LATVIJAS UNIVERSITĀTE

JURIDISKĀ FAKULTĀTE

Krimināltiesisko zinātņu katedra

Bakalaura darbs

JURISDIKCIJA PAR NOZIEDZĪGIEM NODARĪJUMIEM KIBERTELPĀ

Autore: **Aleksandra Gavrilova**

Studenta apliecības Nr.: ag14059

Darba vadītāja: Dr.iur. Diāna Hamkova

RĪGA, 2017

ANOTĀCIJA

Kibernoziegumu attīstība aktualizē problēmas ar jurisdikcijas noteikšanu pār noziedzīgo nodarījumu. No valstīm piemītošās suverenitātes kā primārais izriet teritoriālais jurisdikcijas prinicps, tomēr, ņemot vērā kibernoziegumu šauro piesaisti kādai konkrētai teritrorijai, rodas problēmas ar principa piemērošanu. Ņemot vērā plašo iesaistīto personu loku un nekonkrēto teritoriju, ir neizbēgama situācija, kurā rodas jurisdikcijas konflikts.

Darba ietvaros tiks analizēti pastāvošie jurisdikcijas principi un to attiecināmība uz kibernoziegumiem, meklējot iespējamus risinājumus jurisdikcijas konfliktu gadījumos.

Atslēgvārdi: kibernoziegumi, jurisdikcijas principi, starptautiski noziegumi, kibertelpa.

ABSTRACT

Development of cybercrimes raises the issue of jurisdiction over the crimes. From sovereignty that belongs to the states deprives the territoriality principle of jurisdiction, however, taking into account the specifics of the cybercrimes, such as narrow connection with a territory, the application of the principle can be encumbered. Considering the wide range of people involved and unlimited territory, the situation of the conflict of jurisdictions is inevitable.

Within the research it is analyzed what kind of principles of jurisdiction exist and how they are applied to cybercrimes, trying to find a possible solutions in case of conflict of jurisdictions.

Key words: cybercrimes, principles of jurisdiction, international crimes, cyberspace.

SATURS

IEVADS

Jau 1984.gadā Apvienoto Nāciju Organizācijas kibernoziegumu eksperts, Norvēģijas "Mosbaret" tiesas priekšsēdētājs S. Sjolbergs rakstīja, ka termins "datornoziegums" kļūs par vienu no visbiežāk lietojamiem vārdiem 21. gadsimtā.[1]

Tēmas aktualitāti izceļ fakts, ka mūsdienu pasaules pastāvēšana vairs nav iedomājama bez interneta. Internets ir kļuvis par platformu praktiski visam – komunikācijai, datu apmaiņai, preču un pakalpojumu iegādei, naudas apmaiņai. Līdz ar interneta plašo attīstību ir neizbēgama arī tā izmantošana kā platforma noziedzīgu nodarījumu izdarīšanai. Kibernoziegumi ir noziegumi, kas ir vērsti pret jebkuru datu apstrādes sistēmu, planšeti, telefonu utt. – jebkādu ierīci, kur ir kāda informācija.

Likumi ir ievērojami attīstījušies un mainījušies laika gaitā, tomēr interneta attīstība liek vēl vairāk izmanīt daudzus līdz šim pieņemtus juridiskus konceptus. Lai gan ir nostiprināts uzskats, ka interneta vide juridiski ir jāaplūko tieši tāpat kā reālā vide, attiecinot uz to analogus tiesību principus[2], tomēr ir skaidrs, ka interneta vidē paveikti noziedzīgi nodarījumi un to kontrole ir liels izaicinājums mūsdienu tiesību sistēmām. Uzsverot, ka kiberdrošība ir mūsdienu nacionālās drošības centrālais jautājums [3] 2001.gadā tika pieņemtā Konvencija par kibernoziegumiem, kura regulē attiecināmos jurisdikcijas principus un valstu pienākumu sadarboties.

Kibernoziegumu anonimitāte, robežu nepastāvēšana un plašais iesaistīto personu loks raisa jautājumus par atbilstošas jurisdikcija piemērošanu, nosakot valsti, kura ir tiesīga vainīgo personu sodīt. Kā darba mērķi autore izvirza visu līdzšinējā praksē pastāvošo jurisdikcijas principu izpētīšanu un to analīzi kibernoziegumu kontekstā, nosakot, kuru principu piemērošana varētu visefektīvāk atrisināt kibernoziegumus.

---

[1] U. Ķinis. Kibernoziegumi un krimināprocess. Jurista Vārds, 20.02.2001., Nr. 4 (197).
[2] The working party on the protection of individuals with regard to the processing of personal data. Recommendation 3/97 Anonymity on the internet, adopted by working party, 3.December 1997. Pieejams: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf [aplūkots: 12.05.2017].
[3] Valstīm jāsaskaņo izmeklēšanas metodes cīņā pret kibernoziegumiem. Pieejams: https://eu2015.lv/lv/jaunumi/zinas/1136-valstim-jasaskano-izmeklesanas-metodes-cina-pret-kibernoziegumiem [aplūkots: 12.05.2017].

Darbs sastāv no trim daļām – jurisdikcijas principu analīzes, Latvijas un ārvalstu prakses attiecībā uz kibernoziegumiem, un Latvijas regulējuma kibernoziegumu jomā, kā arī jurisdikcijas konfliktiem.

Veicot pētījumu, izmantota salīdzinošā, vēsturiskā un analīzes zinātniski pētnieciskā metode. Salīdzinošā metode tika izmantota, salīdzinot jurisdikcijas principu tvērumu un konkrēto valstu pielietojumu nacionālajās tiesībās, Eiropas Savienības tiesībās un starptautiskajās tiesībās. Vēsturisko metodi autore izmantoja, apskatot jurisdikcijas principu attīstību laika gaitā un apskatot kibernoziegumu un to regulējumu attīstību. Ar analīzes zinātniski pētnieciskās metodes palīdzību autore analizēja pastāvošos jurisdikcijas konfliktus attiecībā pret kibernoziegumiem, pētot un noskaidrojot, to iespējamos risinājumus un problēmjautājumus.

Pētījumā autore izmantoja dažādas tiesību doktrīnas, normatīvos aktus, zinātniskos rakstus, interneta resursus un vadošo kibernoziegumu speciālistu viedokļus.

1. KRIMINĀLTIESISKĀS JURISDIKCIJAS VEIDI UN TO NOZĪME

Krimināltiesisko jurisdikciju definē kā suverēnas valsts spēju pieņemt likumus, kas paredz kriminālatbildību par noziedzīgiem nodarījumiem, un spēju šo likumu piemērot, saucot pie atbildības valsts teritorijā jebkuru personu, ja tās darbībā vai bezdarbībā saskatāmas noziedzīga nodarījuma pazīmes (*corpus delicti*), un tiesas piekritību šo lietu iztiesāšanā.[4] Jurisdikcijas realizēšanas nav iespējama bez valsts suverenitātes. Atbilstoši tiesību ekspertu atziņām, krimināltiesiskās jurisdikcijas doktrīnā ir plaši atzīts, ka krimināltiesisko jurisdikciju var iedalīt trīs līmeņu varas izpausmēs: 1) varu noteikt jurisdikciju (spēja izveidot un noteikt krimināla sankcijas), 2) varu spriest tiesu (noklausīties strīdu tiesā) un 3) varu piespriest sodu.[5]

Mūsdienu tiesību doktrīna paredz vairākus jurisdikcijas principus, un turpmākajās nodaļās autore tos analizēs detalizēti.

Starptautiskās tiesības atzīst starptautisko principu piemērošanu, kas ir nostiprinās arī Apvienoto Nācijas Organizācijas Starptautiskās tiesas statūtu 38. pantā, kurš paredz starptautisko principu piemērošanu strīdu risināšanā.[6] Starptautisko principu piemērošana paredz tādas lietas kā labticības principu, principu, kurš paredz, ka nevienu peronu nevar sodīt par vienu noziedzīgo nodarījumu vairāk nekā vienu reizi, kā arī principu, ka bez pastāvoša likumu nevienu personu nevar saukt pie atbildības.[7]

Runājot par Eiropas Savienība tiesībām attiecība uz jurisdikcijas principiem, ir skaidrs, ka tā seko starptautiskajiem principiem un kā primāro izvirza valsts suverenitāti.[8] Eiropas Savienībā kā primārais tiek izvirzīts teritoriālais jurisdikcijas princips, kas nozīmē, ka noziedzīgais nodarījums, kurš paveikts kādā no dalībvalstīm, nonāk šīs valsts jurisdikcijā.[9] Šis princips ir konkretizēts Direktīvas 2013/40/ES Par uzbrukumiem informācijas sistēmā 12.

---

[4] U.Ķinis. Jurisdikcija un kibernoziegumi. Apgāds "Jumava", Rīga, 2013., 18.lpp.

[5] Susan W.Brenner and Bert-Jaap Koops. "Approches to Cybercrime Jurisdiction",p.4. According to Ian Brownlie, Principles of Public International Law, 5th ed., Oxford, University Press, 2002 (1998), p.58.

[6] Rome Statute of the International Criminal Court. Pieejams: https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf [aplūkots: 14.05.2017].

[7] J.Klabbers. International law. Cambridge University Press, United Kingdom, 2013., p.34.

[8] S.Summers. The emergence of EU criminal law, cyber crime and the regulation of internet society. Oxford publishing, 2014., p.101.

[9] A. Klip. European Criminal law, 2nd edition. Cambridge, Intersentia, 2012., p.192.

pantā. Eiropas Savienības krimināltiesību "atbilde" uz uzplaukstošajiem kibernoziegumiem ir balstīta uz dalībvalstu krimināla regulējumu harmonizāciju.[10]

Turpmāk darbā autore detalizēti apskatīs, kādus jurisdikcijas veidus paredz Konvencija par kibernoziegumiem[11] (turpmāk tekstā "Konvencija par kibernoziegumiem"), tomēr autore uzsver, ka Direktīva 2013/40/ES paplašina konvencijā noteiktos jurisdikcijas veidus, paredzot situāciju, kad dalībvalsts var noteikt jurisdikciju pār noziedzīgo nodarījumu, kas izdarīts ārpus tās teritorijas, ja nodarījuma izdarītāja patstāvīgā dzīvesvieta ir dalībvalsts vai ja nodarījums ir izdarīts tādas juridiskās personas labā, kas veic uzņēmējdarbību valsts teritorijā.[12]

Jurisdikcijas īstenošana ir jāapskata neatrauti no *aut dedere aut judicare* (tiesā vai izdod) principa, kurš ir nostiprināts Konvencijas par kibernoziegumiem 22. panta trešajā daļā, kura uzliek Līgumslēdzējpusēm pienākumu veikt visus nepieciešamos pasākumus, lai nodibinātu jurisdikciju pār kibernoziegumiem. *Aut dedere aut judicare* ir viens no starptautisko tiesību principiem, kurš ir ieguvis paražas statusu[13], līdz ar to tā piemērošana neaprobežojas ar konvencijas ratificēšanu.

1.1. Teritoriālais princips un tā nozīme

Teritoriālais princips vistiešākajā veidā izriet no valsts suverenitātes pamatidejas. Valsts suverenitāte jau sākotnēji sevī ietver nosacījumu par valsts varas efektīvu kontroli pār savu suverēno teritoriju. Valsts realizē savu krimināltiesisko jurisdikciju attiecībā uz noziegumiem, kuri ir veikti tās teritorijā, attiecīgi persona tiks pakļauta tās valsts jurisdikcijai, kurā tā veiks noziedzīgu nodarījumu.

Saskaņā ar Krimināllikuma (turpmāk "Krimināllikums") 2. pantu, persona, kas izdarījusi noziedzīgu nodarījumu Latvijas teritorijā, atbild saskaņā ar šo likumu.[14] Šis ir viens

---

[10] C. Schwarzenegger. The emergence of EU criminal law. Hart Publishing, 2014, p.231.
[11] Konvencija par Kibernoziegumiem.
Pieejams: [aplūkots: 12.04.2017].
[12] Eiropas Parlamenta un Padomes direktīva 2013/40.ES (2013.gada 12.augusts) par uzbrukumiem informācijas sistēmām, 12.pants.
Pieejams:
http://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:32013L0040 [aplūkots: 12.05.2017].
[13] Cybercrime, Cyberterrorism and Jurisdiction:
An Analysis of Article 22 of the COE Convention Cybercrime.
Pieejams: http://www.ejls.eu/6/78UK.htm [aplūkots: 13.04.2017].
[14] Krimināllikums, Publicēts: "Latvijas Vēstnesis", 199/200 (1260/1261), 08.07.1998.

no fundamentālajiem jurisdikcijas principiem, jo tieši teritorijas esamība un patstāvīga, un efektīva kontrole pār to ir arī viens no valsts suverenitātes pamatprincipiem.

Teritoriālais princips ir ļoti nozīmīgs jurisdikcijas princips tieši Eiropā, jo saskaņā ar klasisko Eiropas jurisdikcijas teoriju, valsts varas jurisdikcija, saskaņā ar starptautiskajām publiskajām tiesībām, nevar sniegties ārpus šīs valsts teritorijas[15], jo notikumi, kas izdarīti vienas valsts teritorijā, ir pakļauti tikai šīs valsts jurisdikcijai.

Visbiežāk problēmsituācijas, kuras tiek novērotas praksē un ar kurām saskaras tiesību aizsardzības iestāžu darbinieki un tiesas rodas brīžos, kad jānoskaidro, kuras valsts teritorijā noziegums ir izdarīts. Šī ir būtiska problēma kibernoziedzībā, jo bieži vien personas, kas veic kibernoziegumus, atrodas dažādās valstīs. Mūsdienu globalizācijas laikmetā pastāv daudz komplicētu situāciju ar teritorijas noteikšanu. Var rasties situācijas, kad noziegums ir izplānots vienas valsts teritorijā, izveidojot domēnu, kurš satur datorvīrusu, un trešās valsts teritorijā tiek uzsākta nozieguma izpildīšana, kas noved pie seku iestāšanās ceturtās valsts teritorijā, ielaužoties personu datos. Kā piemēru jāmin, turpmākajā darbā detalizētāk apskatīto Bogačeva lietu, kad personas, atrodoties Krievijas Federācijā, paveica noziedzīgu nodarījumu pret Amerikas Savienoto Valstu pilsoņiem no domēniem, kas tika reģistrēti Kanādā un Ukrainā.

Teritoriālās jurisdikcijas princips, autores ieskatā, šķiet visloģiskākais, nosakot valsti, kura īstenos savu jurisdikciju pār noziegumu, tomēr, ņemot vēra gadījumus, kuros ir praktiski neiespējami noteikt nozieguma laika gaitā, attīstoties nepieciešamībai pēc papildus jurisdikcijas veidiem, krimināltiesību kontekstā valstis ir paplašinājušas pieeju jurisdikcijas piemērošanas jautājumos, papildinot līdz tam klasiski pazīstamo principu ar jauniem jurisdikcijas veidiem. Uldis Ķinis savā grāmatā "Jurisdikcija un kibernoziegumi", izdala vienkāršo teritoriālo jurisdikciju un paplašināto teritoriālo jurisdikciju, kura sevī ietver:

1) likumpārkāpēja valstspiederības principu;

2) karoga principu (kuģi un lidmašīnas);

3) cietušā valstspiederības principu;

4) aizsardzības principu;

5) pārstāvniecības principu;

6) universālo principu.

