

## 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.

Vēl iesākumā jānorāda šīs publikācijas mērķis – aplūkot kriminālprocesa attīstības pamataspektus IT noziegumu jomā. Tāpēc 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, ko pilnvērtīgi var izskatīt vien atsevišķā grāmatā.

Uzreiz jāuzsver, ka kriminālprocesa tiesību attīstība nenotiek tikpat strauji, kā IT<sup>1</sup> 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 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<sup>2</sup> 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<sup>3</sup> par bērnu

<sup>1</sup> 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.

<sup>2</sup> 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 uzteverei 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.

<sup>3</sup> <http://www.un-documents.net/a54r263.htm>

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) Konvencijas par kibernoziegumiem, kuras mērķis ir nodrošināt vienotu tiesību politiku šajā jomā visām dalībvalstīm (un vēl aizvien ne visās 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:

- 2008.gadā IBM superdators *Roadrunner* strādā ar ātrumu 1,026 petaflopī (kvadriljoni kalkulāciju sekundē). Datu pārraides ātrums optiskajā kabelī sasniedz 25,6 Tb/s (vairāk kā 600 DVD vienā sekundē) 80 km distancē; bet 1500 jūdžu jeb 2414 km distancē īstenota datu pārraide 16,4 Tb/s. *Cisco* izveido maršrutētāju datu pārraides ātrumam 92 Tb/s.
- Informācijas tehnoloģiju jomā tiek veikti zinātniski pētījumi saistīti gan ar kvantu fiziku nolūkā izstrādāt *kvantu datorus* un *kvantu sakarus sistēmas*, gan ar neirozinātnei 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*,<sup>4</sup> gan ar nanotehnoloģiju un biotehnoloģiju pētījumiem nolūkā izstrādāt *datorus uz bioloģisku sistēmu, t.sk. gēnu molekulas DNS bāzes* utt.<sup>5</sup>
- Tiek attīstīti līdztekus Internetam pastāvoši akadēmiskie un pētniecības datortīkli GÉANT2, Abilene jeb Internet2 Network, GLORIAD, JANET, CERNET u.c., dažādi Grid tīkli,<sup>6</sup> tajā skaitā ar semantiskā tīmekļa<sup>7</sup> tehnoloģiju, un arī militārām vajadzībām veidotais GIG (*Global Information Grid*) utt.
- Arī entuziasti attīsta dažādas tīklu tehnoloģijas, īpaši pievēršoties vienādranga (p2p) tīkliem, tajā skaitā Tor, Freenet, Turtle, WASTE, Entropy, anoNet, GNUnet, P-Grid,

<sup>4</sup> Tā kā mākslīgā intelekta izveide satricinātu tiesību sistēmu un arī sabiedrības pārvaldi pašos pamatos, turklāt ar neprognozējamām sekām, autors cer, ka viņam izrādīsies taisnība pārliecībā, ka mākslīgais intelekts faktiski nemaz nav iespējams. Katrā ziņā, I.Azimova 1942.gadā nosauktie trīs *robotu tiesību principi* ir ne vien pārāk primitīvi, bet arī nepiemēroti apstākļiem, kad pastāv īsts mākslīgais intelekts, tāpēc par tiem pat nav vērts runāt.

<sup>5</sup> Plašāk sk. <http://cordis.europa.eu/ist/fet/areas.htm>

<sup>6</sup> 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).

<sup>7</sup> Semantiskā tīmekļa (*semantic web*) tehnoloģijas mērķis ir padarīt tiešsaistē pieejamo decentralizēto un lielākoties nestrukturēto informāciju saprotamu ne tikai cilvēkiem, bet arī automatizētām 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 zinātnē jau piedāvā piemērotus risinājumus. Šī joma saistīta arī ar attēlu atpazīšanas tehnoloģiju pilnveidi.

XeroBank, Skype, Ripple tīkli u.c., kuros uzmanība būtiski pievērsta drošas un konfidencialas saziņas iespējām (dažkārt apzīmē *F2F* jeb *Friend-to-Friend*).

- 2008.gadā Internetu lieto gandrīz pusotrs miljards cilvēku pasaulē jeb apt. 22% cilvēces,<sup>8</sup> bet Eiropas Savienībā vairāk nekā puse iedzīvotāju regulāri lieto Internetu.<sup>9</sup> 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”,<sup>10</sup> tajā skaitā arī visdažādākā sadzīves tehnika un preces ar radiofrekvenču identifikatoriem RFID<sup>11</sup> var būt integrēti 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*.
- Aizvien ciešāk tiek saistītas datortīklu, mobilo telekomunikāciju un satelītsakaru tehnoloģijas, kā arī alternatīvās enerģijas avotu tehnoloģijas, nodrošinot elektronisko sakaru tīklu plašu pieejamību gan ģeogrāfiski, 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, personu elektroniskās identifikācijas datiem, ar ko apmaksā braucienus sabiedriskajā transportā, mobilo telefonu atrašanās vietas datiem, visiem publisko reģistru datiem, papildinot vēl ar pilnveidotu sejas atpazīšanas un automašīnu reģistrācijas numuru fiksēšanas tehnoloģiju, priekšmetu marķēšanu ar RFID vai GPS tehnoloģiju, kā arī dažādu speciālu 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).
- 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 bezmaksas piekļuves punkti

<sup>8</sup> <http://www.internetworldstats.com/>

<sup>9</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:LV:HTML>

<sup>10</sup> Turpat

rada nozīmīgu konkurenci komerciālām telekomunikāciju sistēmām. Bet *virtuālās naudas*<sup>12</sup> lietošana rada mulsinošus izaicinājumus finanšu sistēmām, tajā skaitā attiecībā uz cīņu pret naudas atmazgāšanu virtuālo spēļu vidē (tādās kā *Second Life*, *Entropia Universe* u.tml.)<sup>13</sup> un nodokļu iekasēšanu virtuālo lietu tirdzniecībā, juridiskiem aspektiem attiecībā uz *virtuālajiem noziegumiem*, piemēram, virtuālo spēļu pasaulē veiktām krāpšanām un zādībām,<sup>14</sup> vai pat jautājumus par virtuālās naudas ietekmi uz valsts centrālās bankas emitētās reālās naudas vērtības izmaiņām, utt.

- 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 pazīstamas Interneta tehnoloģijas, piemēram, Usenet, IRC, FTP, e-pasts jeb POP / SMTP, Telnet, tāpat kā jau ir novecojuši Gopher, BBS / FidoNet u.tml. (bet WWW pilnveido uz Web 2.0 vai pat Web 3.0, Web 4.0 jeb WebOS...).
- Daudzas agrāk izmantotas datu pārraides tehnoloģijas vairs netiek lietotas nepietiekamas to efektivitātes un arī drošības dēļ. 2007.gadā Interpol septītajā konferencē pat tika pausts viedoklis, ka mūsdienās ir lielāka iespēja personai kļūst par cietušo no IT nozieguma,<sup>15</sup> nekā no cita veida nozieguma.<sup>16</sup> Var piebilst atsevišķu speciālistu izteikto prognozi, ka ap 2012.gadu tiešsaites apdraudējumu, autortiesību pārkāpumu un mēstuļu problēmu dēļ

---

<sup>11</sup> Radio Frequency Identification. OECD Policy Guidance. A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008. – <http://www.oecd.org/dataoecd/19/42/40892347.pdf>

<sup>12</sup> Nejaukt ar *elektronisko naudu* jeb *digitālo naudu*, kas ir vien oficiālajā finanšu sistēmā lietotās naudas forma. 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.

