu pārstāvji dažkārt pat nesaprot tādu nošķirtību starp izmeklēšanu un kriminālmeklēšanu, kas Latvijā un citās valstīs ir pārmantota no t.s. sociālistiskās tiesību tradīcijas.

[82] ES Direktīvas 95/46/EK 29.panta darba grupas atzinums 2/2006 Par privātās dzīves aizsardzības jautājumiem, kas saistīti ar e-pasta caurlūkošanas pakalpojumiem. / 00451/06/LV. WP 118., pieņemts Briselē 21.02.2006. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_lv.pdf - [EC Informatics Directorate]

[83] Fizisko personu datu aizsardzības likums. / Ar grozījumiem uz 2010.gada 2.jūniju. Latvijas Vēstnesis Nr.123/124, 2000.gada 6.aprīlī.

[84] Elektronisko sakaru likums. / Ar grozījumiem uz 2011.gada 1.janvāri. Latvijas Vēstnesis Nr.183, 2004.gada 17.novembrī.

Tiesībsarga birojs publiskoja[85] šādu, no iepriekšējās juridiskās prakses atšķirīgu viedokli: «Šāda datu pieprasīšana nopietni aizskar Satversmē un *Eiropas Cilvēktiesību konvencijā* garantētās personas tiesības uz privātās dzīves un korespondences neaizskaramību. Šo tiesību uzdevums ir nodrošināt brīvu saziņu starp personām, un tās aizsargā ne tikai saziņas saturu, bet arī informāciju par saziņas apstākļiem. Vienlaikus Tiesībsargs atzīst, ka 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. Tāpēc Tiesībsargs aicina atbildīgās institūcijas interpretēt normatīvos aktus atbilstoši Satversmei un saņemt tiesas atļauju saglabājamo datu pieprasīšanai.

Tiesībsargs uzskata, ka pašlaik spēkā esošos likumus, tajā skaitā *Elektronisko sakaru likumu*, var dažādi interpretēt. Taču tiesiskā valstī normatīvajos aktos ietvertās tiesību normas ir jātulko pēc iespējas atbilstoši konstitūcijai, un no Satversmes izriet prasība pēc tiesas atļaujas saglabājamo datu nodošanas gadījumā. Turklāt arī citu likumu normu, kas attiecas uz izmeklēšanas darbību veikšanu, formulējumi neizslēdz šādu interpretāciju. Tāpēc jau šobrīd normatīvie akti būtu jāinterpretē tā, ka tiesas atļauja saglabājamo datu pieprasīšanai ir nepieciešama.

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 likumā*.»

Saistībā ar šo Tiesībsarga pozīciju, autors vēlas izteikt viedokli, ka, tiešām, saskaņā ar *Latvijas Republikas Satversmes* 96.pantu ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību. Savukārt, saskaņā ar Satversmes 116.pantu personas tiesības, kas noteiktas Satversmes 96.pantā, var ierobežot likumā paredzētajos gadījumos, lai aizsargātu citu cilvēku tiesības, demokrātisko valsts iekārtu, sabiedrības drošību, labklājību un tikumību. ESL paredzēto saglabājamo datu pieprasīšana kriminālprocesā vai operatīvās darbības procesā izmeklēšanas vajadzībām aizskar personas privāto dzīvi, līdz ar to tiešām ierobežo personai Satversmes 96.pantā paredzētās tiesības, tomēr šāds tiesību ierobežojums ir noteikts ar likumu un tas atbilst leģitīmam mērķim, kuru valsts vēlas sasniegt, nosakot šo ierobežojumu, proti – lai nodrošinātu efektīvu noziedzīgu nodarījumu izmeklēšanu, kriminālvajāšanu un krimināllietu iztiesāšanu. Ierobežojot Satversmes 96.pantā paredzētās tiesības, valstij jānodrošina kontrole pār to, lai šīs tiesības nebūtu nepamatoti aizskartas. ESL paredzēto saglabājamo datu atklāšana aizskar personas privātās dzīves noslēpumu, bet ne tik būtiski kā gadījumos, kad tiek atklāta personas korespondence. ESL paredzētie dati neatklāj personas paustās informācijas saturu, tāpēc izmeklēšanas tiesneša vai Augstākās tiesas tiesneša kontrole pār šādu datu pieprasīšanu ir

[85] http://www.tiesibsargs.lv/lat/tiesibsargs/jaunumi/?doc=162

nesamērīga un prasa no valsts nesamērīgu finanšu un cilvēkresursu ieguldījumu, kā arī mazina iespējas tiesībsargājošām iestādēm veikt *Kriminālprocesa likumā* paredzētos uzdevumus samērīgos termiņos. Turklāt šādā aspektā nav saprotama jēga atšķirīgajai reglamentācijai kriminālprocesā un operatīvās darbības procesā.

Šā jautājuma sakarā Latvijā 2008.gadā tika izveidota darba grupa *Elektronisko sakaru likuma* pilnveidei, kurā apspriests arī minētais jautājums. Latvijā nav nostiprinājusies vienota izmeklēšanas prakse ESL definēto «saglabājamo datu» ieguvei kriminālprocesā, saskaņā ar ESL 71.[1] panta nosacījumiem un ņemot vērā KPL 192.panta normu.

Autors te vēlas uzsvērt, ka ESL 1.pantā ir nepārprotami definēti «saglabājamie dati»,[86] norādot, ka tie neiekļauj personas korespondenci, un ESL 71.[1] pantā noteikts pienākums elektronisko sakaru tīkla operatoriem izsniegt šādus datus tiesībsargājošām iestādēm, turklāt ne par kādu tiesneša lēmumu nav runa un tā nav arī veidota kā blanketa norma, bet gan, gluži pretēji, šajā pantā ir reglamentēts, ka šie dati tiek nodoti tiesībsargājošām institūcijām «pēc to pieprasījuma».[87] Arī Ministru kabineta noteikumos,[88] kas reglamentē šādu datu izsniegšanas kārtību, nav prasība pēc tiesneša lēmuma.

Savukārt KPL 192.pantā noteikts, ka vienīgi ar tiesneša lēmumu kriminālprocesā var iegūt tādus datus, kas ir saglabāti KPL 191.panta kārtībā, kur var būt arī personas korespondence (tāpēc arī ir šis nosacījums par tiesneša lēmumu). KPL 191. un 192.pantā lietotais jēdziens «saglabātie dati» un ESL 1.pantā definētais un 71.[1] pantā lietotais jēdziens «saglabājamie dati» acīmredzami nav viens un tas pats. Tāpēc nav juridisks pamats pieprasīt tiesneša lēmumu tajos gadījumos, kad tiek pieprasīti dati saskaņā ar ESL 71.[1] pantu un nav piemērots KPL 191.pants. Neraugoties uz to, pēc viena Latvijas mobilo telekomunikāciju operatora noteiktas nostājas, ievērojot arī viedokļu apmaiņu, kas 2007.gadā norisinājās starp Valsts policiju, Ģenerālprokuratūru, Tieslietu ministriju un Tiesībsargu, Latvijas juridiskajā praksē tika ieviesta kārtība, ka visos gadījumos kriminālprocesa virzītājs pieprasa datus no elektronisko sakaru tīkla operatora tikai uz izmeklēšanas tiesneša lēmuma pamata. Ir gan redzēti arī izmeklēšanas tiesnešu argumentēti atteikumi pieņemt šādus lēmumus, kad policijas izmeklētājs vēršas ar tādu lūgumu, pēc kā elektronisko sakaru tīkla operators ir izsniedzis attiecīgos datus arī uz izmeklētāja vēstules pamata, vienlaikus norādot, ka nepiekrīt izmeklēšanas tiesneša argumentiem. Tādā veidā tad nu