---

[15] C.Ryngaert. Jurisdiction in international law. Oxford; New York: Oxford University Press, 2008, p.10.

Ņemot vērā iepriekš minēto, autore secina, ka pastāv divas jurisdikciju veidu grupas – teritoriālais un paplašinātais teritoriālais, kurš sevī ietver visus pārējos doktrīnās aprakstītos principus, pēc kuriem valstis var realizēt savu jurisdikciju pār noziegumiem.

Pēc Ulda Ķiņa rakstītā izriet, ka gadījumos, kad valstis īsteno savu jurisdikciju uz tai piederoša kuģa vai lidmašīnas (karoga princips), šāda jurisdikcija vairs nav teritoriālā, bet gan paplašinātā teritoriālā. Šajā ziņā nozīmīga ir *S.S.Lotus*[16] lieta, kurā tika realizēta jurisdikcija uz valstij piederoša kuģa, un citi tiesību zinātnieki šādu jurisdikciju tomēr apraksta pie teritoriālā principa.

Turpmāk minētais situācijas apraksts ir vispietuvinātākais kibernoziegumiem realitātē, tomēr pārrobežu noziedzības jurisdikcijas problēmas saskatāmas jau 1929. gadā lietā *S.S.Lotus*, kad lietu skatīja Tautu Savienības patstāvīgā Starptautiskā šķīrējtiesa. Strīds risinājās starp Franciju un Turciju saistībā ar Turcijas mēģinājumu saukt pie atbildības Francijas pilsoni, sakarā ar Vidusjūrā notikušo sadursmi starp franču un turku kuģi, kā rezultātā turku kuģis nogrima un bojā gāja 8 turku jūrnieki. Turcijas varas iestādes aizturēja franču kuģa virsnieku, jo viņš bija pie kuģa vadības stūres sadursmes brīdī, vēloties viņu saukt pie krimināltatbildības par Turcijas pilsoņu nogalināšanu. Francijā šāda Turcijas rīcība izsauca ļoti asus protestus. Valstis vienojās domstarpības nodot Starptautiskajai tiesai ar jautājumu, vai Turcijai ir tiesības realizēt krimināltiesisko jurisdikciju attiecība uz Francijas pilsoni, saskaņā ar teritoriālo jurisdikcijas principu. Lietu skatīja 15 tiesneši un balsis sadalījās 7:8, tiesai nolemjot, ka Turcijai ir tiesības saukt pie atbildības Francijas pilsoni, jo lai gan noziegums tika izdarīts uz objekta, kur bija spēkā Francijas jurisdikcija, proti, uz Francijas kuģa (*kā vispār zināms uz jūras kuģiem darbojās tās valsts jurisdikcija, zem kuras valsts karoga kuģis „atrodas"; kuģa teritorija tika pielīdzināta Francijas teritorijai*[17]*),* taču nozieguma sekas iestājās uz objekta, proti uz kuģa, kur darbojas Turcijas jurisdikcija, pielīdzinot Turcijas kuģi Turcijas teritorijai, kas nozīmē, seku iestāšanos Turcijas teritorijā, un to, ka noziegums izdarīts Turcijā. Lietas iznākumā Turcija atteicās realizēt savu krimināltiesisko jurisdikciju attiecībā uz franču kuģa virsnieku, tomēr šī lieta nostiprināja teritoriālās jurisdikcijas principu.

---

[16]Permanent Court of International Justice (Ordinary) Session, The Case of the S.S. Lotus, France v. Turkey, 7 September 1927. Pieejams: http://www.internationallawbureau.com/blog/wp-content/uploads/2012/07/The-SS-Lotus-Case.pdf [aplūkots: 11.04.2017].

[17]Apvienoto Nāciju Organizācijs Jūras tiesību konvencija un nolīgums par tās XI daļas īstenošanu. Pieejams:http://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A21998A0623(01) [aplūkots: 10.04.2017].

Konvencijā par kibernoziegumiem, kura tika noslēgta 2001. gadā un stājās spēkā 2004. gadā, 22. panta 1. punktā ir noteikts, ka "Katra Puse pieņem tādus normatīvos aktus un veic citus nepieciešamos pasākumus, lai nodibinātu jurisdikciju pār jebkuru noziedzīgu nodarījumu, ja noziedzīgs nodarījums izdarīts: a) tās teritorijā, vai b) uz kuģa, kas brauc zem šīs Puses karoga, vai c) uz lidmašīnas, kas reģistrēta pēc šīs Puses likumiem, klāja".

Tādā veidā Konvencija par kibernoziegumiem sevī ietver teritoriālo principu, kad nodarījums notiek valsts teritorijā un paplašināto teritoriālo principu, kad nodarījums notiek uz valstij piederoša kuģa vai lidmašīnas.

Suverenitāte nozīmē arī to, ka valstīm ir tiesības attiecināt savu jurisdikciju uz kibertelpu, ciktāl tā ir saistīta ar valsts teritorijā izvietotajiem kiberinfrastruktūras objektiem (*jurisdictio in rem*), un šajā infrastruktūrā veiktajām darbībām.[18]

Teritoriālā principa un tā piemērošanas problēmas ir skaidri redzamas arī 2000.gada Francijas lietā pret *Yahoo*. *Yahoo* ir interneta platforma, kura lietotājiem no visas pasaules ļauj komunicēt un platformas ietvaros ievietot dažādus materiālus un padarīt tos pieejamus lietotājiem visā pasaulē.[19]

Francijas *Yahoo* lietotājiem bija pieejami dažādi priekšmeti ar nacisma tematiku, par ko Francijas anti-rasisma organizācijas vērsās Francijas tiesā, pieprasot šos materiālus izņemt no Francijā pieejamās *Yahoo* mājaslapas. Nacisms un jebkāda ar to saistīta tematika ar likumu ir aizliegta Francijā.[20] Francijas tiesa, balstoties uz teritoriālās jurisdikcijas principu, balstoties uz to, ka materiāli bija redzami Francijas teritorijā un aizliegti tur ar likumu, piesprieda *Yahoo* izņemt Francijas lietotājus no platformas, kur var iegādāties šādus materiālus, un iznīcināt visus failus no serveriem.[21] *Yahoo* cēla prasību Amerikas Savienotajās Valstīs, apstrīdot Francijas tiesas spriedumu un, apgalvojot, ka sprieduma izpilde nav spēkā ārpus Francijas teritorijas, jo ir pret Amerikas Savienoto Valstu Konstitūcijas 1.pantu. Amerikas Savienoto Valstu tiesa lēma par labu *Yahoo*, nosakot, ka Francijas tiesai nebija pilnvaras, piespriest šādu lēmumu.

Kibernoziegumu kontekstā problēma ar teritoriālās jurisdikcijas principa piemērošanu rodas gadījumos, kad nav iespējams noteikt konkrētu teritoriju valsts robežās, kur noziedzīgais

---

[18] Tallin manual on the International law applicable to cyber warfare.
Pieejams: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [aplūkots: 17.04.2017].
[19] Yahoo! Inc.v. La Ligue Contre Le Racisme et l'Antisemitisme.
Pieejams:https://en.wikipedia.org/wiki/Yahoo!_Inc._v._La_Ligue_Contre_Le_Racisme_et_l%27Antisemitisme [aplūkots: 15.05.2017].
[20] Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention Cybercrime. Pieejams: http://www.ejls.eu/6/78UK.htm [aplūkots: 13.04.2017].
[21] Ibid.

nodarījums ir pastrādās un tā sekas iestājušās. Tiesiskais regulējums šo problēmu cenšas risināt Konvencijā par kibernoziegumiem nostiprinot principa piemērošanu gadījumos, kad kibernoziegums ir pastrādāts valsts teritorijā vai uz tai piederošiem kuģiem un lidmašīnām, uzliekot valstij pienākumu tādā gadījumā īstenot jurisdikciju pār noziedzīgu nodarījumu. Pēc autores domām, attiecībā uz kibernoziegumiem, konvencija nesatur pietiekami detalizētu regulējumu par to, kas tiek uzskatīta kā "teritorija", jo interneta vide jeb kibertelpa nav mērāma telpā.

1.2. Nacionālais princips un tā nozīme

Nacionālais princips ir cieši saistīts ar uzskatu, ka valstij ir praktiski neierobežota kontrole attiecībā uz tās valstspiederīgajiem.[22] Valsts ir tiesīga realizēt jurisdikciju pār saviem pilsoņiem arī attiecībā uz noziegumiem, kuri izdarīti citas valsts teritorijā. Latvijas Krimināllikuma 4. pantā par krimināllikuma spēku ārpus Latvijas teritorijas teikts, ka „Latvijas pilsoņi, nepilsoņi vai ārzemnieki, kuriem ir pastāvīgās uzturēšanās atļauja Latvijas Republikā, par citas valsts teritorijā vai ārpus jebkuras valsts teritorijas izdarītu nodarījumu neatkarīgi no tā, vai tas izdarīšanas vietā atzīts par noziedzīgu un sodāmu, saucami pie atbildības Latvijas teritorijā saskaņā ar šo likumu."

Nacionālās jurisdikcijas princips ir tieši saistīts ar suverenitāti, proti, nacionālais princips nav realizējams bez valsts suverenitātes. Suverenitāte – tā ir neierobežota, neatkarīga, augstākā politiskā vara pār valsts teritoriju.[23]

Šajā gadījumā var atzīt, ka gadījumi, kad kāda valsts veic kibernoziegumu citai valstij piederošiem kiberinfrastruktūras objektiem, nodarot tiem zaudējumus, varētu tikt uzskatīts, ka tādā veidā tiek apdraudēta tās suverenitāte.[24]

Starptautisko tiesību vadošais eksperts Jans Klabers nacionālo principu salīdzina ar Amerikas Savienotajās Valstīs pastāvošu praksi, ka tās valstspiederīgajiem ir pienākums maksāt nodokļus valstij, lai arī kur tie atrastos un pelnītu naudu.[25] Mūsdienas, kad personām ir iespējama dubultpilsonība, šī principa piemērošana arī varētu tikt apgrūtināta, tomēr no

---

[22] Ray August, "International Cyber-Jurisdiction: A Comprative Analysis", American Law Journal, vol.39 (summer, 2002), p.539.
[23] Victoria Neufeldt and David B. Guralnik. Webster's New world dictionary, Third college, 1989., p. 1283.
[24] U.Ķinis. Jurisdikcija un kibernoziegumi. Apgāds "Jumava", Rīga, 2013., 23.lpp.
[25] J.Klabbers. International law. Cambridge University Press, United Kingdom, 2013., p.93.

līdzšinējās tiesu prakses izriet, ka šādā gadījumā personai ir nosakāma vadošā pilsonība (piemēram, reālā personas dzīves vieta), un tādā gadījumā jurisdikcija tiek realizēta pēc tās.[26]

Konvencijas par kibernoziegumiem 22. pants paredz, ka katrai dalībvalstij ir pienākums pieņemt tādus normatīvos aktus un veikt citus nepieciešamos pasākumus, lai nodibinātu jurisdikciju pār jebkuru noziedzīgu nodarījumu, ja noziedzīgo nodarījumus izdarījusi persona, kura ir šīs valsts pilsonis un šis noziedzīgais nodarījums ir sodāms pēc tās vietas krimināltiesiskajiem normatīviem aktiem, vai arī, ja noziedzīgais nodarījums izdarīts ārpus jebkuras valsts teritoriālās jurisdikcijas. No šīs panta daļas izriet, ka valstis ir tiesīgas realizēt nacionālo jurisdikcijas principu pār saviem pilsoņiem.

Ņemot vērā, ka kibernoziegumu gadījumā ir praktiski neiespējami noteikt patieso noziedzīgā nodarījuma laiku un teritoriju, jo ļoti bieži šādi noziedzīgie nodarījumi tiek veikti no citā valstī reģistrētiem serveriem, nacionālā principa piemērošana būtu visatbilstošākā sodot vainīgo personu. Kibernoziegumu gadījumos ir skaidrs, ka jurisdikcijas piemērošana tiks veikta tās valsts teritorijā, kur procesa virzītājiem būs iespēja iegūt visvairāk pierādījumus par noziedzīgo nodarījumu. Kibernoziegumu gadījumos ļoti bieži kaitīgās sekas iestājas pavisam citā teritorijā, nekā tajā, kur ir aizdomās turamās personas domicils, līdz ar to ir ļoti svarīgi spēt konstatēt vainīgās personas objektīvo saikni ar valsts suverēno teritoriju. Šo saikni visvieglāk ir noteikt tieši pēc personas pilsonības, kura veido nacionālās jurisdikcijas piemērošanu. Autore uzskata, ka lai gan nacionālā jurisdikcijas principa piemērošana, salīdzinājumā ar teritoriālās jurisdikcijas principu, nerada problēmas ar konkrētas teritorijas noteikšanu, tomēr šis jurisdikcijas princips rada problēmas gadījumos, kad noziedznieka valsts nav ieinteresēta personas saukšanā pie atbildības.

1.3. Pasīvais personālais princips un tā nozīme

Pasīvais personālais princips ir viens no visjaunākajiem, un daudzi to uzskata par ļoti kontraversālu. Princips nozīmē, ka valsts ir tiesīga realizēt jurisdikciju pār jebkuru personu, kura aizskar tās valstspiederīgo.[27] Ja nacionalitātes princips balstās uz noziedzīgā nodarījuma paveikušās personas valstspiederību, tad pasīvais personālais pretēji balstās uz upura valstspiederību. Principu kontraversālu padara fakts, ka tā īstenošanas gadījumā valsts iejauktos otras valsts suverenitātē, kā arī izrietētu, ka valsts uzskata, ka otras valsts nacionālā tiesību

[26] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committe of the regions. Brussels, 08.05.2013. Pieejams: http://ec.europa.eu/justice/citizen/files/com_2013_270_en.pdf [aplūkots: 17.04.2017].
[27] J.Klabbers. International law. Cambridge University Press, United Kingdom, 2013., p.93.

sistēma nav pietiekami efektīva, lai sodītu vainīgo personu. Princips nav vispārēji atzīts nacionālajās tiesās, bet tas kļūst aizvien izplatītāks, attiecinot to uz teroristiskiem uzbrukumiem, ņemot vērā faktu, ka šādi uzbrukumi pārsvarā tiek vērsti tieši pret kādu konkrētu nacionalitāti.[28]

Attiecībā uz kibernoziegumiem princips tika pielietots 2003.gadā, kad Amerikas Savienotās Valstis tiesāja Krievijas valstspiederīgo Alekseju Ivanovu, kurš tajā laikā dzīvoja Čeļabinskā, Krievijas Federācijā, par ielaušanos Amerikas Savienoto Valstu datoros, un nozogot informāciju.[29]

Konvencija par kibernoziegumiem *expressis verbis* neparedz pasīvā personālā principa piemērošanu, tomēr neizslēdz iespēju valstīm to piemērot, ja tas ir paredzēts tās normatīvajos aktos. Latvijas Krimināllikums 4. panta trešā daļa paredz šī principa piemērošanu tikai gadījumos, kad pret Latvijas iedzīvotājiem ir pastrādāts "smags vai sevišķi smags noziegums". Autore kā problēmu, principa piemērošanā, saskata nosacījumu par noziedzīgā nodarījuma smaguma pakāpi, ņemot vērā, ka saskaņā ar Krimināllikumu ir gadījumu, kuros kibernoziegumi nekvalificējas kā "smagi", piemēram, 244.[1] panta noziedzīgais nodarījums.