<sup>13</sup> <http://en.wikipedia.org/wiki/MMORPG> ; <http://en.wikipedia.org/wiki/MMO>

<sup>14</sup> Piemēram, ASV policija atteicās uzsākt izmeklēšanu, kad 2008.gada februāra sākumā 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](http://www.ige.com). Policijas atteikumu šajā lietā asi kritizēja ievērojami ASV juristi. Savukārt Nīderlandē policija 2007.gada novembrī arestēja kādu 17 gadīgu jaunieci 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.

<sup>15</sup> IT noziegumu kategorija aptver vairāk kā 30 Latvijas Krimināllikumā iekļautos 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 netiek veikts.

Internets mums pazīstamā formā vispār vairs nepastāvēs, jo tas 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*<sup>17</sup> 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-business 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<sup>18</sup> Tūkstošgades projektā (*Millennium Project*). Eiropas Savienība 2005.gadā izskatīja «*Europe 2005 Action Plan*» rezultātus un pieņēma jaunu piecgades iniciatīvu *i2010 «A European Information Society for growth and employment»*.<sup>19</sup>

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, ir 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,<sup>20</sup> 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

---

<sup>16</sup> <http://www.interpol.int/Public/ICPO/speeches/India20070912.asp>

<sup>17</sup> Jēdziens «informācijas sabiedrība» tiek lietots kā vispārējs civilizācijas attīstību raksturojošs termins, kur cilvēku suga kultūras evolūcijā ir izgājusi cauri pirmatnējai sabiedrībai, agrrikulturālai sabiedrībai un industriālajai sabiedrībai, sasniedzot postindustriālās sabiedrības pakāpi, kad civilizācijas attīstību pamatā raksturo plaša IT izmantošana, «uz zināšanām balstīta ekonomika» (*knowledge economy*) utt.

<sup>18</sup> <http://www.itu.int/wsis/index.html>

<sup>19</sup> [http://ec.europa.eu/information\\_society/eeurope/i2010/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm)

<sup>20</sup> Piemēram, ASV valdība atļāva Pentagonam veidot *botnetu* kiberuzbrukumu veikšanai – tādā pašā veidā, kā to dara kibernoiedznieki. Savukārt pēc kiberuzbrukumiem ar botneta palīdzību 2006.gadā Igaunijai, vēlāk Gruzijai un Lietuvai, kas tika īstenots politisku motīvu dēļ, NATO atzina šāda veida apdraudējumu par līdzvērtīgu militāram raķešu triecienam.

noslēpuma neaizskaramību. Rietumvalstu sabiedrībā nereti tiek izplatīts negatīvs viedoklis par valstīm, kuras īsteno cenzūru Internetā, piemēram, Ķīnu, Kubu, Ziemeļkoreju, vairākām islāma valstīm u.c.<sup>21</sup> Tomēr cilvēktiesību aizstāvji kritizē cilvēktiesību apdraudējumu arī virknē demokrātisko rietumvalstu, piemēram, ASV valdības vēlmi papildus jau esošajām ASV iedzīvotāju saziņas totālas kontroles iespējām vēl arī bez tiesneša akcepta noklausīties ārvalstnieku telefona sarunas un kontrolēt elektronisko saziņu<sup>22</sup> (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).

No vienas puses ir ļoti liela sabiedrības daļa, kas cīnās par Interneta brīvību<sup>23</sup> jeb viedokļu<sup>24</sup> un informācijas plūsmas brīvību elektroniskā vidē, no otras puses ir arī ļoti spēcīgs politiskais un biznesa lobījs, 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,<sup>25</sup> 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,

<sup>21</sup> <http://opennet.net/>

<sup>22</sup> <http://www.aclu.org/legislative/index.html>

<sup>23</sup> [http://en.wikipedia.org/wiki/Internet\\_Freedom](http://en.wikipedia.org/wiki/Internet_Freedom)

<sup>24</sup> 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 kibernetiskajiem noziedzīgiem, 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.

<sup>25</sup> <http://www.itu.int/wsis/index.html>

par juridisko pilnvaru piešķiršanu ANO kompetencei – lietās, kas saistītas ar globālā datortīkla pārvaldīšanas funkcijām (*Internet Governance*).<sup>26</sup> Tam iebilda ASV, kuras Tirdzniecības ministrija ir noteicēja Interneta domēnu vārdu sistēmas uzturēšanā, un kurai ir veto tiesības attiecībā uz starptautiskās pārvaldes organizācijas ICANN<sup>27</sup> lēmumiem (tas faktiski nodarbojas ar šo jautājumu risināšanu), ievērojot arī, ka vairums DNS *root* serveru ir ASV uzņēmumu un augstskolu pārziņā. Šādu ASV nostāju atbalstīja arī Apvienotā Karaliste. Līdz ar to patlaban šis jautājums vairs netiek starptautiskā mērogā apspriests, tomēr nevar izslēgt, ka nākotnē starptautiskā sabiedrība var atgriezties pie tā, ja izmainīsies globālais politisko spēku samērs un IT jomas attīstība radīs tādus jaunus izaicinājumus, kuru risinājums būs iespējams vienīgi ciešas starptautiskas sadarbības ceļā.

Tiesībsargājošo iestāžu pret darbība 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 pret darbības stratēģija IT noziegumiem savieno – (a) tiesību aizsardzību, (b) tehnoloģiskos un (c) tirgus attiecību risinājumus. Jāpiebilst gan, ka jebkādā aspektā pret darbība 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,<sup>28</sup> OECD,<sup>29</sup> G8,<sup>30</sup> NATO,<sup>31</sup> Interpols,<sup>32</sup> Europols,<sup>33</sup> Eiropas Padome,<sup>34</sup> ES,<sup>35</sup> EK,<sup>36</sup> Eiropas

<sup>26</sup> <http://www.wgig.org/> ; <http://www.internetgovernance.org/>

<sup>27</sup> <http://www.icann.org/>

<sup>28</sup> 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](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](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf)

<sup>29</sup> 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. 16<sup>th</sup> December 2005. – <http://www.oecd.org/dataoecd/16/27/35884541.pdf>

<sup>30</sup> 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](http://www.g8.utoronto.ca/justice/g8justice2005-practices.pdf)

<sup>31</sup> [http://www.nato.int/issues/cyber\\_defence/index.html](http://www.nato.int/issues/cyber_defence/index.html)

<sup>32</sup> <http://www.interpol.int/Public/TechnologyCrime/default.asp>

<sup>33</sup> <http://www.europol.europa.eu/index.asp?page=news&news=pr061124.htm>

<sup>34</sup> [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default\\_en.asp](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp)

<sup>35</sup> <http://europa.eu/scadplus/leg/en/lvb/l33193b.htm> ; <http://www.enisa.europa.eu/>