[86] To saglabāšanas pienākumu uzliek ES Direktīva 2006/24/EK, pieņemta 2006.gada 15.martā. Latvijā saskaņā ar ESL 71.[1] p. (8) d. saglabājamie dati tiek saglabāti ESL 19. p. (1) d. 11. p. noteikto termiņu, proti – 18 mēnešus. Te gan jāpiebilst, ka 2010.gadā divi eiroparlamentārieši minēto ES Direktīvu ieteica papildināt, nosakot interneta pakalpojumu sniedzējiem pienākumu vismaz sešus mēnešus saglabāt arī visus vārdus, ar kuriem internetā meklēta informācija (tātad, ne tikai interneta pārlūkošanas savienojumu datus, bet arī satura datus). Vēl var norādīt, ka interneta meklētājs *Google* saglabā informācijas meklēšanas arhīvu 9 mēnešus, bet *Bing* – 6 mēnešus.

[87] Elektronisko sakaru likums. – [71.[1] panta (3) daļa]

[88] Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamos datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu. / Ministru kabineta noteikumi Nr. 820. Latvijas Vēstnesis Nr.197, 2007.gada 7.decembrī.

arī attīstas Latvijas juridiskā prakse, kad telekomunikācijas uzņēmums iebilst tiesībsargājošai iestādei un izmeklēšanas tiesnešiem par to, kā iztulkot likumu.

Ievērojot, cik ilgs ir izmeklēšanas tiesneša lēmuma ieguves process un cik būtiski dažkārt kriminālprocesā ir šādu datu ieguve pēc iespējas ātrākā termiņā, minētā kārtība, saskaņā ar autora viedokli, ir nesamērīga un vienpusēja cilvēktiesību interpretācija (atceroties, ka cilvēktiesības ir ne vien noziegumu izdarītājiem, bet arī tiem cilvēkiem, kuri var kļūt par noziegumos cietušajiem). Īpaši ņemot vērā, ka operatīvās darbības procesā, kur daudz biežāk tiek pieprasīti šādi dati, tāds nosacījums nepastāv.

Lai atrisinātu šo jautājumu, 2009.gadā Iekšlietu ministrija izstrādāja un 2010.gada 14.janvārī Saeima pieņēma (stājās spēkā 2010.gada 4.februārī) grozījumus KPL 192.pantā, nošķirot, ka bez tiesneša atļaujas pieprasa atklāt *Elektronisko sakaru likumā* noteiktajā kārtībā saglabājamos datus, savukārt pamatojoties uz izmeklēšanas tiesneša lēmumu (vai ar datu subjekta piekrišanu) pieprasa atklāt KPL 191.panta kārtībā saglabātos datus.

Runājot par samērīguma principu, var vēl pieminēt Eiropas Kopienu tiesas spriedumu lietā C-275/06,[89] kur jautājumā par personas datu izpaušanu autortiesību aizsardzības vajadzībām tiesa uzsvēra, ka ir jāpanāk līdzsvars starp intelektuālā īpašuma pamattiesībām un personas datu aizsardzību, tostarp interneta pakalpojumu sniedzējam nav pienākums izpaust personas datus civilprocesā, konkrētajā gadījumā – autortiesību pārkāpuma lietā. Minētajā spriedumā šajā aspektā ir uzsvērta atšķirība starp civilprocesu un kriminālprocesu.

Saistībā ar mobilo telekomunikāciju operatoriem lietderīgi norādīt uz problēmu, kas būtiski ietekmē iespējas novērst un arī atklāt mobilo telefonu zādzības un laupīšanas. Saskaņā ar ESL 46.panta (5) daļu un uz tā pamata izdotajiem Ministru kabineta noteikumiem Nr. 619,[90] kopš 2008.gada 1.janvāra Latvijas visi operatori uztur bloķēto IMEI kodu[91] datu bāzi, kurā iekļauj informāciju tikai par Latvijas operatoru abonentiem. Lai novērstu un atklātu mobilo telefonu zādzības, Apvienotās Karalistes un vēl vairāku valstu[92] operatori datus par attiecīgajiem mobilo telefonu IMEI iesniedz Centrālajā EIR jeb CEIR (*Central Equipment Identity Register*),[93] kas uztur t.s. «balto sarakstu» (visi IMEI kodi, kas ir piešķirti saražotajiem mobilajiem telefiniem un nav bloķēti), «pelēko sarakstu» (pārbaudē esošie IMEI kodi) un «melno sarakstu» (IMEI kodi, kuri ir bloķēti pēc paziņojuma par telefona nolaupīšanu vai nozaudēšanu). Latvijas operatori gan

[89] Productores de Música de España (Promusicae) v. Telefónica de España SAU. Judgment of the Court (Grand Chamber) in Case C-275/06. 29 January, 2008. – http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79919870C19060275&doc=T&ouvert=T&seance=ARRET

[90] Noteikumi par zudušu identificējamu elektronisko sakaru galiekārtu centralizētas datubāzes veidošanu, uzturēšanu un izmantošanu, kā arī šādu galiekārtu izmantošanas iespējas pārtraukšanu un atjaunošanu. / Ministru kabineta noteikumi Nr.619. Latvijas Vēstnesis Nr.160, 2007.gada 4.oktobrī.

[91] Miķelsons U. Noziedzīgu nodarījumu, kas saistīti ar mobilo tālruņu lietošanu, izmeklēšanas īpatnības: Monogrāfija – Rīga, Latvijas Policijas akadēmija, 2007. – 95 lpp.

[92] Apvienotā Karaliste, Beļģija, Čehija, Čīle, Dānija, Dienvidāfrikas Republika, Francija, Grieķija, Itālija, Īrija, Kenija, Kipra, Malta, Norvēģija, Portugāle, Somija, Spānija, Ungārija, Vācija, Zviedrija.

[93] Sk. http://www.gsmworld.com/using/security/index.shtml

nelieto starptautiskā CEIR pakalpojumus, līdz ar ko nav novērsta iespēja Latvijā zagtus un nolaupītus telefonus lietot citās valstīs, kā arī Latvijā lietot no citām valstīm ievestus zagtus mobilos telefonus.

Vēl viens diskutēts jautājums ir par to, vai būtu jānosaka aizdomās turētajiem un apsūdzētajam pienākums izsniegt kriptēšanas atslēgas, kad izmeklēšanas laikā tiek izņemts viņa dators vai cits informācijas nesējs. Šāds nosacījums nav nedz Latvijā, nedz arī citās valstīs, taču tiesību speciālisti norāda uz šīs problēmas risinājuma nepieciešamību. Te gan jāpiebilst, ka šāds pienākums nebūtu atbilstošs vispārējiem nosacījumiem, kas attiecas uz aizdomās turēto un apsūdzēto tiesībām, kā arī diez vai bieži būtu gadījumi, kad persona labprātīgi arī pateiktu pareizu kriptēšanas atslēgu tādā situācijā, kad viņa datorā var atrast informāciju, kas var iegūt pierādījuma nozīmi ar viņa izdarītu noziegumu.