1.4. Universālais princips un tā nozīme

Universālā jurisdikcijas principa pastāvēšana ir cieši saistīta ar ideju, ka daži noziedzīgie nodarījumi ir tik smagi, ka visas pasaules valstis ir tiesīgas vainīgo personu saukt pie atbildības, neatkarīgi no jebkādas piesaistes formas valstij.[30] Līdzšinējā vēsturē universālā jurisdikcija ir tikusi plaši piemērota pirātisma gadījumos un smagos cilvēktiesību pārkāpumos – genocīdos un noziegumos pret cilvēci.[31] Jurisdikcijas pamatā ir ideja, ka padarītais noziedzīgais nodarījums sava apmēra un rakstura dēļ apdraud jebkuru pasaules valsti, neņemot vērā, nodarījuma teritoriju vai tā pastrādājušā valstspiederību. Universālās jurisdikcijas doktrīnai starptautiskajās krimināltiesībās nav nekādas līdzības ar nacionālo jurisdikciju.[32] Līdzšinējā tiesu praksē ir nostiprināts, ka attiecībā uz *jus cogens* pārkāpumiem, valstis ir tiesīgas

---

[28] Restatement (third) of the foreign relations law of the United States,1987, Section 402(g).- Jurisdiction To Prescribe-Comment.
Pieejams: https://jura.urz.uni-heidelberg.de/mat/file_viewer.php?fid=10946
[aplūkots: 12.05.2017].

[29] U.S.A. v. Ivanov (2003), 172 C.C.C. (3d) 551 (Nfld.C.A.). See also U.S. Department of Justice. United States Attorney, "Russian Man Sentenced for Hacking into Computers in the United States".
Pieejams:https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/ivanovSent.htm
[aplūkots: 10.05.2017].

[30] Ibid. p.94.

[31] Ibid.

[32] Constitutional limits over exterritorial jurisdiction: terrorism and the intersections of national and international law by Anthony J. Colangelo. //Harwardnint. Law. Journal, vol.48, Number one, Winter 2007, 130.lpp.

realizēt universālo jurisdikciju. Genocīds ir viens no skaidrākajiem *jus cogens* piemēriem, tomēr Konvencijā par genocīda nepieļaujamību un sodīšanu par to universālās jurisdikcijas piemērošana nav minēta. Lai gan starptautiskās tiesības paredz universālo jurisdikciju kā vienu no jurisdikcijas veidiem[33], tomēr tā nav nostiprināta nevienā starptautiskā līgumā un pastāv vairāk, kā paraža.

Ir skaidrs, ka kibernoziegumi nav uzskatāmi par *jus cogens* normu, tomēr autore izvirza tēzi, ka, ņemot vērā pašreizējo situāciju, ir nepieciešams paplašināt universālās jurisdikcijas piemērošanas robežas. 21.gadsimtā internets ir visizplatītākais komunikācijas un datu uzglabāšanas un apstrādes veids un interneta telpa aptver visu pasaules globālo tīmekli un ir uzskatāma par kvazitelpu, kura aptver visus tās lietotājus pasaulē. Neviena privātpersona, organizācija vai uzņēmums interneta tīmeklī nav pasargāts un, ņemot vērā, interneta straujo un neparedzamo attīstības virzienu, nav paredzamie iespējamie nākotnes kaitējumi un noziedzīgie nodarījumi. Jau 2011. gada statistika liecināja, ka katru dienu pasaulē vairāk nekā viens miljons cilvēku kļūst par kibernoziegumu upuriem.[34] Ir skaidrs, ka līdz ar pieaugošo interneta attīstību pēdējo gadu laikā, statistika pavisam noteikti ir augusi.

Autore jau iepriekš minēja, ka universālās jurisdikcijas princips izriet no idejas, ka daži noziedzīgie nodarījumi ir tik smagi un skar tik lielu cilvēku apmēru, ka jebkura valsts ir tiesīga saukt vainīgo pie atbildības. Tiek lēsts, ka izmaksas, kuras no kibernoziegumiem tika radītas sabiedrībai līdz 2011.gadam, ir apmēram 388 miljardi ASV dolāru, kas kibernoziedzību padara ienesīgāku par tirdzniecību ar marihuānu, kokaīnu un heroīnu visu kopā.[35]

Pēc Latvijas Sabiedrisko mediju sniegtās informācijas ik gadu kibernoziegumi rada zaudējumus vismaz 3,5 miljardu ASV dolāru apmērā[36], un tiek lēsts, ka līdz 2019. gadam zaudējumi varētu sasniegt 2 triljonus ASV dolāru.[37] Amerikas Savienoto Valstu bijušais prezidents Baraks Obama apgalvoja, ka kibernoziegumi ASV pēdējo divu gadu laikā ir radījuši zaudējumus vismaz 8 miljardu ASV dolāru apmērā.[38] Līdz ar to ir pamats uzskatīt, ka kibernoziegumi ir smaga apmēra un skar ļoti lielu daļu pasaules iedzīvotāju.

---

[33] J.Klabbers. International law. Cambridge University Press, United Kingdom, 2013., p.95.
[34] Norton by Symantec. Cybercrime report 2011., p.1. Pieejams: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf [aplūkots: 12.05.2017].
[35] Ibid.
[36] Hakeri no Indijas uzbrūk flīžu veikalam un divreiz izdzēš tā datus. Pieejams:http://www.lsm.lv/raksts/latvija/zinas/hakeri-no-indijas-uzbruk-latvijas-flizu-veikalam-un-divreiz-izdzes-ta-datus.a229497/ [aplūkots: 18.05.2017].
[37] 20 Eye-Opening Cybercrime Statistics. Pieejams: https://securityintelligence.com/20-eye-opening-cybercrime-statistics/ [aplūkots: 12.05.2017].
[38] A brief history of Cybercrime.

Kā Saeimas Cilvēktiesību un sociālo lietu komisijas sēdē norādījis Valsts policijas Galvenās kriminālpolicijas pārvaldes Ekonomisko noziegumu atklāšanas pārvaldes 3. nodaļas priekšnieks Dmitrijs Homenko "*pašlaik viena daļa uzskata, ka kibertelpai nevar būt robežas, savukārt otra, ka kibertelpa ir sasaistāma ar cilvēkiem un to rīcību, un tās jurisdikcija ir piekritīga tai valstij, kuras teritorijā iestājas kaitīgās sekas*". No viedokļa, ka kibertelpai nav robežu, izriet, ka tieši universālās jurisdikcijas princips būtu vispiemērotākais, apkarojot kibernoziegumus. Eiropas Komisija 1997. gada rekomendācijā 3/97 "Par anonimitāti internetā" uzsvēra, ka e-vidē nepastāv juridisks vakuums un uz to ir pilnībā attiecināmi vispārējie tiesību principi. Dalībvalstīm ir jānodrošina principa "kas ir nelikumīgs reālajā vidē (*off-line*), par tādu atzīstams arī e-vidē (*on-line*)" ieviešana tiesību sistēmā.[39]

Neatņemama universālās jurisdikcijas principa daļa ir *aut detere, aud judicare* princips, kurš nosaka, ka personu ir pienākums vai nu tiesāt, vai nu izdot tālāk uz valsti, kura uzņemsies personas saukšanu pie atbildības. Konvencijas par kibernoziegumiem 22.panta trešā daļa faktiski šo principu attiecina arī uz konvencijā paredzētajiem kibernoziegumiem, un ir vērtējams kopā ar konvencijas 24.pantā noteiktos izdošanas pamatus attiecībā uz konvencijas piemērošanu.[40]

Autore izvirza tēzi, ka, apskatot kibernoziegumu apmēru un attīstības tendenci, ir pamats paplašināt universālās jurisdikcijas doktrīnu kibernoziegumu plašo apmēru un nenosakāmās teritorijas dēļ. Tomēr šādas prakses piemērošana radītu problēmu gadījumos, kad kāda valsts, izveidojot normatīvos aktus, kuri satur zemākus priekšnosacījumus, lai iestātos krimināatbildība par kibernoziegumiem, būtu tiesīga saukt pie atbildības jebkuru personu pasaulē. Aprakstītajā situācijā viena valsts varētu izveidot "monopolu" kibernoziegumu regulējumā, tikai tāpēc, ka pasaulē nepastāv vienots regulējums attiecībā pret kibernoziegumiem.

Pieejams: http://content.time.com/time/nation/article/0,8599,1902073,00.html [aplūkots: 12.05.2017].

The working party on the protection of individuals with regard to the processing of personal data. Recommendation 3/97 Anonymity on the internet, adopted by working party, 3.December 1997. Pieejams: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf [aplūkots: 12.05.2017].

[40] U.Ķinis. Jurisdikcija un kibernoziegumi. Apgāds "Jumava", Rīga, 2013., 226.lpp.

2. KIBERNOZIEGUMA JĒDZIENS UN TIESISKO SASTĀVU VEIDI

2.1. Vēsturiskā kibernozieguma jēdziena attīstība

Jāsāk ar to, ka kibernoziegums tiek uzskatīts par noziedzīgu nodarījumu[41], tādēļ, lai labāk izprastu jēdziena nozīmi, ir jānoskaidro, kas ir noziedzīgs nodarījums. Proti, noziedzīgs nodarījums ir personas konkrēta uzvedība, kas izpaužas viņas darbībā vai bezdarbībā. Nodarījuma kaitīgums ir svarīgākā krimināltiesības pamatīpašība, kaitīgums var izpausties kā būtisks apdraudējums valsts, sabiedrības un atsevišķu personu pašām nozīmīgākajām interesēm.[42] Jāpiekrīt Ulda Ķiņa izteiktajam viedoklim,, ka kibernozieguma definīcija sāksies ar vārdiem – krimināllikumā aizliegta darbība.[43]

Kibernoziegums ir tradicionāla nozieguma veids, kurš tiek izdarīts reālā vidē un kura darbības lauks ir saistīts ar e-vidi.[44] Autore uzskata, ka vispirms jāapskata jēdziens e-vide jeb internets. Internets (vārds atvasināts no "starptīkls") jeb Vispasaules tīmeklis[45], ir globāla vispasaules datoru sistēma, ar kuras palīdzību var iegūt informāciju (ja tā ir atļauta) no jebkuras datorsistēmas, jebkurā datorsistēmā, jo interneta lietošana sniedz iespēju piekļūt miljoniem mājaslapu ar informāciju.[46] Kibernoziegumu pastrādāšana pārsvarā tiek veikta caur domēniem, kas ir interneta mājaslapas adrese. Domēni tiek izmantoti, lai atcerētos un atrastu mājaslapas, produktus un dažādus pakalpojumus.[47]

Kibertelpa vai elektroniskā vide ir konkrēta kvazi telpa, kas vienlaikus aptver visus pasaules kontinentus un nacionālo valstu jurisdikcijas.[48] Internets ir kļuvis par bezrobežu telpu, kur nav ne robežu, ne vienotas pārvaldības, kas padara par gandrīz neiespējamu kontroles veikšanu pār šo telpu. Pēdējā laikā globālā interneta vide ir nonākusi uzmanības centrā, gan drošības iestādēm, gan krimināltiesību speciālistiem, kas nodarbojas ar noziedzīgu noziegumu atklāšanu.[49] Lai gan kibernoziegums tiek pastrādāts kibertelpā, nevis reālajā vidē, kā pārējie

---

[41] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 69.lpp.
[42] U.Krastiņš. Noziedzīgs nodarījums. Tiesu namu aģentūra, Rīga, 2000., 7.lpp.
[43] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 74.lpp.
[44] U.Ķinis. Kibernoziegumi un kriminālprocess. Jurista Vārds, 2011., 20.februāris., Nr.4.
[45] Internets. Pieejams: https://lv.wikipedia.org/wiki/Internets [aplūkots: 12.05.2017.
[46] Internet.
Pieejams: http://searchwindevelopment.techtarget.com/definition/Internet [aplūkots: 12.05.2017].
[47] Domēna vārds. Pieejams: https://www.hostnet.lv/domena-vards/ [aplūkots: 15.04.2017].
[48] U.Ķinis. Jurisdikcija un kibernoziegumi. Apgāds "Jumava", Rīga, 2013., 9.lpp.
[49] D.Ivašins. Krāpšana kibertelpā kā viens no internetnoziegumu veidiem.//Administratīvā un Krimināla Justīcija,2/2012, 17.lpp.

noziedzīgie nodarījumi, ir skaidrs, ka tā sekas nepaliek tikai kibertelpā, bet gan izpaužas reālajā vidē, nodarot personām reālus kaitējumus.

Detalizētāk apskatot kibernoziegumus un pasākumus, kurus valstis veic to apkarošanā, ir jāpiemin "Eurojust", kas ir Eiropas Savienības tiesu sadarbības organizācija, kura izmantojot savas specializētas zināšanas, atbalsta, nostiprina un uzlabo izmeklēšanas un apsūdzības procesu koordinēšanu starp Eiropas Savienības dalībvalstu kompetentajām tiesu iestādēm smagu pārrobežu noziegumu apkarošanā. [50] Pēc "Eurojust" noteikumiem, termins "kibernoziegums" var attiekties uz jebkuru noziegumu, kurā ir kāds no kiberelementiem.

Jauni noziegumi ir vērsti pret informācijas un komunikāciju tehnoloģijām, piemēram, tā ir ielaušanās datoros, digitālo pakalpojumu uzbrukumi vai datu aizsardzības pārkāpumi. Pastāv arī "normālie noziegumi", kuri ļoti lielā mērā ir atkarīgi no informācijas un komunikāciju tehnoloģijām, piemēram, cilvēku kontrabanda internetā, krāpšanās ar maksājumu karšu datiem vai teroristu aktivitātes internetā.[51]

Vēsturiski par pirmo kibernoziegumu pasaulē uzskata 1820. gadā reģistrēto sabotāžu, kad tekstilrūpnieks ar perfokartes palīdzību veica daļēju sava uzņēmuma automatizāciju. Strādnieki, baidoties pazaudēt darbu, šo ierīci sabojāja.[52]

Kopš 19. gadsimta sākuma kibernoziegumi līdz ar interneta attīstību ir nesalīdzināmi attīstījusies. Īstais kibernoziegumu ēras sākums tiek uzskatīts par laiku, kad pārdošanā nonāca pirmie personīgie datori. [53] Nākamais attīstības posms norisinājās no 1980. gada līdz astoņdesmito gadu beigām, kad plaši izplatījās dažādo kaitīgo programmu klāsts. Pasaule šajos gados iepazina vairākas datoru vīrusu programmas, kā piemēram, *Chernobyl, Netksy, Sasser* utt., kuras tika veidotas ar primāro mērķi veikt autortiesību objektu zādzības.[54] Otrajā attīstības posmā, kas norisinājās deviņdesmitajos gados kā jauna tendence tika novēroti kibernoziegumi, kuri ir vērsti pret dažādām komunikācijām, satelītiem un interneta pārlūkiem. Šis laiks tiek

---

[50]Eurojust legal framework.
Pieejams:http://www.eurojust.europa.eu/careers/Documents/AD2017/VN_Administrative%20Director_17EJ01_AD14_LV.pdf [aplūkots: 14.05.2017].