<sup>36</sup> Vispārīgā politika cīņai ar kibernetiskā drošību / 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>

drošības un sadarbības organizācija (OSCE),<sup>37</sup> Baltijas jūras valstu padome (CBSS),<sup>38</sup> Starptautiskā tirdzniecības palāta (ICC),<sup>39</sup> Starptautiskā sodu tiesību asociācija (IAPL),<sup>40</sup> Pasaules intelektuālā īpašuma organizācija (WIPO),<sup>41</sup> Starptautiskā telekomunikāciju savienība (ITU),<sup>42</sup> Amerikas valstu organizācija (OAS),<sup>43</sup> Nāciju Sadraudzība (*The Commonwealth of Nations*),<sup>44</sup> Āzijas – Klusā okeāna sadarbības organizācija (APEC),<sup>45</sup> Arābu valstu līga<sup>46</sup> u.c.,<sup>47</sup> 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 U.Sībers (*Ulrich Sieber*) savā pētījumā<sup>48</sup> norādīja, ka nedz Eiropā, nedz arī ASV un Kanādā, nemaz nerunājot par citām valstīm, nav pietiekami efektīvas tiesiskās bāzes cīņai ar kibernetiskajiem. Vēl aizvien tiek turpināta tiesiskā reglamentācijas pilveide gan tajās valstīs, kur šis darbs uzsākts pirms vairākiem gadiem, gan tajās, kur tikai mūsdienās sāk risināt šo problēmu.

1981.gada decembrī Interpol Ģenerāļsekretariāts organizēja pirmo apmācības semināru par datornoziedzību atklāšanu, bet 1995.gadā notika Interpol pirmā starptautiskā konference par datornoziedzību, kurā piedalījās 49 valstu tiesību aizsardzības iestāžu un citu valstisku un privātu

<sup>37</sup> 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](http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf)

<sup>38</sup> <http://www.cbss.st/baltinfo/2005/dbaFile9297.html>

<sup>39</sup> 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](http://www.icc-ccs.org/pdfs/II_2009_Brochure.pdf)

<sup>40</sup> 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](http://www.penal.org/pdf/ReAIDP2007/RICPL.pdf)

<sup>41</sup> 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>

<sup>42</sup> <http://www.itu.int/cybersecurity/>

<sup>43</sup> 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](http://scm.oas.org/doc_public/ENGLISH/HIST_04/CP12893E04.doc)

<sup>44</sup> Model Law on Computer and Computer Related Crime. Commonwealth Secretariat. Marlborough House, London. SW1Y 5HX. October 2002. - <http://www.thecommonwealth.org/Internal/38061/documents/>

<sup>45</sup> Lima Declaration / The Sixth APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN6). 1-3 June, 2005. Lima, Peru. – [http://www.apec.org/apec/ministerial\\_statements/sectoral\\_ministerial/telecommunications/2005.html](http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005.html)

<sup>46</sup> Cairo Declaration against Cybercrime. 27 November 2007. - [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007\\_EN.pdf](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf)

<sup>47</sup> <http://www.first.org/>

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 dotortehnoloģiju attīstību. Lielākajā daļā valstu tiesību aizsardzības iestādēm tas ir jauns noziedzības veids, kuram tās ne vienmēr ir sagatavotas. Arvien lielāku izplatību gūst starptautiskas ar datoriem saistītas noziedzības fakti. Īpaši starp šiem noziegumiem jāpiemin krāpšana, nelikumīgi iegūtu līdzekļu legalizācija, datorvīrusu izplatīšana, neautorizēta iekļūšana starptautiskās informācijas sistēmās un informācijas zādzības. 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 cīnītos ar šiem noziegumiem. Pamatiemesls tam ir apstākļi, ka lielākajā daļā valstu likumdošana attīstījās, pirms radās datornoiedzības problēma, turklāt normatīvās bāzes pilnveidošana ir lēns process.

Šajā sakarā var minēt piemēru<sup>49</sup> – Argentīnas iedzīvotājs J.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 J.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.<sup>50</sup> Šāda veida noziegumus Argentīnā kriminalizēja tikai 2008.gada jūlija sākumā, pēc trīs gadus ilgušām debatēm parlamentā.

1992.gadā OECD izstrādāja «Informāciju sistēmu drošības vadlīnijas»,<sup>51</sup> 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

---

<sup>48</sup> 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. 1<sup>st</sup> January 1998., 240 p. - <http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone64-12Dirittimanipaesieextracom/DonneAfghanistan/Desktop/sieber.pdf>

<sup>49</sup> Computers and International Criminal Law: High Tech Crimes and Criminals / By João Godoy - <http://www.nesl.edu/intljournal/vol6/godoy.pdf>

<sup>50</sup> <http://news.bbc.co.uk/1/hi/world/americas/1932191.stm>

<sup>51</sup> 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](http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_1_1_1_1,00.html)

līgumu pieņemšanu, tostarp nosacījumus: kriminālai, 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 publicēja jau pilnveidotas vadlīnijas šajā jomā,<sup>52</sup> bet 2005.gadā – to veicinošu programmu.<sup>53</sup>

1995.gadā pēc ASV Federālā Izmeklēšanas biroja Datornoziedzumu 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 noziedzumu 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.

1997.gada 10.decembrī tika noslēgta vienošanās starp G8 valstīm – ASV, Kanādu, Apvienoto Karalisti, Vāciju, Franciju, Itāliju, Krieviju un Japānu par ciešu sadarbību IT noziedzumu izmeklēšanā. Saskaņā ar to, balstoties uz G8 Lionas – Romas Progresīvo tehnoloģiju noziedzības apkarošanas grupas rekomendācijām, dalībvalstis vienojās pilnībā atbalstīt citā valstī notikuša IT noziedzuma 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 noziedzumu 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 samītā 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

<sup>52</sup> 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](http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html)

<sup>53</sup> 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. 16<sup>th</sup> December 2005. – <http://www.oecd.org/dataoecd/16/27/35884541.pdf>

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.<sup>54</sup> 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.

Savukārt Eiropas Savienība izveidojusi pastāvīgi darbojošos Eiropas tīklu un informācijas drošības aģentūru (ENISA)<sup>55</sup> 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. Bez tam 2008.gada oktobrī ES izlēma veidot visām 27 ES dalībvalstīm kopīgu informācijas sistēmu, kurā reģistrēs nelegālas darbības Internetā un informāciju par aizdomās turētajām personām šādos noziegumos. Šo IS izveidos un uzturēs Europol. Tā uzturēs arī vietni, kur jebkura persona varēs ziņot par nelikumīgu saturu Interneta lapās. ES arī atbalstīs dalībvalstu vietējās IS, kas būs saistītas ar centrālo Eiropas IS.

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)<sup>56</sup> 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

<sup>54</sup> <http://www.un.org/events/10thcongress/2088h.htm>

<sup>55</sup> <http://www.enisa.europa.eu/>

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,<sup>57</sup> kas stājās spēkā 2004.gada 1.jūlijā. 2003.gadā tai tika pievienots papildus protokols par neiecietības nodarījumiem.<sup>58</sup> 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. 2008.gada septembrī tā bija stājusies spēkā kopumā 23 valstīs, bet tikai parakstījušas to bija vēl 22 valstis.<sup>59</sup> 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 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.<sup>60</sup>

Ja pasaulē būs valstis, kuras nesadarbosies ar citām kibernoziegumu izmeklēšanā, tad, diemžēl, netiks īstenots ANO aicinājums nepieļaut “drošas debesis” kibernoziegumiem, 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.