Saistībā ar minēto var pieskarties citai problēmai – par tiesībām kriminālprocesa virzītājam (faktiski ekspertam, kurš veic datortehnisko ekspertīzi un tāpēc ir ierakstīts konkrētā kriminālprocesa reģistrā) pielietot tādas metodes, kas ļauj piekļūt kriptētai informācijai,[94] proti – "uzlauzt" šifrētas mapes un failus. No vienas puses, nav būtisku juridisku problēmu – ja kriminālprocesā ir juridiskas pilnvaras aizskart personas korespondences noslēpumu (tādas rodas vienmēr, kad tiesnesis pieņēmis lēmumu par kratīšanu, kuras gaitā paredzēts iegūt lietas, kas var saturēt arī personas sagatavotu informāciju), tad nav nekāda nozīme, vai attiecīgā informācija ir nekriptētā, kriptētā vai varbūt pat bojāta, normāliem līdzekļiem nelasāma faila formā. No otras puses, tādas metodes, ar kurām piekļūst kriptētai informācijai, nespeciālistiem var asociēties ar *hakeru* [95] darbībām, piemēram, kad lokālā tīkla *sniffer* [96] programmas pārtverti paroļu faili tiek dekriptēti, veicot paroles piemeklēšanu,[97] piemēram, pēc *hash* kolīziju[98] tabulām,[99] vai arī kad faili tiek dekriptēti, izmantojot šifrēšanas paroli, kura no personas datora iegūta ar *Trojan* tipa kaitīgu programmu[100] vai *XSS* metodi[101] utt. Faktiski tomēr dekriptēšanas metodes ir plaši pielietotas arī kriminālistikas apakšnozarē, kas attiecas uz datortehnisko ekspertīzi,[102] tajā skaitā ir izstrādāta dažāda, gan komerciāli, gan bez maksas izplatīta specializēta programmatūra,[103] kas pielāgota tieši tiesībsargājošo iestāžu ekspertu vajadzībām – datora cietā diska un citu

---

94 http://en.wikipedia.org/wiki/Cryptanalysis

95 http://en.wikipedia.org/wiki/Hacker_(computing)
Jāpiebilst, ka no visām personām, kuras nodarbojas ar IS apdraudējumiem, mazāk kā 10% ir *hakeri*, bet pārējie ir t.s. *script kiddies* jeb interneta vandāļi, kuriem nav dziļu zināšanu IT jomā, bet kuri lieto jau gatavu programmatūru IS ievainojamību izmantošanai.

96 http://en.wikipedia.org/wiki/Sniffer ; http://www.oxid.it/downloads/apr-intro.swf

97 http://en.wikipedia.org/wiki/Password_cracking

98 http://www.cryptography.com/cnews/hash.html ; http://en.wikipedia.org/wiki/Cryptographic_hash

99 http://www.freerainbowtables.com/ ; http://www.rainbowtables.net/

100 http://en.wikipedia.org/wiki/Trojan_horse_(computing)

101 http://en.wikipedia.org/wiki/Cross-site_scripting

102 http://en.wikipedia.org/wiki/Computer_forensics

103 http://www.sleuthkit.org/ ; http://www.forensics.nl/tools

informācijas nesēju izpētei, mobilo telefonu izpētei, datu ieguvei no strādājoša datora, lokāla datortīkla izpētei u.c. Lai gan sākotnēji var šķist, ka šīs divas jomas – *hakeru* darbības un ekspertīzes kriminālprocesā – ir nesavienojami jēdzieni, tomēr no tehniskā aspekta tās pārklājas, jo gan vieni, gan otri izmanto efektīvus IT līdzekļus un metodes informācijas ieguvei. Pamatatšķirība ir vien šo darbību nolūks un juridiskie apstākļi. Bez tam jāņem vērā, ka datu šifrēšanu dažkārt veic tādi cilvēki, kuri vēlas izvairīties no pierādījumu ieguves par viņu izdarītiem noziegumiem.

Var vēl piebilst, ka datoru, mobilo telefonu u.c. ierīču izpēti var veikt ne vien kriminālprocesuālas ekspertīzes ietvaros, bet arī kā operatīvo izpēti (*tomēr apzinoties, ka, sakarā ar ODL 12.panta (3) daļas normu, tas ir lietderīgi vien tad, ja nav paredzēts iegūt pierādījumus kriminālprocesā*). Bez tam šāda izpēte var būt veikta arī starptautiskas nozīmes izmeklēšanā. Piemēram, Interpol īpaša ekspertu vienība pētīja teroristiskās organizācijas FARC datorus, kas bija iegūti pēc 2008.gada 1.martā sekmīgi īstenotās policejiskās operācijas Kolumbijā, nolūkā neatkarīgi konstatēt, vai Kolumbijas varas iestādes ir izmainījušas kaut kādu informāciju šajos datoros pēc to atsavināšanas.[104]

Elektroniskas informācijas izpēte nolūkā iegūt elektroniskos pierādījumus kriminālprocesā (tāpat arī civilprocesā), ir no tehniskā un metodiskā viedokļa plašs un daudzpusīgs temats. To risina dažādas darba grupas gan starptautiskā, gan nacionālā mērogā, apspriež konferencēs un semināros, lietišķos pētījumos, un šajā jomā izstrādā dažādus tehniskos līdzekļus un programmatūru. Gan starptautiskā, gan vairākās valstīs arī nacionālā līmenī ir arī izstrādātas metodikas vadlīnijas elektronisko pierādījumu iegūšanai un izpētei,[105] un tādas izstrādātas arī Latvijā[106] (kaut gan jānorāda, ka šī joma pastāvīgi attīstās, tāpēc arī metodiskie ieteikumi pastāvīgi jāpilnveido). Tāpat arī Latvijā ir veikti pētījumi par IT noziegumu izmeklēšanu, izstrādājot metodiskos ieteikumus tiesībsargājošām iestādēm,[107] tajā skaitā 2007.gadā Latvijas Policijas akadēmijā tika veikts pētījums attiecībā uz noziedzīgiem nodarījumiem, kas saistīti ar mobilajiem telefoniem.[108]

Pateicoties autora ierosinājumam, *Kriminālprocesa likuma* 136.pantā arī ir iekļauts tāds

---

[104] Interpol's Forensic Report on FARC Computers and Hardware Seized by Colombia. May 2008. - http://www.interpol.int/Public/ICPO/PressReleases/PR2008/pdfPR200817/ipPublicReportNoCoverEN.pdf

[105] Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section. / Criminal Division. United States Department of Justice. July 2002. – http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

[106] Miķelsons U. Sākotnējās darbības ar informācijas tehnoloģiju saistītās lietās un datorekspertīzes noteikšanas metodika. – Rīga: LPA, 2000. – 35 lpp.
Sk. arī autora web lapu http://eksperts.gold.lv/gramatas.html

[107] Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas metodika: Monogrāfija. – Rīga: Biznesa augstskola Turība, 2003. – 387 lpp.
Miķelsons U. Elektronisko pierādījumu tiesiskie aspekti. // Latvijas Vēstneša izdevums «Jurista vārds», 2004.g., Nr. 12., 13., 14.

[108] Miķelsons U. Noziedzīgu nodarījumu, kas saistīti ar mobilo tālruņu lietošanu, izmeklēšanas īpatnības. – Rīga, Latvijas Policijas akadēmija, 2007. – 95 lpp.

pierādījumu veids kā elektroniskie pierādījumi: «Par pierādījumu kriminālprocesā var būt ziņas par faktiem elektroniskas informācijas formā, kas apstrādāta, uzglabāta vai pārraidīta ar automatizētas datu apstrādes ierīcēm vai sistēmām.» Līdz ar to nav juridisku šķēršļu Latvijā veikt šīs kategorijas noziegumu izmeklēšanu.