[51] Ar "naudas mūļu" ķeršanu vien nepietiek – ES stirprinās cīņu ar kibernoziegumiem. Pieejams: http://www.lsm.lv/lv/raksts/arzemes/zinas/ar-naudas-mulu-kersanu-vien-nepietiek--es-stiprinas-cinu-ar-kibernoziegumiem.a172328/ [aplūkots: 12.05.2017].

[52] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 30.lpp.

[53] The next generation of cybercrimes. How it has evolved and where it is going. Pieejams: http://www.allstream.com/wp-content/uploads/2015/11/white-paper-cybercrime.pdf [aplūkots: 16.04.2017].

[54]Ghorbani A. & Ghorbani A. (2014) Investigating computer crimes in cyberspace. Kuwait Chapter of the Arabian Journal of Bussiness and Managment Rewiew, 3(10), p. 299-403.
Pieejams: http://platform.almanhal.com/Files/?ID=T2-74850-MLA0028934.pdf [aplūkots: 15.05.2017.].

saistīts ar globālu pornogrāfijas tirdzniecības uzplaukumu, ko sekmēja straujā interneta attīstība.[55] Šajā laika posmā attīstījās arī interneta kā datu glabātāja loma, kura to padarīja pievilcīgu kibernoziegumu mērķim. Mūsdienās kibernoziedznieku mērķis ir gan datu glabātuves, gan personu profili sociālajos tīklos, kā arī tie tiek izmantoti spiegošanai, terorismam un plašam nelegālo preču pārdošanas tīklam. Kiberterorisms tiek definēts kā iepriekšplānota, politiski motivēta darbība, kas ir vērsta pret nemilitāru objektu informācijas sistēmām, ar mērķi radīt kaitējumu.[56]

Mūsdienās vēl joprojām nav skaidra, vienota definīcija, kas ir kibernoziegums. Konvencijā par kibernoziegumu apkarošanu ir minēti priekšnoteikumi, lai darbību varētu kvalificēt kā kibernoziegumu. Turpmākajās nodaļās tiks minēti šie priekšnoteikumi.

Pēc autores domām, šobrīd, tik strauji attīstošajā elektronikas un viedierīču laikmetā, nemaz nav iespējams definēt, kas ir kibernoziegums, jo ja kibernoziedzība ir saistīta ar jeb kāda veida datu nelikumīgu apstrādi, vai izmantošanu, tad līdz galam nav iespējams identificēt visas ierīces, kas var veikt datu apstrādi.

Konvencijā par kibernoziegumiem tiek uzskaiti 4 kibernoziegumi veidi 1) noziedzīgi nodarījumi pret datu un datorsistēmu konfidencialitāti, integritāti un pieejamību, kas sevī ietver patvaļīgu piekļūšanu, pārtveršanu, datu un sistēmas traucēšanu, un ierīces ļaunprātīgu izmantošanu; 2) ar datoru saistītie noziedzīgie nodarījumi, kas sevī ietver ar datoru saistītu viltošanu un krāpšanu; 3) ar saturu saistītie noziedzīgie nodarījumi, kas sevī ietver ar bērnu pornogrāfiju saistītos noziedzīgos nodarījumus un 4.) ar autortiesību un blakustiesību pārkāpšanu saistītie noziedzīgie nodarījumi, kas sevī ietver ar autortiesību un blakustiesību pārkāpšanu saistītos noziedzīgos nodarījumus.

Mūsdienās pastāv doktrīna, kura visus kibernoziegumus iedala divās kategorijās – iejaukšanās (*trespass*) kibernoziegumi un zādzības kibernoziegumi [57] Iejaukšanās kibernoziegumi personīgajā dzīvē rodas, kad persona bez atļautas piekļuves iekļūst kādas personas datora failos, vai nu tiem vienkārši piekļūstot un iegūstot informāciju vai arī šos failus iznīcinot. [58] Zādzības kibernoziegumi attiecas uz gadījumiem, kad persona bez atļaujas

---

[55] Wang W. Cybercrime and cyberspace. Pieejams: http://www.swansea.ac.uk/library/archive-and-research-collections/hocc/communicationsandtheinternet/sociallifeoftheinternet/cybercrime/cybercrimeandcyberspace/ [aplūkots: 17.04.2017].

[56] Latvijas Kiberdrošības stratēģija. 2014-2018. Pieejams: https://www.unodc.org/res/cld/lessons-learned/lva/latvijas_kiberdrobas_stratija_html/Kiberdrosibas_strategija.pdf [aplūkots: 13.04.2017].

[57] @Risk, Internet and E-Commerce, Insurance and Reinsurance Legal issues, Edited by Robert Hammesfahr of Blatt Hammesfahr & Eaton, London, Reactions Publishings Group Ltd., 2000., p.44.

[58] Ibid. p.45.

piekļuvei iegūst komercnoslēpumus, kredītkaršu informāciju un citus vērtīgus datus, vai arī veic naudas pārskaitījumus virtuālajā vidē.[59]

Pretēji tradicionālajiem noziegumiem, kibernoziegumus ir grūti identificēt, jo nozagto informāciju ir grūti novērtēt reāla kaitējumā, kura radusies personai. Lai tiktu ierosināta krimināllieta par pastrādātu kibernoziegumu, personai ir pienākums pierādīt reālu būtisku kaitējumu, kas no noziedzīgā nodarījuma radies. Ar būtisku kaitējumu, saskaņā ar likuma "Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību" 23.pantu ir jāsaprot gadījums, kad noziedzīgā nodarījuma rezultātā ne vien nodarīts ievērojams mantisks zaudējums, bet arī apdraudētas vēl citas ar likumu aizsargātās intereses vai, ja šāds apdraudējums ir ievērojams.[60]

Būtiska kaitējuma pareiza izpratne ir priekšnosacījums, pirmkārt, noziedzīga nodarījuma sastāva konstatācijai un, otrkārt, pareizai noziedzīga nodarījuma kvalifikācijai.[61] Kibernoziegumu kontekstā, būtiska kaitējuma noteikšana un izmērīšana ir problemātiska, jo bieži vien personas datus nav iespējams novertēt reālā mantiskā izteiksmē. Latvijas Kriminālprocesa likuma 96.panta pirmā daļa nosaka, ka personu par cietušo atzīst procesa virzītājs ar savu lēmumu.[62]

2.2. Kibernozieguma mūsdienu tiesiskais tvērums.

2.2.1. Ārvalstu prakse

2017. gadā apkopotie statistikas dati liecina, ka valsts pret kuru ir ticis vērsts vislielākais kibernoziegumu skaits ir Amerikas Savienotās Valstis[63], savukārt vislielākais skaits kibernoziegumu ir veikts no hakeriem, kas atrodas Ķīnā.[64] Par vienu no lielākajām datu zādzībām vēsturē līdz šim ir uzskatāma 2013. gada interneta platformas *Yahoo* domēna apzagšana, kuras rezultātā vairāk nekā 1 miljarda personu dati tika nozagti.[65] 2016. gada Amerikas Savienoto Valstu vēlešanu kibernoziegumi skaidri parāda, kā kibernoziedzība tiek izmantots arī kā 21. gadsmista politisks ierocis.

---

[59] Ibid. p.48.
[60] Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību. Publicēts: "Latvijas Vēstnesis", 331/332 (1392/1393), 04.11.1998.
[61] V.Liholaja, D.Hamkova. Būtiska kaitējuma izpratne: likums, teorija,prakse. Jurista Vārds, 10.01.2012., Nr. 2 (701).
[62] Kriminālprocesa likums. Publicēts: "Latvijas Vēstnesis", 74(3232), 11.05.2005.
[63] Top 10 countries worst hit by hackers. Pieejams: http://www.guidingtech.com/67467/top-hacked-countries-data-breaches-identities-stolen/ [aplūkots: 13.05.2017].
[64] Top 10 countries with most hackers in the world. Pieejams: https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e [aplūkots: 15.05.2017].
[65] 1 Billion plus Yahoo account information hacked; Safeguard yours.
Pieejams: http://www.guidingtech.com/62880/1-billion-yahoo-accounts-hacked/ [aplūkots: 20.05.2017]

Par vienu no pēdējās desmitgades vērienīgākajiem kibernoziedzniekiem tiek uzskatīts Mihaela Bogačeva, par kuru šobrīd Amerikas Savienoto Valstu Federālās izmeklēšanas birojs ir izsolījis 3 miljardu ASV dolāru atlīdzību. Bogačevs šobrīd atrodas Krievijas Federācijā, kura neizdod viņu tiesāšanai Amerikas Savienotajās Valstīs, balstoties uz neeksistējošu abu valstu divpusējo izdošanas līgumu.[66] Amerikas Savienotās Valstis apsūdz Bogačevu par tīkla *Zeus Trojan* izveidošanu, ar kura palīdzību tikai nozagta nauda no personu banku kontiem vairāku miljonu ASV dolāru vērtībā.[67] Vīruss inficēja datorus ar viltotu e-pasta adrešu vai interneta veikalu piegādes paziņojumu palīdzību, kurš līdz ko ielādēts datorā ļauj kibernoziedzniekiem kontrolēt pilnīgi visus datorā esošos failus un informāciju – paroles, lietotājvārdus, PIN kodus. [68] Bogačevs nedarbojās viens pats, bet gan kopā ar vismaz 50 citiem kibernoziedzniekiem, no kuriem tikai viens šobrīd atrodas apcietinājumā Amerikas Savienotajās Valstīs. Bogačeva vārds tiek saistīts arī 2016. gada Amerikas Savienoto Valstu prezidenta vēlēšanu informācijas uzlaušanu, kā uz to norādīja Federālās Izmeklēšanas birojs savos ziņojumos. Ņemot vēra, ka Bogačevam ir piekļuve miljoniem datoru daudzās pasaules valstīs, ir skaidrs, ka Krievijas Federācija varētu būt ieinteresēta viņu izmantot kā spiegu.[69] Bogačeva un viņa sabiedroto interneta serveri bija reģistrēti daudzās valstīs, kā, piemēram, Kanādā, Ukrainā un Amerikas Savienotajās Valstīs[70], kas padarīja notveršanu un pierādījumu apkopošanu vēl sarežģītāku. Viena no kibernoziegumu galvenajām pazīmēm, problēmām un īstenošanas iespējām ir tieši anonimitāte.

Šī ir viena no izplatītākajām problēmām kibernoziegumu identificēšanā un apturēšanā, jo lielākā daļa reģistrē serverus dažādās pasaules valstīs, no kurām veic noziedzīgus nodarījumus citās valstīs. Līdz ar to šajā gadījumā, Amerikas Savienotās Valstis nevarēja realizēt teritoriālo jurisdikciju, jo, lai gan sekas iestājās tur – radot zaudējumus un nodarot reālu kaitējumu miljoniem tās iedzīvotāju, pats noziedzīgais nodarījums tika pastrādāts no citu valstu teritorijās reģistrētiem serveriem. Šajā gadījumā Amerikas Savienotās Valstis, izvirzot

---

[66] The World's Most Wanted Hacker Sounds Like a Goddamn James Bond Villain. Pieejams: http://gizmodo.com/the-worlds-most-wanted-hacker-sounds-like-a-goddamn-jam-1793211745 [aplūkots: 25.04.2017].

[67] Russian Espionage Piggybacks on a Cybercriminal's Hacking. Pieejams: https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=1 [aplūkots: 12.05.2017].

[68] Inside the Hunt for Russia's Most Notorious Hacker. Pieejams: https://www.wired.com/2017/03/russian-hacker-spy-botnet/ [aplūkots: 12.05.2017].

[69] Russian Espionage Piggybacks on a Cybercriminal's Hacking. Pieejams:https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=1 [aplūkots: 12.05.2017].

[70] Inside the Hunt for Russia's Most Notorious Hacker. Pieejams: https://www.wired.com/2017/03/russian-hacker-spy-botnet/ [aplūkots: 12.05.2017].

apsūdzības Bogačevam un solot atlīdzību par viņu, teorētiski, izmantoja pasīvo personālo jurisdikcijas principu, aizsargājot savus valstspiederīgos, kuriem tika nodarīti zaudējumi. Šo konkrēto situāciju sarežģī arī fakts, ka Krievijas Federācija nav Konvencijas par kibernoziegumiem dalībvalsts, un tā ir apgalvojusi, ka konvencijas ratificēšana būtu pret Krievijas Federācijas suverenitāti, jo tā nepiekrīt sadarbībai starptautisku kibernoziegumu izmeklēšanās.[71] No tā izriet, ka Krievijas Federācijai nav nekādu starptautisku pienākumu attiecībā uz sadarbību kibernoziegumu atrisināšanā vai apturēšanā. Kā jau autore iepriekš norādīja, no Konvencijas par kibernoziegumiem netieši izriet *aut detere, aud judicare* principa piemērošana, kura šajā gadījumā būtu uzlikusi Krievijas Federācijai pienākumu, vai nu saukt Bogačevu pie atbildības savā teritorijā, vai arī izdot viņu uz valsti, kur viņš varētu tikt saukts pie atbildības.

Kā vēl viens prakses piemērs ir jāpiemin Džulians Asanžs (*Julian Assange*) un viņa izveidotā starptautiskā bezpeļņas organizācija *Wikileaks*. Laika posmā no 2006.gada *Wikileaks* ir nopludinājusi vairākus Amerikas Savienoto Valstu valdības un militāro spēku dokumentus un video. 2010.gadā, izraisot lielu ažiotāžu, tika nopludināti vairāk nekā 90 000 klasificētu e-pastu saistībā ar Afganistānas karu.[72] Pats Asanžs, noziedzīgo nodarījumu pastrādāšanas mirklī, neatradās Amerikas Savienotajās Valstīs, līdz ar to, atkal izslēdzot teritoriālā jurisdikcijas principa piemērošanu. Šobrīd Asanžam Ekvadora ir devusi patvērumu un viņš atrodas tās vēstniecībā Londonā, tādā veidā kļūstot neaizsniedzams Amerikas Savienotajām Valstīm jebkādai saukšanai pie atbildības. Tas gan nav traucējis *Wikileaks* turpināt nopludināt lielu daudzumu klasificētas un ierobežotas pieejamības informācijas no Amerika Savienoto Valstu valdības e-pastiem.

Visām iepriekš apskatītajām situācijām ir kopīgs tieši tas, ka nav vienota regulējuma par jurisdikciju kibernoziegumu apkarošanā. Šī problēma ir cieši saistīta ar faktu, ka daudzas valstis ir ieinteresētas izmantot kibernoziegumus spiegošanai citās valstīs un nevēlas, lai tie pamet valsts teritoriju un tiek saukti pie atbildības citā valstī.

2.2.2. Latvijas prakse

Lai gan 2014.gadā Latvijā tika oficiāli reģistrēti tikai apmēram 400 kibernoziegumi, šis skaitlis neatspoguļo patieso noziegumu skaitu to slēptā rakstura un citu ar to saistīto īpatnību

---

[71] Convention on Cybercrime. Pieejams: https://en.wikipedia.org/wiki/Convention_on_Cybercrime [aplūkots: 28.04.2017].
[72] Julian Assange Fast Facts. Pieejams: http://edition.cnn.com/2013/01/18/world/julian-assange-fast-facts/ [aplūkots: 23.04.2017].

dēļ.[73] Tiesu prakse saistībā ar kibernoziegumiem Latvijā ir salīdzinoši maza, jo vairumā situāciju ir grūti pierādīt būtiskā kaitējuma esamību.