---

<sup>56</sup> [www.coe.int/T/E/Legal\\_Affairs/Legal\\_co-operation/Steering\\_Committees/Cdpc/](http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Steering_Committees/Cdpc/)

<sup>57</sup> 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>

<sup>58</sup> 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>

<sup>59</sup> <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>

<sup>60</sup> <http://www.newsland.ru/News/Detail/id/238312/>

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

Ratificējot šo konvenciju, arī Latvijas Kriminālprocesa likumā (KPL)<sup>61</sup> 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 regulētas speciālās izmeklēšanas darbības, kas saistītas ar sakaru līdzekļu kontroli, elektroniskajā informācijas sistēmā esošo datu kontroli, pārraidīto datu satura kontroli, atsevišķi regulēti nosacījumi informācijas ieguvei no elektroniskās informācijas sistēmas, kā arī definēti elektroniskie pierādījumi. Bez tam, atsevišķā KPL sadaļā 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 pietiekami efektīva kriminālprocesuālā regulējuma IT noziegumu izmeklēšanai.

Tomēr tas nenozīmē, ka šīs jomas tiesiskās regulējuma 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 regulējuma attīstība turpinās.

Piemēram, jautājums, 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 ieguvei datorsistēmās, ko pieļauj EP Konvencija par kibernetiskajiem.) var būt slēpti aizskarts tikai attiecīgas valsts jurisdikcijā un tikai ar tiesneša atļauju. Tomēr ne visas valstis strikti pieturas pie tieši šādas regulējuma.

Piemēram, atšķirīga nostāja ir ASV prezidenta administrācijai un Augstākajai tiesai, no kuras 2006.gada sprieduma Hamdan v. Rumsfeld lietā<sup>62</sup> izrietēja, ka ASV Konstitūcijai neatbilst 2002.gada saskaņā ar Patriot Act<sup>63</sup> izdots ASV prezidenta Dž.Buša 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

---

<sup>61</sup> Kriminālprocesa likums / Latvijas Republikas likums. Pieņemts Saeimā 21.04.2005., spēkā ar 01.10.2005., publicēts "Latvijas Vēstnesis" Nr. 74. (3232.), 11.05.2005.

<sup>62</sup> 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>

<sup>63</sup> 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>

parakstīja likumu,<sup>64</sup> 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<sup>65</sup> grozījumus, kas turpina iepriekšējo kārtību. Līdzīgi Zviedrijā 2008.gada jūnijā tika pieņemts likums<sup>66</sup> (stāsies spēkā 2009.gada janvārī), kas atbilst 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 septembra beigās Zviedrijas valdība gan paziņoja, ka grasās mīkstināt šī likuma regulējumu, ņemot vērā plašos sabiedrības protestus. 2008.gada 27.februārī Vācijas Konstitucionālā tiesas spriedums,<sup>67</sup> 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.

Aplūkotā jautājuma būtība saistīta arī ar to, ka pastāv diezgan efektīvas tehnoloģijas,<sup>68</sup> kas var veikt elektronisko sakaru *monitoringu* pēc noteiktiem atslēgvārdiem automatizētā režīmā, bet tas nav savienojams ar tiesneša akcepta ieguvī, 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. Ievērojot terorisma draudu līmeni mūsdienās, var domāt, ka diskusijas par šo jautājumu tomēr 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<sup>69</sup> 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<sup>70</sup> noteikto kārtību – speciālās izmeklēšanas darbības kriminālprocesuālā vai sevišķā veidā veicamās operatīvās

<sup>64</sup> Protect America Act of 2007. - <http://www.govtrack.us/congress/billtext.xpd?bill=s110-1927>

<sup>65</sup> 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](http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_36.html)

<sup>66</sup> [http://en.wikipedia.org/wiki/FRA\\_law](http://en.wikipedia.org/wiki/FRA_law)

<sup>67</sup> Leitsätze zum 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](http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html)

<sup>68</sup> Tādas kā *Echelon*, t.s. *Frenchelon*, *Onyx*.

<sup>69</sup> Latvijas Republikas Satversme / Latvijas Republikas pamatlikums. Pieņemts Latvijas Satversmes Sapulcē 15.02.1922., spēkā ar 07.11.1922., publicēts "Latvijas Vēstnesis" Nr. 43., 01.07.1993.

<sup>70</sup> Operatīvās darbības likums / Latvijas Republikas likums. Pieņemts Saeimā 16.12.1993., spēkā ar 13.01.1994., publicēts "Latvijas Vēstnesis" Nr. 131., 30.12.1993.

darbības pasākumus operatīvās darbības procesā, tajā skaitā sakaru līdzekļu kontroli, elektroniskajā informācijas sistēmā esošo datu kontroli, pārraidīto datu satura kontroli pieļaujams veikt vienīgi smagu un sevišķi smagu noziegumu lietās, ierobežotu laika periodu, kriminālprocesā ar izmeklēšanas tiesneša lēmumu, bet operatīvās darbības procesā ar īpaši pilnvarota Augstākās tiesas tiesneša sankcionētu lēmumu.<sup>71</sup>

Par pilnvarojuma jautājumu diskusijas Latvijā nav, tomēr tādas ir par to, vai nebūtu lietderīgi pieļaut veikt speciālās izmeklēšanas darbības arī mazāk smagu noziegumu lietās,<sup>72</sup> ievērojot, ka arī šādi noziegumi bieži rada nozīmīgu apdraudējumu sabiedrībai, bet to izmeklēšana nereti ir sarežģīta.<sup>73</sup>

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 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 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 faktiski nesniedz nekādu informāciju par fizisko personu, īpaši jau tāpēc, ka, piemēram, konkrēto zvanu varēja veikt ne

---

<sup>71</sup> 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 atšķirīgi 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 nereti pat nesaprot šo nošķirtību starp izmeklēšanu un kriminālmeklēšanu, kas Latvijā un citās valstīs ir pārmantota no t.s. sociālistiskās tiesību tradīcijas.

<sup>72</sup> Noziedzīgu nodarījumu smagums tiek noteikts pēc Krimināllikumā attiecīgā pantā noteiktās sankcijas.

<sup>73</sup> Šo priekšlikumu KPL izstrādāja LR Prokuratūras Metodikas nodaļa un publicēja ģenerālprokurors J.Maizītis pārskatā par Prokuratūras darbu 2007.gadā. - [http://www.lrp.gov.lv/doc\\_upl/Maizisa\\_runa\\_13.02.2008.doc](http://www.lrp.gov.lv/doc_upl/Maizisa_runa_13.02.2008.doc)

vien konkrētam numuram reģistrētais lietotājs, bet arī pavisam cita persona, kas ar numura lietotāja atļauju vai varbūt pat bez viņa ziņas lietojusi konkrēto telefona aparātu, vai arī konkrēto e-pastu varēja nosūtīt persona, kuram lietotājs atļāvis pasēdēt pie viņa datora. Protams, praktiski tas nav tik viennozīmīgi, jo, pirmkārt, dati, kas nepieciešami lietotāja identificēšanai, ir fizisko personu dati, kurus aizsargā speciāls likums,<sup>74</sup> 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.<sup>75</sup>

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<sup>76</sup> (ESL), 2007.gada jūlijā – septembrī tāda diskusija bija starp Valsts policijas, Tieslietu ministrijas, Ģenerālprokuratūras pārstāvjiem un Tiesībsargu.