Šāda pieeja ir atbilstīga gan EP *Konvencijas par kibernoziegumiem* nosacījumiem, gan citu starptautisku dokumentu rekomendācijām, gan daudzu ārvalstu juridiskajai praksei. Piemēram, ASV tiesās[109] kā pierādījumus izmanto gan e-pasta vēstules, gan ierakstus web lapās, gan programmatūru, gan attēlus, videoierakstus, kas iegūti izņemtajā datorā, fotoaparātā, CD, DVD, zibatmiņā, videokasetē vai jebkādā citā informācijas nesējā, gan datu bāzu ierakstus, gan lietotāja gatavotus teksta dokumentus, gan grāmatvedības informāciju elektronisko tabulu failos, gan mobilā telefona atmiņā vai SIM (USIM / CSIM) kartē saglabātos ierakstus, utt. – nosacījumi elektronisko pierādījumu ieguvei ir tehnoloģiski neitrāli, tāpēc tie attiecas uz jebkādu datu formātu, tajā skaitā mūsdienās varbūt pat vēl nezināmu.

Elektronisko pierādījumu izmantošana kriminālprocesā atbilst arī ES Direktīvas 1999/93/EK[110] un *Elektronisko dokumentu likuma*[111] 3.panta nosacījumam: «[…] elektroniskā dokumenta kā pierādījuma iesniegšana kompetentām iestādēm nav ierobežojama, pamatojoties tikai uz to, ka 1) dokuments ir elektroniskā formā; 2) tam nav droša elektroniskā paraksta.»

Tomēr, tā kā jautājums par elektroniskiem pierādījumiem galvenokārt saistīts ar tehniskiem un metodiskiem aspektiem, tas iziet ārpus šās publikācijas mērķiem un netiek plašāk aplūkots.

Dažādu valstu tiesiskās reglamentācijas un juridiskās prakses harmonizācija ir ļoti būtiska, jo aizvien biežāk IT noziegumu izmeklēšana tiek veikta starptautiskas sadarbības veidā. To noteic ne vien datortīklu un telekomunikāciju tīklu pārrobežu raksturs, bet arī tas, ka mūsdienās daudzi cilvēki ceļo, līdzi ņemot portatīvos datorus un mobilos telefonus, ar kuriem veic konekcijas citu valstu elektronisko sakaru tīklos. Tāda izmeklēšana ir ne vien organizatoriski sarežģīta, bet dažkārt var arī nebūt sekmīga, ja, piemēram, politisku iemeslu dēļ netiek iegūts tiesiskās palīdzības atbalsts no valsts, kuras starpniekserveri[112] persona izmantojusi konekcijai, vai ja pēc starpniekservera izmantošanas ir izdzēsta informācija par attiecīgo konekciju.

Viens no pirmajiem pazīstamākajiem starptautiskas izmeklēšanas piemēriem ir t.s. Levina lieta, kuras izmeklēšanā sadarbojās sešu valstu tiesībsargājošās iestādes. Lieta tika ierosināta 1994.gada vasarā, kad vienas no pasaulē lielākās starptautiskās bankas *Citibank* Somijas filiāles darbinieks pamanīja patvaļīgas piekļūšanas mēģinājumu bankas tīklā, par ko tika paziņots ASV Federālajam izmeklēšanas birojam (FIB). Šo noziegumu veica personu grupa, kurā viens no galvenajiem tehniskajiem speciālistiem bija Sanktpēterburgas datorprogrammu firmas *Saturn* īpašnieks Vladimirs Levins. Viņš 1994.gadā laika posmā no 30.jūnija līdz 3.oktobrim ar bankas iezvanpieejas tīkla

[109] http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#_V_

[110] Eiropas Parlamenta un Padomes direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu. Oficiālais Vēstnesis L 013., 19.01.2000., 12. – 20.lpp.

[111] Elektronisko dokumentu likums. / Ar grozījumiem uz 2009.gada 22.oktobri. Latvijas Vēstnesis Nr.169, 2002.gada 20.novembrī.

[112] http://en.wikipedia.org/wiki/Proxy_server

starpniecību bija iekļuvis *Citibank* korporatīvajā tīklā un ar vismaz simts pieslēgšanās mēģinājumiem bankas datu bāzēm desmit valstu banku nodaļās, uzlaužot bankas drošības sistēmu, bija ieguvis kontu īpašnieku identifikācijas kodus, pēc kā bija nosūtījis 40 viltotus maksājuma uzdevumus par kopējo summu apt. 10,7 miljoni ASV dolāru uz iepriekš sagatavotiem banku kontiem Krievijā, Somijā, Vācijā, Holandē, Šveicē, Izraēlā un ASV. Kopumā nozieguma shēmā bija iesaistītas 14 valstis.
Šīs lietas izmeklēšanā bija iesaistīti visu minēto valstu tiesībsargājošo iestāžu pārstāvji, strādājot FIB vadībā un cieši sadarbojoties ar *Citibank* un citām iesaistītajām bankām, kā arī noziedzīgajā shēmā iesaistītajiem telekomunikāciju uzņēmumiem. Tikai šādas sadarbības dēļ, neraugoties uz daudzām tiesiskām un tehniskām grūtībām, izmeklēšanas galarezultātā tika noskaidroti visi noziedznieki un nozieguma apstākļi, kā arī atgūta lielākā daļa piesavinātās naudas. Vairāki līdzdalībnieki tika aizturēti naudas saņemšanas laikā dažādās valstīs, tajā skaitā ASV, Nīderlandē, Izraēlā. Kopumā tika arestētas 13 personas.
Šīs lietas izmeklēšanā uzmanību piesaistīja jurisdikcijas jautājums. Pēc pirmo līdzdalībnieku aizturēšanas jau bija aizdomas par Levinu, taču tajā laikā nepastāvēja tiesiskās palīdzības līgums par noziedznieku izdošanu starp ASV un Krieviju. Levins tika aizturēts 1995.gada 3.martā Londonas lidostā. 1995.gada augustā Londonā tiesa atlika Levina lietas izskatīšanu uz nenoteiktu laiku pēc tam, kad viņa advokāts apelācijā norādīja, ka viņš nozieguma izdarīšanai lietojis datoru, kas atradās nevis ASV, kur bija īstenots uzbrukums datorsistēmām, bet gan Krievijas teritorijā, kurā Levins nevienu IS nebija apdraudējis un kur tajā laikā pat nebija kriminalizēta patvaļīga piekļūšana IS. Tāda situācija nebija paredzēta Apvienotās Karalistes krimināla jā reglamentācijā, tāpēc ASV lūgums izdot viņiem Levinu krimināl vajāšanai netika izpildīts. Tomēr 1997.gada jūnijā Apvienotās Karalistes Lordu palāta noraidīja šo apelāciju un izdeva viņu ASV. 1998.gada 24.februārī Ņujorkas tiesā viņš tika notiesāts ar trīs gadiem brīvības atņemšanu un naudas sodu 240'000 ASV dolāru. *Citibank* apgalvoja, ka tā atguvusi visus nozagtos līdzekļus, izņemot apt. 400 tūkstošus ASV dolāru.
Te var piebilst, ka 2005.gadā (kad bija beidzies noilgums par šo noziegumu saskaņā ar ASV likumu)[113] interviju anonīmi sniedza kāds Sanktpēterburgas hakeris "ArkanoiD", kurš norādīja, ka Levinam nebija nedz speciālu zināšanu, nedz arī nepieciešamība tādas pielietot, lai piekļūtu Citibank tīklam, jo viņš bija vienkārši nopircis piekļuvei nepieciešamo informāciju no hakeriem, kuri bija atklājuši un izpētījuši šīs bankas tīkla ievainojamību. Tāpēc nav nekāda pamata Levinu uzskatīt par hakeri.[114] Intervijā "ArkanoiD" arī izklāstīja šī bankas tīkla tehniskās nepilnības, norādot gan, ka pēc nozieguma banka tās novērsa.