Kā nesenākais gadījums Latvijas tiesu praksē saistībā ar kibernoziegumiem un jurisdikcijas īstenošanu, ir jāmin Deniss Čalovskis, pret kuru 2013. gadā Amerikas Savienoto Valstu federālie prokurori izvirzīja apsūdzības par datorvīrusa radīšanu, kurš nonācis Amerikas Savienoto Valstu Nacionālās aeronautikas un kosmosa pārvaldes (NASA) datoros.[74]

Amerikas Savienotās Valstis, balstoties uz 2005. gada Latvijas un Amerikas Savienoto Valstu Līgumu par izdošanu, pieprasīja izdot Čalovski, lai sauktu pie atbildības.[75] Šajā jautājumā Čalovskis vērsās Satversmes tiesā, lūdzot atzīt Līgumu par izdošanu par neatbilstošu Latvijas Republikas Satversmē nostiprinātajām cilvēktiesībām zināt savas tiesības un tiesībām uz taisnīgu tiesu. Satversmes tiesa lietu atteicās ierosināt, atzīstot starptautisko līgumu par konstitucionālu.[76] 2013. gadā Latvijas Republikas Saeima Čalovskis nolēma izdot tiesāšanai Amerikas Savienotajās Valstīs.[77] Tomēr, ņemot vērā faktu, ka Čalovskis par izdošanu Amerikas Savienotajām Valstīm, iesniedza sūdzību Eiropas Cilvēktiesību tiesā, Latvijas lēmums par izdošanu tika uz kādu laiku apturēts.[78] 2014. gadā Eiropas Cilvēktiesību tiesa pasludināja lēmumu lietā *Čalovskis pret Latviju*, atzīstot, ka izdošanas uz Amerikas Savienotajām Valstīm par tiesisku, nesaskatot iespējamu cietsirdīgu vai pazemojošu

---

[73]Valstīm jāsaskaņo izmeklēšanas metodes cīņā pret kibernoziegumiem. Pieejams: https://eu2015.lv/lv/jaunumi/zinas/1136-valstim-jasaskano-izmeklesanas-metodes-cina-pret-kibernoziegumiem [aplūkots: 18.05.2017].

[74]Rinkēvičs apšauba Imantas hakera izdošanu tiesāšanai ASV. Pieejams: http://www.lsm.lv/raksts/dzive--stils/tehnologijas-un-zinatne/rinkevics-apsauba-imantas-hakera-izdosanu-tiesasanai-asv.a53349/ [aplūkots: 12.05.2017].

[75]Eiropas Cilvēktiesību tiesa pasludina spriedumu lietā Čalovskis pret Latviju. Pieejams:http://www.mfa.gov.lv/ministrija/latvijas-parstavis-starptautiskajas-cilvektiesibu-institucijas/aktualitates/eiropas-cilvektiesibu-tiesa-pasludina-spriedumu-lieta-calovskis-pret-latviju [aplūkots: 12.05.2017].
Satversmes tiesa atteic ierosināt lietu par Latvijas un ASV līgumu par izdošanu. Pieejams: http://www.satv.tiesa.gov.lv/press-release/satversmes-tiesa-atteic-ierosinat-lietu-par-latvijas-un-asv-ligumu-par-izdosanu/ [aplūkots: 12.05.2017].

[77] Čalovski izdod tiesāšanai ASV. Pieejams: http://www.lsm.lv/raksts/zinas/latvija/calovski-izdos-tiesasanai-asv.a62573/ [aplūkots: 13.05.2017].

[78] ECT pieņem pieteikumu par Čalovski; aptur viņa izdošanu. Pieejams:http://www.lsm.lv/raksts/zinas/latvija/ect-pienem-pieteikumu-par-calovski-aptur-viņa-izdosanu.a62721/ [aplūkots: 12.05.2017].

izturēšanos pret Čalovski.[79] Pēc sprieduma pasludināšanas Čalovskis tika izdots Amerikas Savienotajām Valstīm tiesāšanai.[80]

2017.gadā Latvijas uzņēmums, kurš nodarbojas ar flīžu tirdzniecību, kļuva par kibernoziegumu upuri. Hakeri ar datorvīrusa palīdzību izdzēsa visus uzņēmumam piederošos datus un pieprasīja izpirkuma naudu par to atgriešanu. Pēc IP adreses izdevās noskaidrot, ka serveris, no kura tika veikts uzbrukums, ir reģistrēts Indijā.[81] Indija nav Konvencijas par kibernoziegumiem līgumslēdzējpuse[82], līdz ar to uz Indiju nevar attiecināt konvencijas 23.pantā paredzēto starptautiskās sadarbības principu.[83]

2.3. Noziedzīgu nodarījumu sastāvu analīze

Latvijas Krimināllikumā noziedzīgi nodarījumi, kas saistīti ar kibertelpu, ir aprakstīti 10. nodaļā – "Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību", turpretim Igaunijas Sodu kodeksā noziegumi ar automatizētu datu apstrādes sistēmu ir apkopoti nodaļā – "Noziedzīgi nodarījumi pret īpašumu".[84] No šāda Baltijas valstu salīdzinājuma izriet valstu atšķirīgā attieksme pret kibernoziegumiem – Latvijā tie tiek vērtēti kā noziegumi pret sabiedrisko kārtību, savukārt Igaunijā kā noziegumi pret īpašumu. No Igaunijas regulējuma ir skaidrs, ka personas dati tiek uzskatīti par personas īpašumu, bet Latvijā kibernoziegumus uztver kā sabiedrības drošības apdraudējumu. Ir skaidrs, ka visi turpmākajā darbā apskatītie Krimināllikuma panti rada kaitējumu, kurš ir ikviena noziedzīga nodarījuma pamatpazīme tādā nozīmē, ka tas rada kaitējumu sabiedrības interesēm.[85]

---

[79] Eiropas Cilvēktiesību tiesa pasludina spriedumu lietā Čalovskis pret Latviju. Pieejams: http://www.mfa.gov.lv/ministrija/latvijas-parstavis-starptautiskajas-cilvektiesibu-institucijas/aktualitates/eiropas-cilvektiesibu-tiesa-pasludina-spriedumu-lieta-calovskis-pret-latviju [aplūkots: 13.05.2017].

[80] ASV tiesas spriedums: Čalovskim vairs nav ilgāk jāpaliek ieslodzījumā. Pieejams: http://www.lsm.lv/raksts/zinas/latvija/asv-tiesas-spriedums-calovskim-vairs-nav-ilgak-japaliek-ieslodzijuma.a162766/ [aplūkots: 12.05.2017].

[81] Hakeri no Indijas uzbrūk Latvijas flīžu veikala un divreiž izdzēš tā datus. Pieejams: http://www.lsm.lv/raksts/zinas/latvija/hakeri-no-indijas-uzbruk-latvijas-flizu-veikalam-un-divreiz-izdzes-ta-datus.a229497/ [aplūkots: 18.05.2017].

[82] Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime. Pieejams: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VNC624sW [aplūkots: 13.05.2017].

[83] Konvencija par Kibernoziegumiem. Pieejams: https://likumi.lv/doc.php?id=146481 [aplūkots: 12.05.2017].

[84] Igaunijas Sodu kodekss. Pieejams: https://www.riigiteataja.ee/en/eli/522012015002/ [aplūkots: 20.04.2017].

[85] A. Judins Krimināltatbildības izslēdzamības apstākļi, Rīga, Tiesu namu aģentūra, 2000., 18.lpp.

2001.gadā tika pieņemta Konvencija par kibernoziegumiem, kas pirmo reizi starptautiskā tiesību jomā definēja noziedzīgo nodarījumu sastāvus, kas attiecīgi sagrupēti: noziedzīgi nodarījumi pret informācijas sistēmu drošību (patvaļīga piekļuve, pārtveršana, datu traucēšana, sistēmu traucēšana, kaitīgās ierīces); ar datoriem saistīti noziegumi – datorkrāpšana, datorviltošana; noziegumi pret autortiesībām un blakustiesībām; tā dēvētie satura noziegumi – saistīti ar nelikumīgas informācijas apriti (rasu naida, genocīda, kara kurināšana, bērnu pornogrāfijas aprite). [86] Autore vēlētos norādīt, ka pat Konvencijā par kibernoziegumiem nav sniegta skaidra definīcija, kas ir "kibernoziegumi", tā satur tikai iepriekšminētos noziedzīgo nodarījumu sastāvus.

Turpmākajās apakšnodaļās autore analizēs Krimināllikuma pantus, kuri regulē noziedzīgus nodarījumus pret informācijas sistēmas drošību Latvijā. Jāmin, ka turpmākajā darbā apskatīto Krimināllikuma pantu grupas objekts ir informācijas sistēmu drošība, kā vispārīgās drošības integrētā sastāvdaļa.

2.3.1. Krimināllikuma 241.pants

Krimināllikuma 241. pants regulē patvaļīgu piekļūšanu automatizētai datu apstrādes sistēmai un sankcijas par noziedzīgā nodarījuma veikšanu. Patvaļīga piekļuve automatizētai datu apstrādes sistēmai gan teorijā, gan arī praksē tiek uzskatīta par visu nodarījumu, kas vērsti pret informācijas sistēmu drošību, stūrakmeni.[87]

Par noziedzīga nodarījuma objektu jeb aizskarto interesi panta tvērumā ir jāsaprot jebkura no informācijas sistēmas drošības raksturojošām pazīmēm – integritāte, konfidencialitāte un pieejamība.[88] Šīs pazīmes ir tās, kuras garantē cilvēkam tiesības izmantot automatizētās sistēmas resursus savām vajadzībām. Objektīvā puse (*actus reus*) ir saistīta ar darbību, jo patvaļīga piekļuve vienmēr būs kādas konkrētas personas aktīva darbība, kura tiks vērsta pret piekļuvi informācijas sistēmai. Kā subjekts šī panta tvērumā ir jāsaprot prettiesisko darbību izdarījusī vai bezdarbību pieļāvusī fiziska, un pieskaitāma persona, kas sasniegusi Krimināllikumā paredzētu vecumu, no kura iestājas krimināltatbildība, un līdz ar to viņu par izdarīto noziedzīgo nodarījumu ir pamats saukt pie krimināltatbildības.[89] Subjektīvā puse teorijā

---

[86] U.Ķinis. Krāpšana automizētu datu apstrādes sistēmā. Jurista Vārds, 15.07.2014., Nr. 27 (829)
[87] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 127.lpp.
[88] Ibid. 131.pp.
[89] U.Krastiņš. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Tiesu namu aģentūra, Rīga, 2014., 108.lpp.

paredz personas tiešu vai netiešu nodomu pastrādāt noziedzīgo nodarījumu. Netiešā nodoma gadījumā persona nav vēlējusies kaitīgo seku iestāšanos, tomēr apzināti pieļāvusi, ka šādas sekas iestājas. Uldis Ķinis pauž viedokli, kuram autore piekrīt, ka šī panta tvērumā netiešs nodoms ir pieļaujams tikai teorijā, jo nav iespējams veikt pantā minētos nodarījumus ar netiešu nodomu. Vainojamās personas nodoms materializējas tikai ar mirkli, kad konkrēta persona, zinot, ka tās uzvedība ir pretrunā ar normām, realizē savu nodomu attiecībā pret konkrētu objektu un vēlas kaitīgo seku iestāšanos.[90]

Panta priekšmets ir informācijas sistēmas, tomēr autore piekrīt Ulda Ķiņa viedoklim, ka šāds priekšmets neatbilst mūsdienu prasībām, jo nav skaidrs, kā patvaļīga piekļuve digitālai telekomunikāciju sistēmai vai piekļuve iekšējam datu pārraides tīklam atšķiras no piekļuves datorsistēmai.[91]

Noziedzīgā nodarījuma rezultātu un tā smaguma pakāpi nosaka tieši vainīgas personas motīvs, kura iespaidā tā pastrādāja krimināpārkāpumu.

Kā sankcijas par pantā minēto noziedzīgo nodarījumu likumdevējs ir paredzējis naudas sodu, piespiedu darbu, īslaicīgu brīvības atņemšanu, mantas konfiskāciju, un cietumsodu no diviem līdz pieciem gadiem, atkarībā no panta piemērojamās daļas.[92] Krimināllikuma 241. panta neskaidrie jēdzieni, kaitējuma apmērs un neskaidrība tajā, cik lielā mērā kādai personas ir "jāpārvar sistēmas aizsardzības līdzekļi" pēc autores domām, sarežģī tā piemērošanu.

2.3.2. Krimināllikuma 243.pants

Krimināllikuma 243. pants regulē automatizētas datu apstrādes sistēmas darbības traucēšanu un nelikumīgu rīcību ar šajā sistēmā iekļauto informāciju. Noziedzīgā nodarījuma objekts ir informācijas sistēmu drošība, bet speciālais objekts – interese – nodrošināt sistēmā esošo informācijas resursu integritāti jeb veselumu.[93] Noziedzīgais nodarījums kā sistēmas darbības traucēšana ir ietverts likumā ar mērķi, lai valsts varētu pasargāt savus valstspiederīgos no uzbrukumiem, kas tiek veikti interneta vidē. Objektīvā puse tāpat kā jau pirms tam apskatītajā 241. panta analīzē ir personas aktīva darbība, kuras rezultātā tiek bojāti vai pavisam iznīcināti kādas pastāvošas sistēmas dati. Uldis Ķinis kā konkrētas aktīvas darbības 243. panta ietvaros min datu dzēšanu, datu aizklāšanu, datu pārveidošanu, sistēmas neatgriezenisku

---

[90] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 136.lpp.
[91] U.Ķinis. Kibernoziegumi. SIA "Biznesa augstskola Turība", Rīga, 2007., 205.lpp.
[92] Krimināllikums, Publicēts: "Latvijas Vēstnesis", 199/200 (1260/1261), 08.07.1998.
[93] U.Ķinis. Kibernoziegumi. SIA "Biznesa augstskola Turība", Rīga, 2007., 244.lpp.

bojāšanu, kā arī "konservēšanu" (*spamming)*.[94] Arī subjekts analogi 241. pantam ir fiziska, pieskaitāma un Krimināllikumā noteikto vecumu sasniegusī persona. Panta subjektīvā puse ir analoga jau iepriekš analizētajam 241. pantam.

Darbības, kas saistītas ar nelikumīgu datu ievadīšanu automatizētu datu apstrādes sistēmā, ir nepieciešams konstatēt, inkriminējot nodarījumus pēc Krimināllikuma 243. panta.[95]

2.3.3. Krimināllikuma 244.pants

Krimināllikuma 244. pants regulē nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm, savukārt 244.[1] pants regulē datu programmatūras un iekārtu iegūšanu, izgatavošanu, izmainīšanu, glabāšanu un izplatīšanu nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām. Noziedzīga nodarījuma objekts 244.pantā ir dati, kas var tikt pakļauti nelikumīgām darbībām, bet 244.[1] panta objekts ir visi dati, programmatūras un iekārtas, kas var tikt pakļautas nelikumīgām darbībām. Objektīvā puse abos pantos ir personas aktīva darbība, kuras rezultātā tiek veiktas nelikumīgas darbības ar automatizētu datu apstrādes sistēmas resursu ietekmēšanas ierīcēm un tiek veiktas neatļautas darbības ar datiem, programmatūrām un ierīcēm. Panta subjekts ir tāpat kā pirms tam apskatītajos pantos ir fiziska, pieskaitāma un Krimināllikumā noteikto vecumu sasniegusi persona. Panta subjektīvā puse ir analoga pirms tam analizētajam 241.pantam. Kā panta problēmu autore saskata jau iepriekšminēto problemātiku ar "būtiska kaitējuma" vai pantā minētajām "smagajām sekām" un no noteikšanu kibernoziegumu kontekstā. Pēc autores domām Krimināllikums būtu jāpapildina ar detalizētāku noziedzīga nodarījuma rezultātā iestājušos seku konkretizāciju.