Tiesībsarga birojs publicēja<sup>77</sup> šādu, no līdz tam pastāvējušās 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 neatliekamajos gadījumos iestādes ir

<sup>74</sup> Fizisko personu datu aizsardzības likums / Latvijas Republikas likums. Pieņemts Saeimā 23.03.2000., spēkā ar 20.04.2000., publicēts "Latvijas Vēstnesis" Nr. 123./124. (2034./2035.), 06.04.2000.

<sup>75</sup> To izsniegšana, saskaņā ar MK noteikumiem Nr 820., tiek ieviesta tikai ar 2009.gada 15.martu.

<sup>76</sup> Elektronisko sakaru likums / Latvijas Republikas likums. Pieņemts Saeimā 28.10.2004., spēkā ar 01.12.2004., publicēts "Latvijas Vēstnesis" Nr. 183. (3131.), 17.11.2004.

<sup>77</sup> <http://www.vcb.lv/index.php?open=viedoklis&this=190907.302>

tiesīgas pieprasīt saglabājamus 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 savu 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 legītīmam 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 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.<sup>1</sup> panta nosacījumiem un ņemot vērā KPL 192.panta normu.

Autors te vēlas uzsvērt, ka ESL 1.pantā ir nepārprotami definēti «saglabājamie dati»,<sup>78</sup> norādot, ka tie neiekļauj personas korespondenci, un ESL 71.<sup>1</sup> 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 blanketā norma, bet gan, gluži pretēji, šajā pantā ir reglamentēts, ka šie dati tiek nodoti tiesībsargājošām institūcijām «pēc to pieprasījuma».<sup>79</sup> Arī Ministru kabineta noteikumos,<sup>80</sup> kas reglamentē šādu datu izsniegšanas

<sup>78</sup> To saglabāšanas pienākumu uzliek ES Direktīva 2006/24/EK, pieņemta 2006.gada 15.martā. Latvijā saskaņā ar ESL 71.<sup>1</sup> p. (8) d. saglabājamie dati tiek saglabāti ESL 19. p. (1) d. 11. p. noteikto termiņu, proti – 18 mēnešus.

<sup>79</sup> Elektronisko sakaru likums / Latvijas Republikas likums. Pieņemts Saeimā 28.10.2004., spēkā ar 01.12.2004., redakcijā uz 30.09.2008., publicēts "Latvijas Vēstnesis" Nr. 183. (3131.), 17.11.2004. – [71.<sup>1</sup> panta (3) daļa.]

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.<sup>1</sup> 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.<sup>1</sup> pantu un nav piemērots KPL 191.pants. Neraugoties uz to, pēc viena Latvijas mobilo telekomunikāciju operatora neatlaidīgas nostājas, ievērojot arī viedokļu apmaiņu, kas 2007.gadā norisinājās starp Valsts policiju, Ģenerālprokuratūru, Tieslietu ministriju un Tiesībsargu, Latvijas juridiskajā praksē tiek ieviesta kārtība, ka visos gadījumos kriminālprocesa virzītājs pieprasa datus no elektronisko sakaru tīkla operatora tikai uz izmeklēšanas tiesneša lēmuma pamata. Autors gan ir redzējis vairākus izmeklēšanas tiesnešu argumentētus atteikumus pieņemt šādus lēmumus, kad policijas izmeklētājs vērsas ar tādu lūgumu, pēc kā elektronisko sakaru tīkla operators izsniedz attiecīgos datus arī uz izmeklētāja vēstules pamata, vienlaikus norādot, ka nepiekrīt izmeklēšanas tiesneša argumentiem. Tāda nu pašlaik ir Latvijas prakse, kad telekomunikācijas uzņēmums norāda tiesībsargājošai iestādei un izmeklēšanas tiesnešiem, kā, viņuprāt, jāiztulko likuma normas.

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.

Runājot par samērīguma principu, var vēl pieminēt Eiropas Kopienu tiesas spriedumu lietā C-275/06,<sup>81</sup> 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

---

<sup>80</sup> Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamus datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu. / Ministru kabineta noteikumi Nr. 820. Pieņemti MK 04.12.2007., spēkā ar 08.12.2007., publicēti "Latvijas Vēstnesis" Nr. 197. (3773), 07.12.2007.

<sup>81</sup> 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>

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,<sup>82</sup> kopš 2008.gada 1.janvāra Latvijas visi operatori uztur bloķēto IMEI kodu<sup>83</sup> datu bāzi, kurā iekļauj informāciju tikai par Latvijas operatoru abonentiem. Lai novērstu un atklātu mobilo telefonu zādzības, Apvienotās Karalistes un vēl vairāku valstu<sup>84</sup> operatori iesniedz datus par attiecīgajiem mobilo telefonu IMEI Centrālajā EIR jeb CEIR (*Central Equipment Identity Register*),<sup>85</sup> kas uztur t.s. «balto sarakstu» (visi IMEI kodi, kas ir piešķirti saražotajiem mobilajiem telefoniem 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 līdz šim nelieto un arī neplāno lietot 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, apzinoties, ka viņa datorā var atrast informāciju, kas var iegūt pierādījuma nozīmi viņa krimināllietā.

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,<sup>86</sup> proti – “uzlauzt” šifrētas mapes un failus. No vienas puses, nav nekādu 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

<sup>82</sup> 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 MK 11.09.2007., spēkā ar 01.01.2008., publicēti “Latvijas Vēstnesis” Nr. 160. (3736.), 04.10.2007.

<sup>83</sup> Miķelsons U. Noziedzīgu nodarījumu, kas saistīti ar mobilo tālrunu lietošanu, izmeklēšanas īpatnības: Monogrāfija – Rīga, Latvijas Policijas akadēmija, 2007. – 95 lpp.

<sup>84</sup> Apvienotā Karaliste, Beļģija, Čehija, Čīle, Dānija, Dienvidāfrikas Republika, Francija, Grieķija, Itālija, Īrija, Kenija, Kipra, Malta, Norvēģija, Portugāle, Somija, Spānija, Ungārija, Vācija, Zviedrija.