Svarīgi apzināties principu, ka kriminālprocesu veic tā valsts, kurā ir nodarīts kaitējums, neatkarīgi, vai attiecīga veida darbības ir kriminalizētas tajā valstī, kurā atradies nozieguma īstenotājs, vai kuras pilsonis viņš ir. Kriminālprocesa gaitā jau tiek nosūtīts tiesiskās palīdzības lūgums – par pierādījumu ieguvi, izdošanu utt. – tai valstij, no kuras teritorijas ir veikts noziegums un / vai kurā atrodas nozieguma izdarītājs, un šī valsts to var izpildīt. Tāda izpilde ir noteikti sagaidāma, ja starp abām valstīm pastāv vienošanās par tiesisko palīdzību.

Piemēram,[115] Apvienotās Karalistes (AK) iedzīvotājs Makinons (*Gary McKinnon*) no AK teritorijas 2001. un 2002.gadā bija sekmīgi veicis virkni ielaušanos ASV militāro un kosmisko institūciju datorsistēmās, lai aiz zinātkāres meklētu informāciju par citplanētiešiem, kas tajās varētu būt. Ar šīm darbībām viņš nebija pārkāpis nevienu AK likumu. Taču AK Augstākās tiesas Lordu palāta nolēma izpildīt ASV lūgumu par viņa izdošanu tiesāšanai. Šo AK nolēmumu atbalstīja arī Eiropas Cilvēktiesību tiesa, noraidot Makinona apelāciju.

Cits interesants piemērs[116] ir divu gados jaunu Čeļabinskas programmētāju Vasilija Gorškova un Aleksandra Ivanova lieta – viņi bija mantkārīgā nolūkā sekmīgi ielauzušies vairākās informācijas sistēmās ASV teritorijā, tajā skaitā tiešsaites maksājumu sistēmā *E-money*. 2000.gada 15.jūlijā Gorškovs ar e-pastu vērsās pie *E-money* prezidenta Džona Morgenšterna, pieprasot naudu – 500'000 dolārus par to, lai viņš nepubliskotu *E-money* klientu datubāzi, ieskaitot kredītkaršu datus, ko bija patvaļīgi ieguvis. Kad nākamajā dienā Gorškovs piezvanīja Morgenšternam, viņš uzsāka diskusiju par maksājamās nauda apjomu un turpmāk notikušajās sarunās Gorškovs pakāpeniski arī piekrita samazināt šo summu. Tomēr Morgenšterns aizvien vairāk centās pierunāt viņu, ka naudas vietā viņš – kā augstas klases datorspeciālists varētu iegūt labi apmaksātu darbu *E-money* uzņēmumā.
Faktiski šīs sarunas norisinājās FIB kontrolē, tomēr sarunu gaisotne kļuva aizvien draudzīgāka un Gorškovs aizvien vairāk sāka uzticēties Morgenšternam attiecībā uz tā darba piedāvājumu. Tā kā Krievijā pēc augstskolas pabeigšanas abiem jauniešiem nebija labas darba iespējas, viņi patiešām nosliecās braukt strādāt ASV. Un arī Morgenšterns sāka just līdzi šiem jauniešiem un pat lūdza FIB neaizturēt viņus, ja viņi tiešām iekārtosies legālā darbā.

[113] Computer Fraud and Abuse Act. (18 U.S.C. § 1030.) – http://www.law.cornell.edu/uscode/18/1030.html
[114] http://www.provider.net.ru/article.37.php
[115] http://news.bbc.co.uk/2/hi/uk_news/7585861.stm
[116] Russian Computer Hacker Convicted by Jury. / U.S. Department of Justice. October 10, 2001. – http://www.usdoj.gov/ criminal/cybercrime/gorshkovconvict.htm

Tomēr līdztekus šīm sarunām abi jaunieši vēl turpināja ar dažādām metodēm uzbrukumus citām informācijas sistēmām, tajā skaitā *Western Union, PayPal* un reģionālo banku finanšu sistēmām, kā arī izspiešanas saistībā ar to. Piemēram, *PayPal* vietnē izvietojot XSS skriptu, viņi savāca tās klientu e-pasta adreses, pēc tam uz sava servera izveidoja spoguļattēla kopiju šai vietnei ar maldinošu URL adresi – pēdējā burta mazā 'l' vietā viņi lietoja lielo 'I' – *PayPaI*. No šī vietnes viņi sūtīja e-pasta vēstules *PayPal* klientiem, piedāvājot dāvanu 50 dolāru vērtībā, kuras ieguvei tiem vajadzēja tikai ielogoties savā *PayPal* kontā. Kad viņi to darīja, tad hakeri vienkārši savāca viņu konta autorizācijas datus.

Tā kā Ivanovs bija sūtījis savu CV dažādiem IT uzņēmumiem ASV, tad FIB viņam nosūtīja uz e-pastu darba piedāvājumu fiktīva uzņēmuma *Invita Security* vārdā. Abi jaunieši aizbrauca uz ASV.

Kad viņi 2000.gada novembrī ieradās Sietlā, fiktīvā uzņēmuma darbinieki, faktiski FIB inspektori, lūdza viņiem ofisā nodemonstrēt savas prasmes IS uzlaušanā. Šīs demonstrēšanas laikā viņi no ofisā esošajiem datoriem arī konektējās pie sava servera Čeļabinskā, izmantojot sava paroles. FIB bija instalējis šajos datoros programmatūru, kas nolasīja visu no tastatūras ievadīto informāciju, līdz ar to šādā veidā FIB ieguva šo hakeru paroles. Tūlīt pēc demonstrēšanas viņi abi tika arestēti.

Par izdarītajiem noziegumiem Goršķovam draudēja pieci gadi brīvības atņemšanu par katru no pierādītajām 20 nozieguma epizodēm, kopumā 100 gadi, tomēr tiesa piesprieda tikai trīs gadus, kā arī 700'000 dolāru soda naudu. Savukārt Ivanovam trīs gadus, astoņus mēnešus brīvības atņemšanu un 800'000 dolāru soda naudu.

Izmeklēšanas gaitā FIB izmeklētājs Šulers (*Michael Schuler*), pamatojoties uz ASV tiesneša izdotu sankciju, izmantojot hakeru lietotās paroles, bija attālināti pārmeklējis informāciju viņu serverī Čeļabinskā un bija lejupielādējis hakeru izmantotās programmas, sūtītās vēstules ar naudas izspiešanām, vairāk kā 56'000 kredītkaršu numurus un citus informāciju par viņu veiktajiem noziegumiem, ko visu FIB izmantoja pierādīšanā. Par sekmīgo izmeklēšanu Šulers un viņa kolēģi vēlāk saņēma apbalvojumu.