---

[94] Ibid. 263-264.lpp.
[95]U.Ķinis. Krāpšana automatizētā datu apstrādes sistēmā. Jurista Vārds. 15.07.2014. Nr. 27 (829).

3. JURISDIKCIJAS KONFLIKTI

Jurisdikcijas konflikts izriet no situācijas, kad starp divām vai vairākām pusēm rodas strīds par krimināllietas risināšanu. Puses var būt vienas vai dažādu valstu institūcijas, amatpersonas vai valstis. Gadījumos, kad strīds izveidojies starp vienas valsts subjektiem, konflikts ir iekšējs jeb lokāls, bet, ja jurisdikcijas konflikts ir izveidojies starp valstīm un to institūcijām, tad šāds konflikts ir starptautisks jeb ārējs. Turpmākajā nodaļā autore sīkāk apskatīs starptautisku jeb ārēju jurisdikciju konfliktu situācijas, jo Latvijas Krimināllikums paredz iekšējās jurisdikcijas strīdu nepieļaujamības principu.[96]

Kā jau darbā iepriekš minēts Konvencija par kibernoziegumiem 22.panta 1. daļas a), b) un c) apakšpunkti paredz teritoriālo jurisdikcijas principu, un d) apakšpunkts paredz nacionālo jurisdikcijas principu. Konvencijas 22.panta 5. daļa situācijās, kad rodas jurisdikcijas konflikts, uzliek līgumslēdzējpusēm pienākumu konsultēties, lai spētu piemērot visatbilstošāko jurisdikciju apsūdzības celšanai.

Tomēr jāpiemin, ka Konvencija neparedz situācijas risinājumu gadījumos, kad noziedzīgais nodarījums pastrādāts vietā, kuras normatīvie akti neparedz sodu par konkrēto noziedzīgo nodarījumu. [97] Piemēram, Mongolijā, Afganistānā, Kongo Demokrātiskajā Republikā, Čadā, Lībijā u.c. valstīs nepastāv normatīvie akti, kuri paredzētu sodu par kibernoziegumiem.[98] Saskaņā ar Apvienoto Nāciju sniegtās statistikas 19% pasaules valstu nepastāv kibernoziegumu tiesiska regulējuma.[99]

Teritoriālais un nacionālais jurisdikcijas principi, kurus paredz Konvencija par kibernoziegumiem, ir gan vispārīgo tiesību sistēmas, gan kontinentālās tiesību sistēmas krimināls jurisdikcijas stūrakmeņi.[100] Jurisdikcijas konflikts starp šiem diviem pastāvošajiem principiem ir saistīts ar faktu, ka lokācija, kur persona ir veikusi noziedzīgo nodarījumu var nesakrist ar vietu, kurā tiek apdraudētas ar likumu aizsargātās intereses. Šāda situācija visbiežāk ir sastopama, jo gadījumos, kad kibernoziegumi ir vērsti pret kādas citas valsts pilsoņiem vai pašas valsts drošību, kā, piemēram, Amerikas Savienoto Valstu prezidenta vēlēšanu gadījums [101] , noziegums tiek pastrādāts no kādas trešās valsts teritorijas. Teritoriālais

---

[96] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 419.lpp.
[97] Ibid.
[98] Cybercrime Legislation Worldwide. Pieejams: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx [aplūkots: 17.04.2017].
[99] Ibid.
[100] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 434.lpp.
[101] What we know about Russia's interference in the US election. Pieejams: https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election [aplūkots: 15.04.2017].

jurisdikcijas princips, tostarp kibernoziegumu kontekstā, ir visfundamentālākais no jurisdikcijas pamatiem[102], tomēr mūsdienās doktrīna paredz arī citu jurisdikcijas principu piemērošanu, kā, piemēram, nacionālā jurisdikcijas piemērošanu, kad, piemēram, Latvija savu valstspiederīgo varētu lūgt izdot trešajai valstij, lai tiesātu pēc savas jurisdikcijas. Tomēr problēma rodas gadījumos, kad trešā valsts nevēlas personu izdot sodīšanai viņa nacionalitātes valstī.

Kā piemēru var minēt situāciju, kad Latvijas valstspiederīgais A veic noziedzīgu nodarījumu no Mongolijas, kurā nepastāv nekāds tiesiskais regulējums attiecībā pret kibernoziegumiem, pret Lietuvas pilsoni B. Jāuzver arī, ka Mongolija nav ratificējusi Konvenciju pret kibernoziegumiem.[103] Šādā piemērā izveidojas absurda situācija, kad persona var palikt nesodīta par veikto noziedzīgo nodarījumu, jo Mongolijas nacionālajos normatīvajos aktos tas nav uzskatāms par sodāmu noziedzīgo nodarījumu.

Ņemot vērā faktu, ka starp diviem apskatāmajiem jurisdikcijas principiem nepastāv nekāda hierarhija, nav skaidrs iespējamais risinājums situācijā, kad divas valstis, kurām abām tiesības realizēt jurisdikcija pēc kāda no šiem principiem, vēlas saukt personu pie atbildības. No efektīvas tiesību piemērošanas izrietētu, ka prevalēs valsts, kurā persona faktiski atrodas, jo veidojas objektīva saikne ar suverēnu teritoriju, vai kurā ir veikta vairākas izmeklēšanas darbības, lai to sauktu pie atbildības. Uzmanības vērta ir situācija, kad persona, kurus vēlas saukt pie atbildības valsts A, kurā viņš veica noziedzīgo nodarījumu, un valsts B, kuras valstspiederīgais viņš ir, atrodas kādā pavisam nesaistītā trešajā valstī, kurā nepastāv normatīvais regulējums par noziedzīgiem nodarījumiem kibertelpā.

Šāds gadījums būtu vistiešākais piemērs jurisdikcijas konfliktiem un īpaši aktuāls tieši kibernoziegumu gadījumos, ņemot vērā to ierobežoto piesaisti "reālai" teritorijai. Ierobežotā piesaiste rada arī problēmas tiesām pareizi spriest tiesu pār kibernoziegumiem, jo likumdevējs nav nodalījis noziedzīgos nodarījumus, kuri pastrādāti reālā vidē, no kibernoziegumiem, un tiesas bieži vien cenšas kibernoziegumus risināt analogi reāliem[104], lai gan šāda situācija ir absurda, ņemot vērā abu noziegumu veidu nesalīdzināmo raksturu un vidi, kurā tie notiek.

---

[102] Cybercrime and Internet jurisdiction by H.Kaspersen, March 5, 2009, CoE Project on cybercrime. Discussion paper.
Pieejams:http://www.coe.int/t/dghl/cooperation/economic-crime/cybercrime/Documents/reports-presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf [aplūkots: 15.04.2017].

[103] Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime. Pieejams: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=4CE5gxZo [aplūkots: 18.05.2017].

[104] Betsy Rosenblatt. Principles of Jurisdiction.
Pieejams: https://cyber.harvard.edu/property99/domain/Betsy.html [aplūkots: 28.02.2017].

Gadījumos, kad divas valstis, balstoties uz jurisdikcijas principiem, vēlas saukt personu pie atbildības, ir jāņem vērā *ne bis in idem* (dubultās sodīšanas aizlieguma) princips. Eiropā šis princips ir nostiprināts nacionālo valstu konstitūcijās (Latvijā – Latvijas Republikas Satversmes 92. pantā ietvertajās "tiesībās uz taisnīgu tiesu"[105]) un krimināltiesībās.[106] Nonākšana pie viena jurisdikcijas principa piemērošanas, izvairoties no jurisdikcijas konfliktiem, ir nepieciešama aplūkotā principa pareizai piemērošanai, jo nav pieļaujama situācija, kad attiecība pret vienu noziedzīgo nodarījumu vairāk nekā viena valsts vērš savu jurisdikciju.

Kā jau autore iepriekš minēja, Konvencija par kibernoziegumiem paredz teritoriālā jurisdikcijas principa un nacionālā jurisdikcijas principa piemērošanu. Tomēr jāņem vērā, ka nacionālās jurisdikcijas princips ir ierobežots ar nosacījumu, ka valstī, kur noziedzīgais nodarījums ir pastrādāt, tas tiek uzskatīts par sodāmu noziedzīgu nodarījumu valsts normatīvajos aktos. Latvijas Krimināllikums 2. pantā paredz teritoriālo jurisdikcijas principu, 4. panta, apskatot Krimināllikuma spēku ārpus Latvijas teritorijas, 1. daļā paredz nacionālo jurisdikcijas principu un 3. daļā paredz pasīvo personālo principu. Panta 4. daļa paredz to, ka ārzemnieki, kuri veikuši noziedzīgu nodarījumu trešās valsts teritorijā saucami pie atbildības Latvijā, ja to paredz Latvijas Republikai saistoši starptautiski līgumi. Saskaņā ar Latvijas Republikas Satversmes 89. pantu Latvijai ir saistoši starptautiskie līgumi.[107] Ņemot vērā, ka Latvija ratificēja Konvenciju par kibernoziegumiem 2006. gadā, starptautiskais līgums ir daļa no Latvijas tiesību sistēmas un ir saistošs Latvijai. Salīdzinot Krimināllikumā paredzētos jurisdikcijas veidus un Konvencijā par kibernoziegumiem noteiktos, izriet, ka konvencija sašaurina iespējamos jurisdikcijas veidus, neparedzot pasīvā personālā jurisdikcijas veida piemērošanu attiecībā uz kibernoziegumiem. Tomēr, apskatot konvencijas 22. panta 4. daļu, kura nosaka, ka "Konvencija neizslēdz krimināltiesisko jurisdikciju, ko Puse (šajā gadījumā Latvijas Republika) realizē saskaņā ar tās normatīvajiem aktiem", ir skaidrs, ka Latvija nav ierobežota pasīvā personālā principa piemērošanā. Jāņem vērā arī fakts, ka Krimināllikuma 4. panta 3. daļā attiecina pasīvā personālā principa piemērošanu tikai uz smagiem vai sevišķi smagiem noziedzīgiem nodarījumiem. Par kibernoziegumiem, saskaņā ar Krimināllikuma 243.

---

[105] Satversmes tiesas 2012.gada 18.oktobra spriedums lietā 2012-02-0106, 11.punkts. Pieejams: http://www.satv.tiesa.gov.lv/wp-content/uploads/2012/01/2012-02-0106_Spriedums.pdf [aplūkots: 13.05.2017].

[106] Van Bockel W.B. Two perspectives on the realization of the ne bis in idem principle in Europe. Pieejams: https://www.academia.edu/19950258/Two_Perspectives_on_the_Realization_of_the_European_I_ne_bis_in_idem_I_Principle [aplūkots: 19.05.2017].

[107] Latvijas Republikas Satversme, Publicēts: "Latvijas Vēstnesis", 43, 01.07.1993., "Ziņotājs", 6, 31.03.1994.

panta trešo daļu, ir paredzēta brīvības atņemšanu uz laiku līdz septiņiem gadiem, kas tos kvalificē kā smagus noziegumus.

Uzmanības vērts, varētu būt gadījums, kad kibernoziegumos tiek iesaistīta, piemēram, Afganistāna, kura nav ratificējusi Konvenciju par kibernoziegumiem, kā arī tāda valsts, kuras tiesiskais regulējums neparedz sodu par kibernoziegumiem. Konkrētajā gadījumā (ja vien starp valstīm nav noslēgts divpusējs izdošanas līgums, kā, piemēram, Latvijas un Amerikas Savienoto Valstu 2005. gada izdošanas līgums[108]) valsts, kuras teritorijā izdarīts konkrētais noziegums, var atteikties gan personu izdot, gan arī sniegt savstarpējo palīdzību krimināllietās, ņemot vērā faktu, ka darbība nav izpildītājvalstī atzīstama par noziegumu.[109] Šāda situācija var novest pie rezultāta, kad noziedzīgā nodarījuma izdarīšanas vieta var tikt izmantota apzinātai ļaunprātībai vai, kad persona var nemaz netikt saukta pie atbildības par pastrādāto kibernoziegumu. Aprakstītā situācija ir pavisam reāli iespējama, un, lai gan nedaudz citā kontekstā, tomēr šajā gadījumā jāpiemin iepriekš apskatītā Bogačeva lieta, kad Krievijas Federācija atsakās izdot Bogačevu Amerikas Savienotajām Valstīm saukšanai pie atbildības. Kibernoziegumi un personu izdošana sodīšanai citā valstī ir neizbēgami saistīta ar politisko situāciju. Kā norādījis Vašingtonas Stratēģisko un Starptautisko zinātņu centra Tehnoloģisko un publisko programmu vadītājs Džeims Levis (*James Lewis*) "Lielākā problēma kibernoziegumu apkarošanā ir politika un suverenitāte".[110]

Daudzu kibernoziegumu starptautiskais raksturs ir radījis bažas, ka tieši jurisdikciju konfliktu dēļ ievērojams skaits personu, kuras veikušas noziedzīgus nodarījumus, kuru sekas ir iestājušās citā valstī, efektīvi izvairās no sodāmības un turpina savu kriminālo darbību. [111] Noziedznieki mēģina atrast sev izdevīgākus soda nosacījumus jeb labprātāk vēlas tikt sodīti tajā valsts teritorijā, kur par paveikto noziegumu tiek paredzēts maigāks sods. Pēc autores domām, jurisdikciju konflikti varētu pavērt iespējas noziedzniekiem meklēt sev izdevīgāku situāciju, jo neskaidrības tiesību normu piemērošanā paver iespējas to negodprātīgai izmantošanai.

---

[108] Par Latvijas Republikas valdības un Amerikas Savienoto Valstu valdības līgumu par izdošanu. Publicēts: "Latvijas Vēstnesis", 93(3669),12.06.2007., "Ziņotājs", 13, 12.07.2007.
[109] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 442.lpp.
[110]The Top Countries For Cybercrime.
Pieejams:
https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/2007/07/13/cybercrime-world-regions-techcx_ag_0716cybercrime.html&refURL=https://l.facebook.com/&referrer=https://l.facebook.com/
[aplūkots: 20.04.2017].
[111] .Chawki, A.Darwish, M.A.Khan, S.Tyagi. Cybercrime, digital forensics and jurisdiction. Springer international Publishing, 2015., p.33.