<sup>85</sup> Sk. <http://www.gsmworld.com/using/security/index.shtml>

<sup>86</sup> <http://en.wikipedia.org/wiki/Cryptanalysis>

metodes, ar kurām piekļūst kriptētai informācijai, nespeciālistiem varbūt asociējas ar *hakeru*<sup>87</sup> darbībām, piemēram, kad lokālā tīkla *sniffer*<sup>88</sup> programmas pārtverti paroļu faili tiek dekriptēti, veicot paroles piemeklēšanu,<sup>89</sup> piemēram, pēc *hash* kolīziju<sup>90</sup> tabulām,<sup>91</sup> vai arī kad faili tiek dekriptēti, izmantojot šifrēšanas paroli, kura no personas datora iegūta ar *Trojan* tipa kaitīgu programmu<sup>92</sup> vai *XSS* metodi<sup>93</sup> utt. Faktiski tomēr dekriptēšanas metodes ir plaši pielietotas arī kriminālistikas apakšnozarē, kas attiecas uz dator tehnisko ekspertīzi,<sup>94</sup> tajā skaitā ir izstrādāta dažāda, gan komerciāli, gan brīvi izplatīta specializēta programmatūra,<sup>95</sup> kas pielāgota tieši tiesībsargājošo iestāžu ekspertu vajadzībām – datora cietā diska un citu 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 jānorāda, ka datu šifrēšanu nereti veic tieši 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.<sup>96</sup>

Elektroniskas informācijas izpēte nolūkā iegūt elektroniskos pierādījumus kriminālprocesā (tāpat arī civilprocesā), ir no tehniskā un metodiskā viedokļa ļoti plašs un sarežģīts temats,<sup>97</sup> kā arī diezgan īpatnējs juridiskā aspektā. To risina daudzas darba grupas

<sup>87</sup> [http://en.wikipedia.org/wiki/Hacker\\_\(computing\)](http://en.wikipedia.org/wiki/Hacker_(computing))

Jāpiebilst, ka no visām personām, kuras nodarbojas ar IS uzlaušanu, mazāk kā 10% ir hakeri, bet pārējie ir t.s. *script kiddies* jeb pusaudži, kuriem nav dziļu zināšanu IT jomā, bet kuri lieto jau gatavu programmatūru IS ievainojamību izmantošanai.

<sup>88</sup> <http://en.wikipedia.org/wiki/Sniffer> ; <http://www.oxid.it/downloads/apr-intro.swf>

<sup>89</sup> [http://en.wikipedia.org/wiki/Password\\_cracking](http://en.wikipedia.org/wiki/Password_cracking)

<sup>90</sup> <http://www.cryptography.com/cnews/hash.html> ; [http://en.wikipedia.org/wiki/Cryptographic\\_hash](http://en.wikipedia.org/wiki/Cryptographic_hash)

<sup>91</sup> <http://www.freerainbowtables.com/> ; <http://www.rainbowtables.net/>

<sup>92</sup> [http://en.wikipedia.org/wiki/Trojan\\_horse\\_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))

<sup>93</sup> [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

<sup>94</sup> [http://en.wikipedia.org/wiki/Computer\\_forensics](http://en.wikipedia.org/wiki/Computer_forensics)

<sup>95</sup> <http://www.crime-research.ru/library/resource.htm/> ; <http://www.sleuthkit.org/> ; <http://www.forensics.nl/tools>

<sup>96</sup> 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>

<sup>97</sup> 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>

starptautiskā un nacionālā mērogā, apspriež konferencēs un semināros, pētī speciālos pētījumos un izklāsta publikācijās, kā arī šajā jomā izstrādā dažādus tehniskos līdzekļus un programmatūru. Gan starptautiskā, gan vairākās valstīs arī nacionālā līmenī ir jau izstrādātas vadlīnijas elektronisko pierādījumu iegūšanai un izpētei, un tādas izstrādātas arī Latvijā<sup>98</sup> ( 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,<sup>99</sup> tajā skaitā 2007.gadā Latvijas Policijas akadēmijā tika veikts pētījuma attiecībā uz noziedzīgiem nodarījumiem, kas saistīti ar mobilajiem telefoniem.<sup>100</sup>

Ievērojot šī jautājuma plašumu, te tas netiek atsevišķi aplūkots. Var vien piebilst, ka pateicoties autora ierosinājumam Latvijas Kriminālprocesa likuma 136.pantā ir iekļauts tāds 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 kibernetiskajiem noziedzīgiem nodarījumiem, gan citu starptautisku dokumentu rekomendācijām, gan daudzu ārvalstu juridiskajai praksei. Piemēram, ASV tiesās<sup>101</sup> 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 kartē saglabātos ierakstus, utt. – nosacījumi elektronisko pierādījumu ieguvei ir tehnoloģiski neitrāli, tāpēc tie attiecas uz jebkādu datu formātu, tajā skaitā arī mūsdienās varbūt vēl nezināmu.

Elektronisko pierādījumu izmantošana kriminālprocesā atbilst arī ES Direktīvas 1999/93/EK<sup>102</sup> un Elektronisko dokumentu likuma<sup>103</sup> 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.»

<sup>98</sup> 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>

<sup>99</sup> 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.

<sup>100</sup> Miķelsons U. Noziedzīgu nodarījumu, kas saistīti ar mobilo tālrunu lietošanu, izmeklēšanas īpatnības: Monogrāfija – Rīga, Latvijas Policijas akadēmija, 2007. – 95 lpp.

<sup>101</sup> [http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#\\_V\\_](http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#_V_)

<sup>102</sup> Eiropas Parlamenta un Padomes direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu. Pieņemta 13.12.1999., publicēta "Oficiālais Vēstnesis" L 013., 19.01.2000., 0012. – 0020.lpp.

Dažādu valstu tiesiskās reglamentācijas un juridiskās prakses harmonizācija ir ļoti būtiska, jo aizvien biežāk IT noziegumu izmeklēšana tiek veikta starptautiskā mērogā. To nosaka ne vien datortīklu un telekomunikāciju tīklu pārrobežu raksturs, bet arī tas, ka mūsdienās daudzi cilvēki ceļo, līdzīgi 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<sup>104</sup> persona izmantojusi konekcijai, vai ja pēc starpniekservera izmantošanas ir izdzēsta informācija par attiecīgo konekciju.

Kā viens no 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 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 viņu, taču tajā laikā nepastāvēja tiesiskās palīdzības līgums par noziedznieku izdošanu starp ASV un Krieviju. V. Levins tika aizturēts 1995.gada 3.martā Londonas lidostā. 1995.gada augustā Londonā tiesa atlika V. Levina lietas izskatīšanu uz nenoteiktu laiku pēc tam, kad viņa advokāts apelācijā norādīja, ka viņš nozieguma

---

<sup>103</sup> Elektronisko dokumentu likums / Latvijas Republikas likums. Pieņemts Saeimā 31.10.2002., spēkā ar 01.01.2003., publicēts "Latvijas Vēstnesis" Nr. 169. (2744.), 20.11.2002.

izdarīšanai lietojis datoru, kas atradās nevis ASV, kur bija īstenots uzbrukums datorsistēmām, bet gan Krievijas teritorijā, kurā V.Levins nevienu IS nebija apdraudējis un kur tajā laikā pat nebija kriminalizēta patvaļīga piekļūšana IS. Tāda situācija nebija paredzēta Apvienotās Karalistes kriminālajā reglamentācijā, tāpēc ASV lūgums izdot viņiem V. Levinu kriminālvajāšanai 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)<sup>105</sup> interviju anonīmi sniedza kāds Sanktpēterburgas hakeris "Arkanoid", kurš norādīja, ka V.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 V.Levinu uzskatīt par hakeri.<sup>106</sup> Intervijā "Arkanoid" arī izklāstīja šī bankas tīkla tehniskās nepilnības, norādot gan, ka pēc nozieguma banka tās novērsa.

Attiecībā uz Internetā veiktiem noziegumiem, kuriem ir pārrobežu raksturs (*piemēram, valsts «A» pilsonis, būdams valsts «B» pastāvīgs iedzīvotājs, veicis noziegumu valstī «C», izmantojot Interneta konekcijas caur IP adresēm, kas ir valstīs «D», «E» utt.*), 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 ieguvī, 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 tad, ja starp attiecīgajām abām valstīm pastāv vienošanās par tiesisko palīdzību.

Piemēram,<sup>107</sup> Apvienotās Karalistes (AK) iedzīvotājs G.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 G.Makinona apelāciju.

Cits interesants piemērs<sup>108</sup> ir divu gadus jaunu Čeļabinskas programmētāju Vasilija

---

<sup>104</sup> [http://en.wikipedia.org/wiki/Proxy\\_server](http://en.wikipedia.org/wiki/Proxy_server)

<sup>105</sup> Computer Fraud and Abuse Act. (18 U.S.C. § 1030.) – <http://www.law.cornell.edu/uscode/18/1030.html>

<sup>106</sup> <http://www.provider.net.ru/article.37.php>

<sup>107</sup> [http://news.bbc.co.uk/2/hi/uk\\_news/7585861.stm](http://news.bbc.co.uk/2/hi/uk_news/7585861.stm)

<sup>108</sup> U.S. Department of Justice. Russian Computer Hacker Convicted by Jury. October 10, 2001. – <http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm>

Gorškova un Aleksandra Ivanova lieta – viņi bija mantkārīgā nolūkā sekmīgi ielauzušies vairākās informācijas sistēmās ASV teritorijā, tajā skaitā tiešsaistes maksājumu sistēmā *E-money*. 2000.gada 15.jūlijā V.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 V.Gorškovs piezvanīja Dž.Morgenšternam, viņš uzsāka diskusiju par maksājamās nauda apjomu un turpmāk notikušajās sarunās V.Gorškovs pakāpeniski arī piekrita samazināt šo summu. Tomēr Dž.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 V.Gorškovs aizvien vairāk sāka uzticēties Dž.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 Dž.Morgenšterns sāka just līdzīgu sajūtu šiem jauniešiem un pat lūdza FIB neaizturēt viņus, ja viņi tiešām iekārtosies legālā darbā.

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 'P' – *PayPal*. 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 A.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 izmeklētāji, 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 V.Gorškovam 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 A.Ivanovam trīs gadus, astoņus mēnešus brīvības atņemšanu un 800'000 dolāru soda naudu.

Izmeklēšanas gaitā FIB izmeklētājs M.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 M.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 V.Gorškovu un A.Ivanovu. Par to Krievijas Federālās izmeklēšanas dienests izvirzīja apsūdzītu M.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 kibernetiskajiem noziegumiem, kas veidota kā starptautisks dokuments starpvalstu tiesiskās sadarbības nodrošināšanā.

Turklāt ne vien juridiskos aspektus, bet arī praktiskos – šī konvencija paredz katrai dalībvalstij nodrošināt nepārtraukti pieejamu (24 stundas diennaktī 7 dienas nedēļā) kontakta centru, kur strādā juridiski pietiekami pilnvaroti un tehniski sagatavoti cilvēki – nekavējošai tiesiskai palīdzībai elektronisku pierādījumu ieguvei. Konvencijā uzsvērts: «Dalībvalstij jāpārlicinās, 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. Piemēram, 2008.gadā Interpol ir izveidojis apakšvienības IT noziegumu izmeklēšanas atbalstam jau 111 valstīs pasaulē.

Vēl var piebilst, ka starptautisku sadarbību kibernetiskā drošībā 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 (LU MII) Tīklu risinājumu daļas struktūrvienība<sup>109</sup> un Valsts informācijas tīklu aģentūras (VITA) Datoru drošības incidentu reaģēšanas vienība.<sup>110</sup>

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.<sup>111</sup>

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<sup>112</sup> 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 legālu pieauguša cilvēka 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 tādām viedoklim var piekrist, tomēr nevar apšaubīt, ka šādas metodes pielietošana ir lietderīga šī nozieguma veida prevencijai.

Var piebilst, ka *HoneyNet* metode, kad tiek maldinoši izveidots nepietiekami aizsargāts korporatīvs tīkls, kurā iekļauti *HoneyPot* resursi, savukārt, ir lietderīga hakeru aktivitāšu konstatēšanai. Tomēr šī metode ārvalstīs lielākoties tiek pielietota nevis nolūkā kriminālprocesā iegūt pierādījumus, kurus izskatītu tiesa, bet gan vispārīgai hakeru darbības metožu, taktikas un mērķu izpētei, lai pilnveidotu IS drošības tehnoloģijas kāda atsevišķa uzņēmuma vajadzībām.

---

<sup>109</sup> <http://cert.nic.lv/>

<sup>110</sup> <http://www.ddirv.lv/>

<sup>111</sup> <https://www.inhope.org/> ; <http://www.netsafe.lv/pub/report.php>

Efektīva *HoneyNet* izveidi un hakeru aktivitāšu prasmīgu automatizētu monitoringu un dokumentēšanu var īstenot tikai augsti kvalificēti IT speciālisti.<sup>113</sup> 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<sup>114</sup> 15.pantu, bet tad diez vai var nešaubīgi konstatēt, ka ir noticis mēģinājums izdarīt tādu noziegumu, ar ko būtu nodarīts būtisks kaitējums.<sup>115</sup> 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 apstākļu juridiskai izvērtēšanai.

Apskatot *HoneyNet* pielietojumu, var pieminēt arī kaut kādā ziņā līdzīgu metodi, kad tiesībsargājošā iestāde mērķtiecīgi izveido vietni, kuru savās interesēs apmeklē kibernetoziedznieki, 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 bija viena no populārākajām visā pasaulē šīs jomas noziedznieku (*carders*) vidū. Kopš 2006.gada novembra šīs vietnes viens no administratoriem, kurš uzdevās par hakeri "Master Splynter", bija ASV FIB darbinieks Keith Mularski, kurš bija šai darbībai īpaši autorizēts un sagatavots. Šī vietne tika slēgta vienlaikus ar vairāku personu arestiem, kuru identificējoša informācija, banku konti un noziedzīgā aktivitāte bija dokumentēta, izmantojot viņu uzticēšanos šai *DarkMarket.ws* vietnei.

Kopumā no izskatītajām praktiskajām un juridiskajām problēmām 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 pielietojumu. Proti – cilvēktiesību pareiza piemērošana.

---

<sup>112</sup> 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.

<sup>113</sup> Honeytraps, A Network Forensic Tool. Alec Yasinsac, Yanet Manzano. Department of Computer Science. Florida State University. – [www.cs.fsu.edu/~yasinsac/Papers/MY02.pdf](http://www.cs.fsu.edu/~yasinsac/Papers/MY02.pdf)

<sup>114</sup> Krimināllikums / Latvijas Republikas likums. Pieņemts Saeimā 17.06.1998., spēkā ar 01.04.1999., publicēts "Latvijas Vēstnesis" Nr. 199./200. (1260./1261.), 08.07.1998.