Taču sakarā ar šādi veiktu izmeklēšanu sākās plašas juristu diskusijas, jo no Krievijas viedokļa FIB izmeklētājs bija veicis patvaļīgu piekļuvi serverim Krievijas teritorijā, proti – izdarījis noziegumu saskaņā ar Krievijas likumu, turklāt līdzīgu tam, par ko apsūdzēja Goršķovu un Ivanovu. Par to Krievijas Federālās izmeklēšanas dienests izvirzīja apsūdzību Šuleram, kas tika reģistrēta Krievijas kriminālās reģistrācijas IS. ASV Tieslietu ministrijai tika arī nosūtīta protesta nota, jo šādu metožu pielietošanas precedents var nozīmēt, ka nākotnē ASV pēc saviem ieskatiem ielaužas citu valstu informācijas sistēmās ar hakeru metodēm.

Šis jautājums – par pilnvarām iegūt informāciju, kas atrodas fiziski citas valsts teritorijā izvietotā datorā – ir ļoti būtisks. Valstu suverenitāte nedrīkst būt pārkāpta arī tad, kad tiek veikta noziegumu izmeklēšana. Tikai attiecīgās valsts kompetenta tiesību aizsardzības iestāde drīkst likuma noteiktā kārtībā iegūt informāciju no tās teritorijā esošas IS. Bet citas valsts tiesībsargājošā iestāde var vien vērsties ar tiesiskās palīdzības lūgumu pie šīs valsts institūcijas. Ja tiek veiktas patvaļīgas šādas darbības, tad tas robežojas ar valsts suverenitātes apdraudējumu, kas no starptautisko publisko tiesību viedokļa nav pieļaujams.

Tieši šādu jautājumu risināšanai ļoti būtiski, lai pēc iespējas visas valstis pievienotos EP *Konvencijai par kibernoziegumiem* vai līdzīga starptautiska dokumenta starpvalstu tiesiskās sadarbības nodrošināšanai.

Turklāt Kibernoziegumu konvencija risina ne vien juridiskos, bet arī praktiskos aspektus – tā paredz katrai dalībvalstij nodrošināt nepārtraukti pieejamu (24 stundas diennaktī 7 dienas nedēļā) kontakta centru, kur strādā juridiski pilnvaroti un tehniski sagatavoti cilvēki – nekavējošai tiesiskai palīdzībai elektronisku pierādījumu ieguvei. Konvencijā uzsvērts: «Dalībvalstij jāpārliecinās, ka ir pieejams pietiekami apmācīts un tehniski nodrošināts personāls nepieciešamo darbību veikšanai datortīklā». Latvijā, saskaņā ar šo konvenciju, 24/7 kontaktu centra funkcijas veic Valsts policijas Galvenās kriminālpolicijas pārvaldes Starptautiskā sadarbības pārvalde.

Šis darba virziens par 24/7 kontaktu centru izveidi, ko sākotnēji izvirzīja G8, un ko ievieš

Eiropas Padome, nav vienīgā šāda veida iniciatīva. Arī Interpol pastāvīgi strādā pie starptautiskās sadarbības praktisko aspektu pilnveides, tādā veidā organiski papildinot EP darbību kopēju vienotu mērķu sasniegšanā. Tajā skaitā Interpol ir izveidojis komunikācijas sistēmu «I-24/7», nodrošinot atbalstu IT noziegumu izmeklēšanā visām 188 dalībvalstīm.[117]

Vēl var piebilst, ka starptautisku sadarbību kibernoziegumu novēršanā atbalsta arī drošības incidentu reaģēšanas vienības CERT (*Computer Emergency Response Team*), kādas izveidotas daudzās valstīs uz valsts institūciju vai uzņēmumu bāzes, tajā skaitā Latvijā tādas ir faktiski divas – Latvijas universitātes Matemātikas un informātikas institūta Tīklu risinājumu daļas struktūrvienība[118] un [2010.gadā reorganizētās Valsts informācijas tīklu aģentūras] Datoru drošības incidentu reaģēšanas vienība.[119]

Bez tam ļoti būtiska ir ne vien sadarbība starp tiesībsargājošām iestādēm, bet arī sadarbība ar bankām, elektronisko sakaru tīklu operatoriem un citiem privātā sektora pārstāvjiem, kā arī – sevišķi bērnu pornogrāfijas izplatīšanas lietās – sabiedrības iesaistīšana. Nule minētajam mērķim kopš 1999.gada starptautiski tiek veicināta un daudzās valstīs, ieskaitot Latviju, arī nodrošināta *HotLine* iniciatīva jeb anonīmas ziņošanas sistēma par bērnu tiesību aizskāruma gadījumiem internetā.[120]

Starptautiskā mērogā veiktas policijas operācijas, cieši sadarbojoties gan ar interneta pakalpojumu sniedzējiem, gan ar banku sektoru, vairākkārt veiktas tieši bērnu pornogrāfijas izplatīšanas tīklu apkarošanai. Piemēram, 2006.gada maijā tādā operācijā tika vienlaikus veiktas kratīšanas 12 ES valstīs un ASV.

Bērnu pornogrāfijas izplatīšanas apkarošanai efektīva ir *HoneyPot* metodes pielietošana, proti – tādu maldinošu[121] web lapu izvietošana internetā, kurās par maksu tiek šķietami piedāvāts aplūkot bērnu pornogrāfiju, ko policija dara nolūkā konstatēt personas, kuras cenšas to darīt, veicot maksājumu no savas kredītkartes. Dažkārt gan ir publiskots viedoklis, ka šāda provokatīva metode nav pietiekami selektīva tieši pedofīlu noskaidrošanai, jo nevar izslēgt, ka policija fiksē arī tādus nejaušus šīs vietnes apmeklētājus, kuri ir meklējuši nevis bērnu pornogrāfiju, bet gan legāla veida pornogrāfiju, un pirms attēlu aplūkošanas vienkārši nav izlasījuši brīdinājuma uzrakstu, ka šajā vietnē pieejama tieši bērnu pornogrāfija. Līdz ar to diez vai konstatēts viens policijas *HoneyPot* vietnes apmeklējuma fakts var būt pietiekams pamats personas sodīšanai. Kaut arī daļēji tādam viedoklim var piekrist, tomēr nevar apšaubīt, ka šādas metodes pielietošana ir lietderīga šī nozieguma veida prevencijai.

---

117 http://www.interpol.int/public/ncb/i247/default.asp
118 http://cert.nic.lv/
119 http://www.ddirv.lv/
120 https://www.inhope.org/ ; http://www.netsafe.lv/pub/report.php
121 Latvijā veicot šādu pasākumu tas būtu juridiski jānoformē kā *operatīvais eksperiments* saskaņā ar ODL 15.pantu vai kā *speciālais izmeklēšanas eksperiments* saskaņā ar KPL 225.pantu.