Kā vēl vienu problēmjautājumu attiecībā pret Konvenciju pret kibernoziegumiem jāmin valstu nespēju efektīvi sadarboties kibernoziegumu apkarošanā. Konvencijas 3.nodaļā ir noteikta starptautiskā sadarbība, kura Līgumslēdzējpusēm uzliek pienākumu sadarboties, lai pēc iespējas vairāk veicinātu izmeklēšanu un tiesvedību attiecībā uz noziedzīgajiem nodarījumiem. Tomēr konvencija neparedz detalizētāku regulējumu attiecībā uz valstu sadarbību un noziedzīga nodarījuma izmeklēšana joprojām ir atkarīga no trešās valsts labās gribas palīdzēt izmeklēšanas gaitā.[112] Kā piemēru starptautiskās sadarbības neefektivitātei jāmin gadījums, kad Latvijā vairāku gadu garumā tika meklēta persona, kura bija atbildīga par nelikumīgām darbībām internetā un bija pārcēlusies uz dzīvi Lielbritānijā. Personu neizdevās saukt pie atbildības Latvijā, jo Lielbritānija divu gadu laikā nesniedza atbildi uz Latvijas policijas savstarpējās palīdzības lūgumu.[113]

No iepriekš apskatītajiem jurisdikcijas principiem izriet, ka to īstenošanai ir nepieciešama kāda reāla piesaiste – teritorija vai personas valstspiederība, tomēr, ņemot vērā, kibernoziegumu abstrakto dabu un neierobežoto telpu, ir grūti noteikt pastāvošu piesaisti. Iepriekšējās nodaļās apskatītais universālās jurisdikcijas princips ir vienīgais, kurš neprasa valstij nekādu saikni ar personu, lai sauktu to pie atbildības. Universālās jurisdikcijas materiālais pamats ir starptautisks noziegums.[114] Starptautisku noziegumu krimināltiesību doktrīnā tiek definēts kā "bīstams drauds pret starptautisko sabiedrību kopumā vai pret tās fundamentālajām vērtībām".[115]

Par starptautiskiem krimināltiesību noziegumiem ir uzskatāmi noziegumi pret starptautiskajām tiesībām, un ir jāizpildās trīs kritērijiem, lai noziedzīgais nodarījums kvalificētos par starptautisku:

1) jābūt pārkāptai kādai krimināltiesību normai, kura ir nostiprinātā starptautiskā līgumā vai ir ieguvusi paražas statusu;

2) noziedzīgais nodarījums ir sodāms saskaņā ar starptautiskajām tiesībām;

---

[112] Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention Cybercrime. Pieejams: http://www.ejls.eu/6/78UK.htm [aplūkots: 13.04.2017].
[113] Žurnālisti Lielbritānijā atrod ilgi meklēto draugiem.lv krāpnieku.
Pieejams: https://defense.lv/2015/02/09/zurnalisti-lielbritanija-atrod-ilgi-mekleto-draugiem-lv-krapnieku/ [aplūkots: 13.05.2017].
[114] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 305.lpp.
[115] International Criminal Law – Defining international crimes.
Pieejams: //http://law.jrank.org/pages1382/international-criminal-law-defining-international-crimes.html [aplūkots: 01.05.2017].

3) starptautisks līgums paredz atbildību par pastrādāto noziedzīgo nodarījumu, un atbildības paredzēšana ir saistoša valstu vairākumam.[116]

Apvienoto Nāciju Organizācijas Romas Starptautiskās krimināltiesas statūtu 5.pantā ir uzskaitīti noziegumi, kuri atrodas tiesas jurisdikcijā un kuri tiek uzskatīti par noziegumiem, kuri skar visu starptautisko sabiedrību kopumā. Statūtos kā šādi noziegumi ir uzskatīts – genocīds, noziegumi pret cilvēci, kara noziegumi un agresija. [117] Tomēr, apskatot kibernoziegumus, var secināt, ka tie atbilst visiem iepriekšminētajiem kritērijiem – tie pārkāpj Konvencijā par kibernoziegumiem minētas normas, ir sodāmi saskaņā ar konvenciju un paredz atbildību par to pastrādāšanu. Ņemot vērā, ka Konvenciju par kibernoziegumiem, ir ratificējušas 56 valstis, to var uzskatīt par valstu vairākumu kibernoziegumu kontekstā.[118]

Autore šajā darbā izvirza tēzi, ka, ņemot vērā kibernoziegumu raksturu, plašos apmērus, augošo tendenci un ietekmi uz starptautisko sabiedrību kopumā, tas atbilst "starptautiska nozieguma" definīcijai, un pēc autores domām drīzumā radīsies nepieciešamība kibernoziegumus kvalificēt kā starptautiskus noziegumus.

Autore nepiekrīt vadošā kibernoziedzības eksperta Latvijā Ulda Ķiņa viedoklim, ka kibernoziegumi diezin vai jebkad sasniegs "starptautiskā nosodījuma" pakāpi, lai tos atzītu par starptautiskiem noziegumiem, kuriem piemērojama universālā jurisdikcija. [119] Kibernoziegumiem piemītošās īpašības – anonimitāte, neesoša piesaiste kādai konkrētai teritorijai, plašais mērogs un plašais personu loks, kuriem tiek nodarīti zaudējumi, tos visvairāk pietuvina starptautiskiem noziegumiem.

Kā vēl viens pierādījums kibernoziegumu plašajam mērogam un būtiskajam kaitējumam, kurš tam piešķir starptautiska nozieguma raksturu, ir jāmin tumšā interneta puse jeb tā sauktais *deep web*. *Deep web* ir informācijas sistēma, kuru apzināti nav iespējams atrast ar, piemēram, populārāko meklēšanas sistēmu *google* vai jebkuru citu publiski pieejamu meklēšanas sistēmu.[120] *Deep web* ir visātrāk augošais interneta sektors un tikai 1% no tā satura

---

[116]International crime law and legal definition. Pieejams: https://definitions.uslegal.com/i/international-crime/ [aplūkots: 12.05.2017].

[117] Rome Statute of the International Criminal Court. Pieejams: https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf [aplūkots: 14.05.2017].

[118] Convention on Cybercrime.
Pieejams: https://en.wikipedia.org/wiki/Convention_on_Cybercrime [aplūkots: 12.05.2017].

[119] U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds "Jumava", Rīga, 2015., 433.lpp.

[120] Cybercrime in the Deep Web. Pieejams: https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-In-The-Deep-Web-wp.pdf [aplūkots: 16.05.2017].

ir pieejams parastās meklēšanas sistēmās.[121] Šajā sistēmā ir pieejams praktiski viss – sākot ar narkotiskajām vielām un beidzot ar pasūtījuma slepkavībām. Autore jau iepriekš minēja, ka viens no kibernoziegumu stūrakmeņiem ir tieši anonimitāte, un tieši *deep web* pastāvošā anonimitāte ir tā vislielākais drauds.

Kā piemēru jāmin situācija, kad kāda persona valstī A izveido mājaslapu, kura satur bērnu pornogrāfiju, kuras nelikumīgais saturs veido noziedzīga nodarījuma sastāvu, un mājaslapas saturs ir pieejams lietotājiem visā pasaulē, vai šādā situācijā visas pasaules valstis, kurās mājaslapas saturs tiek apskatīts, ir tiesīgas vērsties pret šo personu?[122] Šāds gadījums būtu vistiešākais piemērs attecināt universālās jurisdikcijas principa nozīmi un mērķi uz kibernoziegumiem. Šādā gadījumā persona teorētiski atrodas vienā mirklī jebkurā pasaules vietā.

Pēc autores domām, universālās jurisdikcijas attiecināšana uz kibernoziegumiem būtu liels solis to novēršanā un apkarošanā, jo šībrīža tiesiskais regulējums nespēj nodrošināt efektīvu cīņu ar pieaugošo kibernoziegumu skaitu. Šāds regulējums arī atrisinātu situāciju ar tām trešajām valstīm, kurās nepastāv nacionālais regulējums attiecībā uz kibernoziegumiem vai kuras nav Konvencijas par kibernoziegumiem līgumslēdzējpuses.

Jurisdikciju konflikti ir tikai viena no problēmām, kas traucē izmeklēt un atrisināt kibernoziegumus. Kā jau iepriekš minēts, būtiska ir problēma ir jurisdikciju principu piemērošanas robežām, tomēr jāpiemin arī nepietiekamas iespējas informācijas apmaiņai, tehniskas grūtības kibernoziedznieku izsekošanā, kvalificētu speciālistu trūkums, un nepastāvīga sadarbība ar pārējām iesaistītajām personām, kas atbildīgas par kiberdrošību. Kā Eiropas Policijas akadēmijas (CEPOL) konferencē „Kibernoziegumi – stratēģiskais līmenis" norādīja Latvijas Republikas Iekšlietu ministrs Rihards Kozlovskis "Ņemot vērā kibernoziedzības draudu globālo raksturu, īpaša loma cīņā pret kibernoziedzību ir sadarbībai un efektīvai saziņai starp valstīm un tiesībaizsardzības iestādēm".[123] Kā konferences galveno secinājumu attiecībā uz kibernoziegumu apkarošanu un prevenciju, jāizvirza tieši starptautiskās sadarbības uzlabošana valstu starpā, kā arī sadarbība ar privāto sektoru.[124]

---

[121]Deep Web: The proverbial safe house for cybercriminals.
Pieejams:https://www.wired.com/insights/2013/08/deep-web-the-proverbial-safe-house-for-cybercriminals/ [aplūkots: 29.04.2017].
[122]Betsy Rosenblatt. Principles of Jurisdiction, Paper.
Pieejams: https://cyber.harvard.edu/property99/domain/Betsy.html [aplūkots: 28.02.2017].
[123]Valstīm jāsaskaņo izmeklēšanas metodes cīņā pret kibernoziegumiem. Jurista Vārds, 30.03.2015.
[124] Ibid.

Neraugoties uz progresu, joprojām pastāv vairāki šķēršļi, lai Eiropas līmenī efektīvi izmeklētu kibernoziegumus un sodītu pārkāpējus. Izmantojot stabilitātes instrumentu, Eiropas Savienība vēršas arī pret strauji augošajiem transnacionālajiem draudiem, kas saistīti ar kibernoziedzību attīstības un pārejas posma valstīs, kurās bieži trūkst nepieciešamie resursi, lai apkarotu šo organizētās noziedzības formu. [125]

Problēma ar jurisdikcijas konfliktiem kibernoziegumos ir neizbēgama, balstoties uz nenosakāmo noziegumu piesaisti reālai valsts teritorijai. Lai gan Konvencija par kibernoziegumiem jurisdikcijas konfliktu gadījumā uzliek līgumslēdzējpusēm pienākumu konsultēties, lai noteiktu vispiemērotākās jurisdikcijas īstenošanu, tomēr nav precīzi noteikts, kā jāveic "konsultēšanās procedūra". Pēc autores domām, konvencija nepiedāvā reālu risinājumu jurisdikcijas konfliktu gadījumos, un neparedz konkrētu darbību kopumu, kas veicams, rodoties konfliktam.

[125] Komisijas paziņojums Padomei un Eiropas parlamentam. Vēršanās pret noziedzību mūsu digitālajā laikmetā: Eiropas Kibernoziedzības centra izveide. Briselē, 2012.gada 28.martā. Pieejams: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0140_/com_com(2012)0140_lv.pdf [aplūkots: 11.05.2017].

KOPSAVILKUMS

Pētījuma rezultātā autore izvirza šādas tēzes:

1. Visbiežāk piemērotākais no jurisdikcijas principiem ir teritoriālais princips, balstoties uz tā sasaisti ar valsts suverenitāti un valsts tiesībām savas teritorijas ietvaros saukt pie atbildības jebkuru personu, kura pastrādā noziedzīgo nodarījumu. Attiecībā uz kibernoziegumiem, Konvencija par kibernoziegumiem, kura paredz principa piemērošanu , nesatur pietiekami detalizētu regulējumu par to, kas tiek uzskatīts par "teritoriju", jo interneta vide jeb kibertelpa nav mērāma telpā.
2. Nacionālā jurisdikcijas principa piemērošana neveido problēmas ar konkrētas teritorijas noteikšanu, tomēr šis jurisdikcijas princips rada problēmas gadījumos, kad noziedznieka valsts, kuras pilsonis veicis noziedzīgu nodarījumu kibertelpā nav ieinteresēta saukt pie atbildības šo personu.
3. Konvencija par kibernoziegumiem *expressis verbis* neparedz pasīvā personālā principa piemērošanu, tomēr neizslēdz iespēju valstīm to piemērot, ja tas ir paredzēts tās normatīvajos aktos, kā, piemēram, tas ir paredzēts Latvijas Krimināllikums 4. panta trešā daļā. Likums paredz šī principa piemērošanu tikai gadījumos, kad pret Latvijas iedzīvotājiem ir pastrādāts "smags vai sevišķi smags noziegums". Panta piemērošanas problēma izriet no likumā noteiktā nosacījumu par noziedzīgo nodarījuma smaguma pakāpi, ņemot vērā, ka saskaņā ar Krimināllikumu pastāv gadījumu, kuros kibernoziegumi nekvalificējas kā "smagi", piemēram, 244.[1] panta noziedzīgais nodarījums.
4. Ir nepieciešams paplašināt universālās jurisdikcijas principa tvērumu, piemērojot to uz kibernoziegumiem, ņemot vērā to globālo izplatību. Tomēr problēma rastos gadījumā ja viena valsts, izveidojot regulējumu noteiktu "monopolu" kibernoziegumu regulēšanā.
5. Latvijas Krimināllikuma panti, kas regulē neatļautas darbības ar automatizētu datu apstrādes sistēmām, nesatur detalizētu seku uzskaitījumu, kā rezultātā kļūst komplicēta noziedzīga nodarījuma kaitējuma konstatēšana. Kaitējuma konstatēšana kibernoziegumos ir sarežģīta, jo nelikumīgo darbību, kas tiek veiktas pret datu apstrādes sistēmām, sekas bieži vien nav nosakāmas likuma noteiktajās robežās.

6. Nepastāvot divpusējiem starpvalstu izdošanas līgumiem, nav iespējams panākt taisnīgu kibernoziedzīgo nodarījumu iztiesāšanu, ņemot vērā iespējamu valstu politisko ieinteresētību neizdot vainīgās personas saukšanai pie atbildības.
7. Kibernoziegumi atbilst visiem trīs "starptautiska kriminālnozieguma" kritērijiem, līdz ar to, būtu pamats kvalificēt tos par starptautiskiem noziegumiem.
8. Vienota regulējuma trūkums attiecībā pret kibernoziegumiem var novest pie potenciālas vainīgās personas izvairīšanās no atbildības par noziedzīgiem nodarījumiem un soda nesaņemšanas.
9. Jurisdikcijas principu hierarhijas nepastāvēšana noved pie jurisdikcijas konfliktiem, kuru novēršanai un piemērotākā principa noteikšanai, Konvencija par kibernoziegumiem nepiedāvā risinājumu.

IZMANTOTĀS LITERATŪRAS SARAKSTS

Literatūra

1. Ray August, “International Cyber-Jurisdiction: A Comprative Analysis”, American Law Journal, vol.39 (summer, 2002)
2. Susan W.Brenner and Bert-Jaap Koops. “Approches to Cybercrime Jurisdiction”,p.4. According to Ian Brownlie, Principles of Public International Law, 5th ed., Oxford, University Press, 2002 (1998)
3. Chawki, A.Darwish, M.A.Khan, S.Tyagi. Cybercrime, digital forensics and jurisdiction. Springer international Publishing, 2015
4. A. Judins Krimināl atbildības izslēdzamības apstākļi, Rīga, Tiesu namu aģentūra,
5. U.Ķinis. Kibernoziedzība, kibernoziegumi un jurisdikcija. Apgāds ”Jumava”, Rīga, 2015
6. U.Ķinis. Jurisdikcija un kibernoziegumi. Apgāds ”Jumava”, Rīga, 2013.
7. U.Krastiņš. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Tiesu namu aģentūra, Rīga, 2014.,
8. U.Krastiņš. Noziedzīgs nodarījums. Tiesu namu aģentūra, Rīga, 2000
9. J.Klabbers. International law. Cambridge University Press, United Kingdom, 2013.,
10. A. Klip. European Criminal law, 2nd edition. Cambridge, Intersentia, 2012
11. Victoria Neufeldt and David B. Guralnik. Webster’s New world dictionary, Third college, 1989., p. 1283.
12. C.Ryngaert. Jurisdiction in international law. Oxford; New York: Oxford University Press, 2008
13. C. Schwarzenegger. The emergence of EU criminal law. Hart Publishing, 2014,
14. S.Summers. The emergence of EU criminal law, cyber crime and the regulation of internet society. Oxford publishing, 2014.,
15. Risk, Internet and E-Commerce, Insurance and Reinsurance Legal issues, Edited by Robert Hammesfahr of Blatt Hammesfahr & Eaton, London, Reactions Publishings Group Ltd., 2000

Normatīvie akti

16. Apvienoto Nāciju Organizācijs Jūras tiesību konvencija un nolīgums par tās XI daļas īstenošanu. Pieejams: http://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A21998A0623(01) [aplūkots: 10.04.2017].