<sup>115</sup> Būtisku kaitējumu definē likums: Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību. / Latvijas Republikas likums. Pieņemts Saeimā 15.10.1998., spēkā ar 05.11.1998., publicēts "Latvijas Vēstnesis" Nr. 331./332. (1392./1393.), 04.11.1998. – [23.pants]

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 / Latvijas Republikas pamatlikums. Pieņemts Latvijas Satversmes Sapulcē 15.02.1922., spēkā ar 07.11.1922., publicēts "Latvijas Vēstnesis" Nr. 43., 01.07.1993.
2. Eiropas Parlamenta un Padomes direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu. Pieņemta 13.12.1999., publicēta "Oficiālais Vēstnesis" L 013., 19.01.2000., 0012. – 0020.lpp.
3. Elektronisko dokumentu likums / Latvijas Republikas likums. Pieņemts Saeimā 31.10.2002., spēkā ar 01.01.2003., publicēts "Latvijas Vēstnesis" Nr. 169. (2744.), 20.11.2002.
4. Elektronisko sakaru likums / Latvijas Republikas likums. Pieņemts Saeimā 28.10.2004., spēkā ar 01.12.2004., publicēts "Latvijas Vēstnesis" Nr. 183. (3131.), 17.11.2004.
5. Fizisko personu datu aizsardzības likums / Latvijas Republikas likums. Pieņemts Saeimā 23.03.2000., spēkā ar 20.04.2000., publicēts "Latvijas Vēstnesis" Nr. 123./124. (2034./2035.), 06.04.2000.
6. Krimināllikums / Latvijas Republikas likums. Pieņemts Saeimā 17.06.1998., spēkā ar 01.04.1999., publicēts "Latvijas Vēstnesis" Nr. 199./200. (1260./1261.), 08.07.1998.
7. Kriminālprocesa likums / Latvijas Republikas likums. Pieņemts Saeimā 21.04.2005., spēkā ar 01.10.2005., publicēts "Latvijas Vēstnesis" Nr. 74. (3232.), 11.05.2005.
8. Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību / Latvijas Republikas likums. Pieņemts Saeimā 15.10.1998., spēkā ar 05.11.1998., publicēts "Latvijas Vēstnesis" Nr. 331./332. (1392./1393.), 04.11.1998.
9. Operatīvās darbības likums / Latvijas Republikas likums. Pieņemts Saeimā 16.12.1993., spēkā ar 13.01.1994., publicēts "Latvijas Vēstnesis" Nr. 131., 30.12.1993.
10. Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamus datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu / Ministru kabineta noteikumi Nr. 820. Pieņemti MK 04.12.2007., spēkā ar 08.12.2007., publicēti "Latvijas Vēstnesis" Nr. 197. (3773), 07.12.2007.
11. 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 MK 11.09.2007., spēkā ar 01.01.2008., publicēti "Latvijas Vēstnesis" Nr. 160. (3736.), 04.10.2007.
12. Ģenerālprokurora J.Maiziša pārskats par Prokuratūras darbu 2007.gadā. - [http://www.lrp.gov.lv/doc\\_upl/Maizisa\\_runa\\_13.02.2008.doc](http://www.lrp.gov.lv/doc_upl/Maizisa_runa_13.02.2008.doc)
13. Miķelsons U. Elektronisko pierādījumu tiesiskie aspekti // Latvijas Vēstneša izdevums «Jurista vārds», 2004.g., Nr. 12., 13., 14.
14. Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas metodika: Monogrāfija. – Rīga: Biznesa augstskola Turība, 2003. – 387 lpp.

15. Miķelsons U. Noziedzīgu nodarījumu, kas saistīti ar mobilo tālrunu lietošanu, izmeklēšanas īpatnības: Monogrāfija – Rīga, Latvijas Policijas akadēmija, 2007. – 95 lpp.
16. Miķelsons U. Sākotnējās darbības ar informācijas tehnoloģiju saistītās lietās un datorekspertīzes noteikšanas metodika. – Rīga: LPA, 2000. – 35 lpp.
17. Vispārīgā politika cīņai ar kibernetizāciju / 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>
18. 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](http://scm.oas.org/doc_public/ENGLISH/HIST_04/CP12893E04.doc)
19. 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](http://www.g8.utoronto.ca/justice/g8justice2005-practices.pdf)
20. Cairo Declaration against Cybercrime. 27 November 2007. – [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007\\_EN.pdf](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf)
21. 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](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf)
22. 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](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf)
23. Computer Fraud and Abuse Act. (18 U.S.C. § 1030.) – <http://www.law.cornell.edu/uscode/18/1030.html>
24. Computers and International Criminal Law: High Tech Crimes and Criminals / By João Godoy - <http://www.nesl.edu/intljournal/vol6/godoy.pdf>
25. 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>

26. 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](http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_36.html)
27. 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](http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf)
28. Honeytraps, A Network Forensic Tool. Alec Yasinsac, Yanet Manzano. Department of Computer Science. Florida State University. – [www.cs.fsu.edu/~yasinsac/Papers/MY02.pdf](http://www.cs.fsu.edu/~yasinsac/Papers/MY02.pdf)
29. 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](http://www.icc-ccs.org/pdfs/II_2009_Brochure.pdf)
30. 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>
31. 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. 1<sup>st</sup> January 1998., 240 p. - <http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone64-12Dirittumanipaesieextracom/DonneAfghanistan/Desktop/sieber.pdf>
32. Lima Declaration / The Sixth APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN6). 1-3 June, 2005. Lima, Peru. – [http://www.apec.org/apec/ministerial\\_statements/sectoral\\_ministerial/telecommunications/2005.html](http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005.html)
33. Model Law on Computer and Computer Related Crime. Commonwealth Secretariat. Marlborough House, London. SW1Y 5HX. October 2002. - <http://www.thecommonwealth.org/Internal/38061/documents/>
34. 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](http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_1_1_1_1,00.html)
35. 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](http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html)
36. Protect America Act of 2007. - <http://www.govtrack.us/congress/billtext.xpd?bill=s110-1927>
37. Radio Frequency Identification. OECD Policy Guidance. A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008. – <http://www.oecd.org/dataoecd/19/42/40892347.pdf>

38. 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>
39. 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>
40. 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. 16<sup>th</sup> December 2005. – <http://www.oecd.org/dataoecd/16/27/35884541.pdf>
41. 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>
42. U.S. Department of Justice. Russian Computer Hacker Convicted by Jury. October 10, 2001. – <http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm>
43. 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](http://www.penal.org/pdf/ReAIDP2007/RICPL.pdf)
44. 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>
45. Leitsätze zum 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](http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html)
46. 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 end of September, 2008), 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 компьютерами связанных преступлений, учитывая ситуацию в конце сентября 2008 года в области развития информационных технологий и широкого разнообразного их применения в обществе, как на национальном уровне Латвии, так и на международном уровне.