Lai apkarotu bērnu pornogrāfijas izplatīšanu, jāvēršas pret tās pircējiem, tomēr vēl svarīgāk ir atklāt šādu attēlu un videoierakstu izgatavotājus, jo tas policiju var novest pie apdraudētajiem bērniem. Bet notvert bērnu pornogrāfijas radītājus nav vienkārši, jo no bildēm vien nereti nav nosakāms, kurš tās ir izgatavojis. ASV Nacionālās bērnu aizstāvības asociācijas izpilddirektors G.Vīks (*Grier Weeks*) norādīja, ka problēma ar tiešsaistes bērnu pornogrāfiju ir tā, ka tās vienkārši ir pārāk daudz. Pat četrkāršojot tiesībsargājošo institūciju spēkus, kas ar to cīnās, tie vienalga būtu pārslogoti. Tāpēc viņš vērsās pēc palīdzības pie pētniekiem Okridžas Nacionālajā laboratorijā, kur darbojas ASV superdators *Cry XT5 Jaguar*. Tajā ir uzsākts projekts, paredzēts uz gadu, kuram ir veltīts 1 miljons stundu *Jaguar* procesoru jaudas. Šīs laboratorijas pētnieks R.Patons (*Robert Patton*) izstrādājis algoritmus interneta trafika analīzei, lai pētītu meklējumus, kurus cilvēki veic internetā vienādranga tīklos. Ar šo algoritmu tiek atzīmēti tie meklējumi, kas attiecas uz bērnu pornogrāfiju, un algoritms analizē, kā dažādas IP adreses atsaucas uz šiem pieprasījumiem. Šāda analīze var dot iespēju tiesībsargājošām iestādēm konstatēt tos datorus, kuri ir jaunizveidotu bērnu pornogrāfijas materiālu izplatīšanas avots.[122]

Var piebilst, ka *HoneyNet* metode,[123] kad tiek maldinoši izveidots nepietiekami aizsargāts korporatīvs tīkls, kurā iekļauti *HoneyPot* resursi, savukārt, ir lietderīga hakeru aktivitāšu konstatēšanai. Tomēr šī metode biežāk gan tiek pielietota nevis nolūkā kriminālprocesā iegūt pierādījumus, kurus izskatītu tiesa, bet vispārīgai hakeru darbības metožu, taktikas un mērķu izpētei, lai pilnveidotu IS drošības tehnoloģijas kāda atsevišķa uzņēmuma vajadzībām. Efektīva *HoneyNet* izveidi un hakeru aktivitāšu prasmīgu automatizētu monitoringu un dokumentēšanu var īstenot tikai augsti kvalificēti IT speciālisti. Jānorāda arī, ka gadījumos, kad veikts uzbrukums *HoneyNet* resursiem, nebūs nodarīts reāls kaitējums, kas ir būtiski noziedzīga nodarījuma krimināltiesiskai kvalifikācijai. Līdz ar to konstatētās hakeru darbības šādā gadījumā var būt uzskatītas tikai par noziedzīga nodarījuma mēģinājumu, saskaņā ar *Krimināllikuma*[124] 15.pantu, bet tad diez vai var nešaubīgi konstatēt, ka ir noticis mēģinājums izdarīt tādu noziegumu, ar ko būtu nodarīts būtisks kaitējums.[125] Šāda problēma nebūtu, ja *Krimināllikuma* 241.pants – «Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai» – būtu veidots kā formāls sastāvs. Tomēr, ņemot vērā juridiskās prakses pakāpenisko attīstību IT noziegumu jomā, patlaban nevar izslēgt iespēju, ka šī metode tiek izmantota arī kriminālprocesā. Tādā gadījumā gan jānodrošina, lai IT speciālisti, kas dokumentējuši hakera aktivitātes, izskaidrotu tiesai saprotamā formā visu konstatēto informāciju, kam var būt nozīme noziedzīgā nodarījuma

[122] http://www.newscientist.com/article/dn19807-supercomputer-hunts-child-abusers.html

[123] Honeytraps, A Network Forensic Tool. Alec Yasinsac, Yanet Manzano. Department of Computer Science. Florida State University. – www.cs.fsu.edu/~yasinsac/Papers/MY02.pdf

[124] Krimināllikums. / Ar grozījumiem uz 2011.gada 1.janvāri. Latvijas Vēstnesis Nr. 199/200, 1998.gada 8.jūlijā.

[125] Būtisku kaitējumu definē likums „Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību" / Ar grozījumiem uz 2011.gada 1.janvāri. Latvijas Vēstnesis Nr. 331/332, 1998.gada 4.novembrī. – [23.pants]

apstākļu juridiskai izvērtēšanai.

Apskatot *HoneyNet* pielietojumu, var pieminēt arī kaut kādā ziņā līdzīgu metodi, kad tiesībsargājošā iestāde mērķtiecīgi izveido vietni, kuru savās interesēs apmeklē kibernoziedznieki, nolūkā dokumentēt šādu personu aktivitātes.

Piemēram, 2008.gada oktobra vidū sabiedrība uzzināja par ASV Federālā izmeklēšanas biroja operāciju – vietnes *DarkMarket.ws* administrēšanu, kurā ļoti aktīvi tika tirgota informācija par zagtām un viltotām kredītkartēm un banku kontiem, kā arī maksājuma karšu izgatavošanas ierīces utt. Šī vietne kādu laiku bija viena no populārākajām pasaulē šīs jomas noziedznieku (*carders*) vidū. Kopš 2006.gada novembra divus gadus šīs vietnes viens no administratoriem, kurš uzdevās par hakeri "Master Splynter", bija ASV FIB darbinieks Keith Mularski, kurš bija šādai juridiskai darbībai īpaši pilnvarots un sagatavots. Šī vietne tika slēgta vienlaikus ar 60 personu arestiem visā pasaulē, kuru identificējoša informācija, banku konti un noziedzīgā aktivitāte bija dokumentēta, izmantojot viņu uzticēšanos *DarkMarket.ws* vietnes administratoriem.

Kopumā no izskatītajiem jautājumiem ir skaidrs, ka IT noziegumu izmeklēšanas jomā viens no galvenajiem aspektiem ir dinamiska līdzsvara jeb samērīguma principa nodrošināšana, lai novērstu gan noziedzīgus apdraudējumus sabiedrībai, gan arī valsts institūciju varas pārmērīgu pielietošanu. Proti – cilvēktiesību pareiza piemērošana.

Nenoliedzami, ka strauji attīstoties informācijas tehnoloģijām, IT noziegumi aizvien vairāk ietekmēs sabiedrības dzīves visdažādākās jomas, aizvien biežāk radot nozīmīgu apdraudējumu sabiedrības tiesībām un interesēm, tāpēc ir ļoti būtiski pastāvīgi turpināt pētījumus par IT noziegumu izmeklēšanas metodiskajiem un tehniskajiem aspektiem, kā arī šīs jomas juridiskajiem jautājumiem, nolūkā nodrošināt tiesībsargājošās iestādes ar pietiekami labi sagatavotiem speciālistiem un metodiskām rekomendācijām, kā arī izveidot skaidru pamatu tiesību sistēmas pilnveidošanā šajā virzienā.

Normatīvo aktu un literatūras saraksts

1. Latvijas Republikas Satversme. / Pieņemta Latvijas Satversmes Sapulcē 15.02.1922., stājās spēkā 7.11.1922., ar grozījumiem uz 2.11.2010. Latvijas Vēstnesis Nr.43, 1.07.1993.
2. Eiropas Parlamenta un Padomes direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu. Pieņemta 13.12.1999., Oficiālais Vēstnesis L 013, 19.01.2000., 12. – 20.lpp.
3. ES Direktīvas 95/46/EK 29.panta darba grupas atzinums 2/2006. Par privātās dzīves aizsardzības jautājumiem, kas saistīti ar e-pasta caurlūkošanas pakalpojumiem. / 00451/06/LV. WP 118., pieņemts Briselē 21.02.2006. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_lv.pdf
4. Elektronisko dokumentu likums. / Pieņemts Saeimā 31.10.2002., stājās spēkā 1.01.2003., ar grozījumiem uz 22.10.2009. Latvijas Vēstnesis Nr.169, 20.11.2002.
5. Krimināllikums. / Pieņemts Saeimā 17.06.1998., stājās spēkā 1.04.1999., ar grozījumiem uz 1.01.2011. Latvijas Vēstnesis Nr.199/200, 8.07.1998.
6. Kriminālprocesa likums. / Pieņemts Saeimā 21.04.2005., stājās spēkā 1.10.2005., ar grozījumiem uz 1.01.2011. Latvijas Vēstnesis Nr.74, 11.05.2005.
7. Likums „Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību". / Pieņemts Saeimā 15.10.1998., stājās spēkā 5.11.1998., ar grozījumiem uz 1.01.2011. Latvijas Vēstnesis Nr.331/332, 04.11.1998.
8. Operatīvās darbības likums. / Pieņemts Saeimā 16.12.1993., stājās spēkā 13.01.1994., ar grozījumiem uz 1.01.2010. Latvijas Vēstnesis Nr.131, 30.12.1993.
9. Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamos datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu. / Ministru kabineta noteikumi Nr.820. Pieņemti 4.12.2007., stājās spēkā 8.12.2007. Latvijas Vēstnesis Nr.197, 7.12.2007.
10. Noteikumi par zudušu identificējamu elektronisko sakaru galiekārtu centralizētas datubāzes veidošanu, uzturēšanu un izmantošanu, kā arī šādu galiekārtu izmantošanas iespējas pārtraukšanu un atjaunošanu. / Ministru kabineta noteikumi Nr.619. Pieņemti 11.09.2007., stājās spēkā 1.01.2008. Latvijas Vēstnesis Nr.160, 4.10.2007.
11. Miķelsons U. Elektronisko pierādījumu tiesiskie aspekti // Jurista vārds, 2004.g., Nr. 12., 13., 14.
12. Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas metodika: Monogrāfija. – Rīga: Biznesa augstskola Turība, 2003. – 387 lpp.
13. Miķelsons U. Noziedzīgu nodarījumu, kas saistīti ar mobilo tālruņu lietošanu, izmeklēšanas īpatnības. – Rīga, Latvijas Policijas akadēmija, 2007. – 95 lpp.

14. Miķelsons U. Sākotnējās darbības ar informācijas tehnoloģiju saistītās lietās un datorekspertīzes noteikšanas metodika. – Rīga: LPA, 2000. – 35 lpp.
15. Vispārīgā politika cīņai ar kibernoziedzību / Eiropas Kopienu Komisijas paziņojums Eiropas Parlamentam, Padomei un Eiropas Reģionu Komitejai, Nr. COM (2007) 267, Briselē, 22.05.2007. – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LV:HTML
16. Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. / Permanent Council of the OEA/Ser.G. Organization of American States CP/CSH-635/04 rev. 2. 13 May 2004. Committee on Hemispheric Security. – http://scm.oas.org/doc_public/ENGLISH/HIST_04/CP12893E04.doc
17. Best Practices for Law Enforcement Interaction with Victim–Companies during a Cybercrime Investigation. Prepared by the G8's Subgroup on High-Tech Crime. June 17, 2005. – www.g8.utoronto.ca/justice/g8justice2005-practices.pdf
18. Cairo Declaration against Cybercrime. 27 November 2007. – http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity %20Cairo/CairoDeclarationAgainstCC2007_EN.pdf
19. Combating the criminal misuse of information technologies. UN Resolution 55/63, adopted by the General Assembly, 4 December 2000. – http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
20. Combating the criminal misuse of information technologies. UN Resolution 56/121, adopted by the General Assembly. 19 December 2001. – www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf
21. Computer Fraud and Abuse Act. (18 U.S.C. § 1030.) – http://www.law.cornell.edu/uscode/18/1030.html
22. Computers and International Criminal Law: High Tech Crimes and Criminals / By João Godoy - http://www.nesl.edu/intljournal/vol6/godoy.pdf
23. Convention on Cybercrime. Council of Europe. Budapest, 23 November 2001. – http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm ; http://www.likumi.lv/doc.php?id=146481

    Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Council of Europe. Strasbourg, 28 January 2003. – http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm ; http://www.likumi.lv/doc.php?id=146481
24. Foreign Intelligence Surveillance Act of 1978. ("FISA" Pub.L. 95-511, 92 Stat. 1783, enacted 1978-10-25, 50 U.S.C. ch.36.) - http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_36.html

25. Honeytraps, A Network Forensic Tool. Alec Yasinsac, Yanet Manzano. Department of Computer Science. Florida State University. – http://www.cs.fsu.edu/~yasinsac/Papers/MY02.pdf
26. Internet Intelligence : A three-day course at Cambridge University on How to use the internet as an Effective Investigative Research Tool : March 29 - 1 April 2009. International Chamber of Commerce. – http://www.icc-ccs.org/pdfs/II_2009_Brochure.pdf
27. Interpol's Forensic Report on FARC Computers and Hardware Seized by Colombia. May 2008. – http://www.interpol.int/Public/ICPO/PressReleases/PR2008/pdfPR200817/
28. Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME-Study / Prepared for the European Commission by Prof. Dr. Ulrich Sieber, University of Würzburg. 1st January 1998., 240 p. – http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf
29. Model Law on Computer and Computer Related Crime. Commonwealth Secretariat. Marlborough House, London. SW1Y 5HX. October 2002. – http://www.thecommonwealth.org/Internal/38061/documents/
30. Protect America Act of 2007. – http://www.govtrack.us/congress/billtext.xpd?bill=s110-1927
31. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section. Criminal Division. United States Department of Justice. July 2002. – http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm
32. Supreme Court of the United States. Hamdan v. Rumsfeld, Secretary of Defense, et al. Certiorari to the United States Court of Appeals for the District of Columbia Circuit. No. 05–184. Argued March 28, 2006. Decided June 29, 2006. - http://www.law.cornell.edu/supct/html/05-184.ZS.html
33. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. – http://epic.org/privacy/terrorism/hr3162.html
34. U.S. Department of Justice. Russian Computer Hacker Convicted by Jury. October 10, 2001. – http://www.usdoj.gov/ criminal/cybercrime/gorshkovconvict.htm
35. XVth International Congress of Penal Law. Rio de Janeiro, 4 – 10 September 1994. (J.L. De La Cuesta (ed.), Resolutions of the Congresses of the International Association of Penal Law (1926 – 2004). – www.penal.org/pdf/ReAIDP2007/RICPL.pdf
36. Leitsätzezum Urteil des Ersten Senats vom 27. Februar 2008. BUNDESVERFASSUNGSGERICHT. - 1 BvR 370/07. - 1 BvR 595/07. - http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
37. Productores de Música de España (Promusicae) v. Telefónica de España SAU. Judgment of the Court (Grand Chamber) in Case C-275/06. 29 January 2008. – http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79919870C19060275&doc=T&ouvert=T&seance=ARRET

Summary

In the article «Information technologies and criminal procedure» there are considered main practical, methodical and juridical aspects of the investigation of cybercrimes and various computer related crimes nowadays (according to situation in the autumn of 2010), taking into consideration the development of information technologies as well as wide and varied using them in society both in Latvian national level and in international level.

Аннотация

В статье «Информационные технологии и уголовный процесс» рассмотрены главные практические, методические и юридические аспекты расследования киберпреступлений и разнообразных с компютерамы связанных преступлений, учитывая ситуяцию осенъю 2010 года в области развития информационных технологий и широкого, разнообразного их применения в обществе, как на национальном уровне Латвии, так и на международном уровне.