17. Konvencija par Kibernoziegumiem. Pieejams: https://likumi.lv/doc.php?id=146481 [aplūkots: 12.04.2017].
18. Par Latvijas Republikas valdības un Amerikas Savienoto Valstu valdības līgumu par izdošanu. Publicēts: "Latvijas Vēstnesis", 93(3669),12.06.2007., "Ziņotājs",
19. Statute of the International Court of Justice. Pieejams: http://www.icj-cij.org/documents/index.php?p1=4&p2=2& [aplūkots:14.05.2017].
20. Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime. Pieejams: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VNC624sW [aplūkots: 13.05.2017].
21. Eiropas Parlamenta un Padomes direktīva 2013/40.ES (2013.gada 12.augusts) par uzbrukumiem informācijas sistēmām, 12.pants. Pieejams: http://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:32013L0040 [aplūkots: 12.05.2017].
22. Komisijas paziņojums Padomei un Eiropas parlamentam. Vēršanās pret noziedzību mūsu digitālajā laikmetā: Eiropas Kibernoziedzības centra izveide. Briselē, 2012.gada 28.martā. Pieejams: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0140_/com_com(2012)0140_lv.pdf [aplūkots: 11.05.2017].
23. Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committe of the regions. Brussels, 08.05.2013. Pieejams: http://ec.europa.eu/justice/citizen/files/com_2013_270_en.pdf [aplūkots: 17.04.2017].
24. The working party on the protection of individuals with regard to the processing of personal data. Recommendation 3/97 Anonymity on the internet, adopted by working party, 3.December 1997. Pieejams: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf [aplūkots: 12.05.2017].
25. Latvijas Republikas Satversme, Publicēts: "Latvijas Vēstnesis", 43, 01.07.1993., "Ziņotājs", 6, 31.03.1994.
26. Krimināllikums, Publicēts: "Latvijas Vēstnesis", 199/200 (1260/1261), 08.07.1998.
27. Kriminālprocesa likums. Publicēts: "Latvijas Vēstnesis", 74(3232), 11.05.2005.
28. Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību. Publicēts: "Latvijas Vēstnesis", 331/332 (1392/1393), 04.11.1998.

29. Igaunijas Sodu kodekss. Pieejams: https://www.riigiteataja.ee/en/eli/522012015002/ [aplūkots: 20.04.2017].
30. Restatement (third) of the foreign relations law of the United States,1987, Section 402(g).- Jurisdiction To Prescribe-Comment. Pieejams: https://jura.urz.uni-heidelberg.de/mat/file_viewer.php?fid=10946 [aplūkots: 12.05.2017].

Periodika

31. Constitutional limits over exterritorial jurisdiction: terrorism and the intersections of national and international law by Anthony J. Colangelo. //Harwardnint. Law. Journal, vol.48, Number one, Winter 2007
32. Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention Cybercrime. Pieejams: http://www.ejls.eu/6/78UK.htm [aplūkots: 13.04.2017].
33. Ghorbani A. & Ghorbani A. (2014) Investigating computer crimes in cyberspace. Kuwait Chapter of the Arabian Journal of Bussiness and Managment Rewiew, 3(10), p. 299-403. Pieejams: http://platform.almanhal.com/Files/?ID=T2-74850-MLA0028934.pdf [aplūkots: 15.05.2017].
34. D.Ivašins. Krāpšana kibertelpā kā viens no internetnoziegumu veidiem.//Administratīvā un Krimināla Justīcija,2/2012
35. U. Ķinis. Kibernoziegumi un kriminālprocess. Jurista Vārds, 20.02.2001., Nr. 4 (197).
36. U.Ķinis. Krāpšana automizētu datu apstrādes sistēmā. Jurista Vārds, 15.07.2014., Nr. 27 (829)
37. V.Liholaja, D.Hamkova. Būtiska kaitējuma izpratne: likums, teorija,prakse. Jurista Vārds, 10.01.2012., Nr. 2 (701).
38. Betsy Rosenblatt.Principles of Jurisdiction. Pieejams: https://cyber.harvard.edu/property99/domain/Betsy.html [aplūkots: 28.02.2017].
39. Tallin manual on the International law applicable to cyber warfare. Pieejams: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [aplūkots: 17.04.2017].
40. Valstīm jāsaskaņo izmeklēšanas metodes cīņā pret kibernoziegumiem. Jurista Vārds, 30.03.2015.
41. Van Bockel W.B. Two perspectives on the realization of the ne bis in idem principle in Europe. Pieejams: https://www.academia.edu/19950258/Two_Perspectives_on_the_Realization_of_the_European_I_ne_bis_in_idem_I_Principle [aplūkots: 19.05.2017].

42. Wang W. Cybercrime and cyberspace. Pieejams: http://www.swansea.ac.uk/library/archive-and-research-collections/hocc/communicationsandtheinternet/sociallifeoftheinternet/cybercrime/cybercrimeandcyberspace/ [aplūkots: 17.04.2017].
43. A brief history of Cybercrime. Pieejams: http://content.time.com/time/nation/article/0,8599,1902073,00.html [aplūkots: 12.05.2017].
44. Ar "naudas mūļu" ķeršanu vien nepietiek – ES stirprinās cīņu ar kibernoziegumiem. Pieejams: http://www.lsm.lv/lv/raksts/arzemes/zinas/ar-naudas-mulu-kersanu-vien-nepietiek--es-stiprinas-cinu-ar-kibernoziegumiem.a172328/ [aplūkots: 12.05.2017].
45. ASV tiesas spriedums: Čalovskim vairs nav ilgāk jāpaliek ieslodzījumā. Pieejams: http://www.lsm.lv/raksts/zinas/latvija/asv-tiesas-spriedums-calovskim-vairs-nav-ilgak-japaliek-ieslodzijuma.a162766/ [aplūkots: 12.05.2017].
46. Convention on Cybercrime. Pieejams: https://en.wikipedia.org/wiki/Convention_on_Cybercrime [aplūkots: 28.04.2017].
47. Čalovski izdod tiesāšanai ASV. Pieejams: http://www.lsm.lv/raksts/zinas/latvija/calovski-izdos-tiesasanai-asv.a62573/ [aplūkots: 13.05.2017].
48. Cybercrime and Internet jurisdiction by H.Kaspersen, March 5, 2009, CoE Project on cybercrime. Discussion paper. Pieejams: http://www.coe.int/t/dghl/cooperation/economic-crime/cybercrime/Documents/reports-presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf [aplūkots: 15.04.2017].
49. Cybercrime in the Deep Web. Pieejams: https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-In-The-Deep-Web-wp.pdf [aplūkots: 16.05.2017].
50. Cybercrime Legislation Worldwide. Pieejams: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx
51. Deep Web: The proverbial safe house for cybercriminals. Pieejams: https://www.wired.com/insights/2013/08/deep-web-the-proverbial-safe-house-for-cybercriminals/ [aplūkots: 29.04.2017].

52. Domēna vārds. Pieejams: https://www.hostnet.lv/domena-vards/ [aplūkots: 15.04.2017].

53. ECT pieņem pieteikumu par Čalovski; aptur viņa izdošanu. Pieejams: http://www.lsm.lv/raksts/zinas/latvija/ect-pienem-pieteikumu-par-calovski-aptur-vina-izdosanu.a62721/ [aplūkots: 12.05.2017].

54. Eiropas Cilvēktiesību tiesa pasludina spriedumu lietā Čalovskis pret Latviju. Pieejams: http://www.mfa.gov.lv/ministrija/latvijas-parstavis-starptautiskajas-cilvektiesibu-institucijas/aktualitates/eiropas-cilvektiesibu-tiesa-pasludina-spriedumu-lieta-calovskis-pret-latviju [aplūkots: 12.05.2017].

55. Eurojust legal framework. Pieejams: http://www.eurojust.europa.eu/careers/Documents/AD2017/VN_Administrative%20Director_17EJ01_AD14_LV.pdf [aplūkots: 14.05.2017].

56. Hakeri no Indijas uzbrūk flīžu veikalam un divreiz izdzēš tā datus. Pieejams: http://www.lsm.lv/raksts/latvija/zinas/hakeri-no-indijas-uzbruk-latvijas-flizu-veikalam-un-divreiz-izdzes-ta-datus.a229497/ [aplūkots: 18.05.2017].

57. International Criminal Law – Defining international crimes. Pieejams: //http://law.jrank.org/pages1382/international-criminal-law-defining-international-crimes.html [aplūkots: 01.05.2017].

58. Inside the Hunt for Russia's Most Notorious Hacker. Pieejams: https://www.wired.com/2017/03/russian-hacker-spy-botnet/ [aplūkots: 12.05.2017].

59. Internet. Pieejams: http://searchwindevelopment.techtarget.com/definition/Internet [aplūkots: 12.05.2017].

60. Internets. Pieejams: https://lv.wikipedia.org/wiki/Internets [aplūkots: 12.05.2017].

61. Julian Assange Fast Facts. Pieejams: http://edition.cnn.com/2013/01/18/world/julian-assange-fast-facts/ [aplūkots: 23.04.2017].

62. Latvijas Kiberdrošības stratēģija. 2014-2018. Pieejams: https://www.unodc.org/res/cld/lessons-learned/lva/latvijas_kiberdrobas_stratija_html/Kiberdrosibas_strategija.pdf [aplūkots: 13.04.2017].

63. Norton by Symantec. Cybercrime report 2011., p.1. Pieejams: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf [aplūkots: 12.05.2017].

64. Rinkēvičs apšauba Imantas hakera izdošanu tiesāšanai ASV. Pieejams: http://www.lsm.lv/raksts/dzive--stils/tehnologijas-un-zinatne/rinkevics-apsauba-imantas-hakera-izdosanu-tiesasanai-asv.a53349/ [aplūkots: 12.05.2017].

65. Russian Espionage Piggybacks on a Cybercriminal's Hacking. Pieejams: https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=1 [aplūkots: 12.05.2017].

66. The next generation of cybercrimes. How it has evolved and where it is going. Pieejams: http://www.allstream.com/wp-content/uploads/2015/11/white-paper-cybercrime.pdf [aplūkots: 16.04.2017].

67. The Top Countries For Cybercrime. Pieejams: https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/2007/07/13/cybercrime-world-regions-techcx_ag_0716cybercrime.html&refURL=https://l.facebook.com/&referrer=https://l.facebook.com/ [aplūkots: 20.04.2017].

68. The working party on the protection of individuals with regard to the processing of personal data. Recommendation 3/97 Anonymity on the internet, adopted by working party, 3.December 1997. Pieejams: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf [aplūkots: 12.05.2017].

69. The World's Most Wanted Hacker Sounds Like a Goddamn James Bond Villain. Pieejams: http://gizmodo.com/the-worlds-most-wanted-hacker-sounds-like-a-goddamn-jam-1793211745 [aplūkots: 25.04.2017].

70. Top 10 countries with most hackers in the worl. Pieejams: https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e [aplūkots: 15.05.2017].

71. Top 10 countries worst hit by hackers. Pieejams: http://www.guidingtech.com/67467/top-hacked-countries-data-breaches-identities-stolen/ [aplūkots: 13.05.2017].

72. Valstīm jāsaskaņo izmeklēšanas metodes cīņā pret kibernoziegumiem. Pieejams: https://eu2015.lv/lv/jaunumi/zinas/1136-valstim-jasaskano-izmeklesanas-metodes-cina-pret-kibernoziegumiem [aplūkots: 12.05.2017].

73. What we know about Russia's interference in the US election. Pieejams: https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election [aplūkots: 15.04.2017]

74. Yahoo! Inc.v. La Ligue Contre Le Racisme et l'Antisemitisme. Pieejams: https://en.wikipedia.org/wiki/Yahoo!_Inc._v._La_Ligue_Contre_Le_Racisme_et_l%27Antisemitisme [aplūkots: 15.05.2017].

75. Žurnālisti Lielbritānijā atrod ilgi meklēto draugiem.lv krāpnieku Pieejams: https://defense.lv/2015/02/09/zurnalisti-lielbritanija-atrod-ilgi-mekleto-draugiem-lv-krapnieku/ [aplūkots: 13.05.2017]

76. 1 Billion plus Yahoo account information hacked; Safeguard yours. Pieejams: http://www.guidingtech.com/62880/1-billion-yahoo-accounts-hacked/ [aplūkots: 20.05.2017].

77. 20 Eye-Opening Cybercrime Statistics. Pieejams: https://securityintelligence.com/20-eye-opening-cybercrime-statistics/ [aplūkots: 12.05.2017].

Judikatūra

78. Satversmes tiesas 2012.gada 18.oktobra spriedums lietā 2012-02-0106, 11.punkts. Pieejams:http://www.satv.tiesa.gov.lv/wp-content/uploads/2012/01/2012-02-0106_Spriedums.pdf [aplūkots: 13.05.2017].

79. Satversmes tiesa atteic ierosināt lietu par Latvijas un ASV līgumu par izdošanu. Pieejams: http://www.satv.tiesa.gov.lv/press-release/satversmes-tiesa-atteic-ierosinat-lietu-par-latvijas-un-asv-ligumu-par-izdosanu/ [aplūkots: 12.05.2017].

80. Permanent Court of International Justice (Ordinary) Session, The Case of the S.S. Lotus, France v. Turkey, 7 September 1927. Pieejams: http://www.internationallawbureau.com/blog/wp-content/uploads/2012/07/The-SS-Lotus-Case.pdf [aplūkots: 11.04.2017].

81. U.S.A. v. Ivanov (2003), 172 C.C.C. (3d) 551 (Nfld.C.A.). See also U.S. Department of Justice. United States Attorney, "Russian Man Sentenced for Hacking into Computers in the United States". Pieejams:

https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/ivanovSent.htm [aplūkots: 10.05.2017].

Bakalaura darbs „Jurisdikcija par noziedzīgiem nodarījumiem kibertelpā" izstrādāts Latvijas Universitātes Juridiskās fakultātes Krimināltiesiko zinātņu katedrā.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autore: Aleksandra Gavrilova

Rekomendēju/nerekomendēju darbu aizstāvēšanai

Vadītāja: docents Diāna Hamkova

Recenzents:

Darbs iesniegts Krimināltiesisko zinātņu katedrā

Dekāna pilnvarotā persona: metodiķe Iveta Balode

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē

Prot. Nr.

Komisijas sekretārs: