LATVIJAS UNIVERSITĀTE
JURIDISKĀ FAKULTĀTE
KRIMINĀLTIESISKO ZINĀTŅU KATEDRA

KRIMINĀLATBILDĪBA PAR PATVAĻĪGU PIEKĻŪŠANU AUTOMATIZĒTAI DATU APSTRĀDES SISTĒMAI

BAKALAURA DARBS

Autors: **Einārs Janukovičs**
Studenta apliecības Nr.: **ej12013**
Zinātniskais konsultants: docente, **Dr.iur. Diāna Hamkova**

RĪGA 2015

ANOTĀCIJA

Krimināllikuma 241.pantā ietvertais noziedzīgais nodarījums regulē atbildību par patvaļīgu piekļūšanu automatizētai datu aizsardzības sistēmai, bet praksē nereti tiek novērots, ka uz šo nodarījumu un nodarījumu grupu prakse vēl svārstās un nav īstas skaidrības kā kvalificēt šos nodarījumus. Krimināllikumā pastāv sodi par līdzīgiem nodarījumiem, kuri tiek regulēti dažādās nodaļās. Latvijas tiesām arī nav īstas skaidrības kā sodīt personas, kuras izdarījušas šo noziedzīgo nodarījumu ārvalstīs, kamēr tās atrodas Latvijas teritorijā. Tiks doti piemērotākie risinājumi, lai praksē varētu veiksmīgāk kvalificēt šo noziedzīgo nodarījumu.

Atslēgvārdi: Patvaļīga piekļuve automatizētai datu apstrādes sistēmai, kibernoziegumi, jurisdikcija, informācijas sistēma, kibertelpa.

ANNOTATION

Criminal law article 241 included Criminal responsibility for unauthorized access to automated data processing system, but in practice are often observed, that on this offense and offense group practice is still fluctuating and there is no real clarity as to the classification of these offenses as the Latvian Criminal Law. In Criminal Law are penalties for similar offenses which are regulated in different chapters. And the Latvian courts do not have a real clarity as to punish the person who committed the offense abroad while the person is in Latvian territory. Will be given the most appropriate solutions to be more successful in practice to gualify the offense.

Keywords: Unauthorized access to automated data processing system , cybercrime, jurisdiction, information system, cyberspace.

SATURA RĀDĪTĀJS

IEVADS

Analizējot Krimināllikuma (turpmāk – KL) 241.pantā minēto noziedzīgo nodarījumu par patvaļīgu piekļūšanu datu apstrādes sistēmām, rodas jautājums, kā tiek kvalificēts šis nodarījums, jo piekļūt pie datora var gan attālināti, gan būt fiziski klātesot šai sistēmai. Ar Krimināllikuma 2005. gada 26.maija grozījumiem tikai grozīts iepriekšējais Krimināllikuma regulējums par patvaļīgu piekļūšanu datorsistēmai, kuru rezultātā tika paplašināts panta regulējamais loks, kas varētu būt saistīts ar to, ka Latvija 2006.gada 5.oktobrī pieņēma sev par saistošu Konvenciju par Kibernoziegumiem, tādējādi vajadzēja mainīt Krimināllikuma redakciju atbilstoši konvencijas regulējumam, lai harmonizētu konvencijas dalībvalstu regulējumus attiecīgajā noziedzīgā nodarījumā. Bez tā Krimināllikumā pastāv līdzīgi noziedzīgi nodarījumi, kurus varētu attiecināt arī uz KL 241.pantā regulējamo loku.

Ints Ķuzis norādījis[1] intervijā, ka strauji pieaug kibernoziegumu skaits, bet speciālistu trūkst, tādējādi ir grūti notvert šīs vainīgās personas. Pat ja izdodas noskaidrot tās, tad vēl valsts dienestiem ir jāsaskaras ar citu valstu jurisdikcijām.

Ja personas atrodas ārzemēs, sarežģīti sodīt vainīgās personas, jo dažās valstīs var būt, ka par šo noziedzīgo nodarījumu nemaz nav paredzēts sods. Un arī Latvijas tiesa nespēj veiksmīgi risināt šos jautājumus, pārsvarā atstājot to citu valstu tiesām.

Ņemot vērā šos apstākļus, autors izvirza mērķi: sniegt vispārēju izpratni par patvaļīgu piekļuvi automatizētai datu apstrādes sistēmai, vērtēt tās atbilstību Kibernozieguma konvencijā dotajam regulējumam, noskaidrot vai Latvijas regulējums spēj sasniegt savu mērķi, ieteikt pareizāko risinājumu kā Latvijas tiesu prakse varētu risināt šo noziedzīgo nodarījumu, ja tiek konstatētas jurisdikcijas problēmas.

Lai sasniegtu attiecīgos mērķus, autors: analizēs KL 241.panta saturu, salīdzinās ar līdzīgiem noziedzīgiem nodarījumiem, kuri doti Krimināllikumā,

[1]Pērn Latvijā reģistrēti aptuveni 400 kibernoziegumi http://www.tvnet.lv/tehnologijas/internets/553247-pern_latvija_registreti_aptuveni_400_kibernoziegumi [aplūkots 18.04.2015.]

aplūkos veiksmīgākos risinājumus, kā tikt galā ar jurisdikcijas problemātiku un salīdzinās KL 241. pantu ar ārvalstu attiecīgajām normām.

Lai sasniegtu izvirzītos mērķus, bakalaura darbā tiks izmantota vairākas zinātniskās metodes:

1) Gramatiskā metode – jēdzienu interpretēšanai;
2) Salīdzinoša metode – salīdzinot ar citu valstu regulējumiem;
3) Induktīvā metode – nosakot vispārīgus secinājumus no iegūtajiem faktiem;
4) Deduktīvā metode – tiesību normu interpretācija;
5) Teleoloģiskā metode – nosakot normu mērķus.

Darbs sastāv no četrām daļām, pirmajā daļā tiks aplūkota patvaļīgas piekļūšana automatizētām datu apstrādes sistēmām izpratne, otrajā daļā tiks analizēts panta sastāvs un tā kvalifikācija, trešajā daļā tiks skatīta jurisdikcijas problemātika un ceturtajā daļā tiks salīdzināts Latvijas regulējums ar ārvalstu regulējumu.

1. Patvaļīgas piekļūšana automatizētai datu apstrādes sistēmām izpratne

1.1 Patvaļīga piekļuve

Lai persona gūtu jebkādu iespēju izdarīt darbības informācijas sistēmā, vispirms tai jāpiekļūst sistēmas informācijas un tehniskajiem resursiem.[2] Tātad patvaļīga, neatļauta piekļuve informācijas sistēmu resursiem vienmēr ir saistīta ar zināmiem nosacījumiem, bez kuru iestāšanās tā nevar tikt realizēta, tas ir, vēršanās pret sistēmā noteikto piekļuves kārtību. [3] Šī kārtība var būt: 1) piekļuvi iegūst, izmantojot viltotus identifikatorus un pieejas kodus; 2) patvaļīga nepieskatītas datorsistēmas lietošana, kad tā lietotājs likumīgi ir pieslēdzies sistēmas resursiem, izmantojot savas piekļuves tiesības.[4]

Saskaņā ar Latvijas Zinātņu akadēmijas Terminoloģijas komisijas slēdzienu piekļūšana ir: "Noteiktiem nosacījumiem pakļautas ekskluzīvas vai neekskluzīvas iekārtu, resursu vai pakalpojumu piekļuves sniegšana citam elektronisko sakaru komersantam. Tiek nodrošināta piekļuve: 1) tīkla elementiem, resursiem un ar tiem saistītām iekārtām, kas var ietvert arī pieslēgumu tīklam; [..] 3) infrastruktūrai, ieskaitot ēkas, kabeļu līnijas un antenu mastus; [..] 4) atbilstošām programmatūras sistēmām, ieskaitot operētājsistēmas u. c." [5]

Jāatzīst, ka šādu piekļuves jēdzienu krimināltiesībās piemērot ir ļoti grūti.[6] Vienīgais, ko no šīs definīcijas var saprast, ir tas, ka piekļuve ir saistāma ar nosacījumiem pakalpojumu saņemšanai.[7] Daudz plašāku un skaidrāku definīciju sniedz ANO vadībā izstrādātais ITU Instrumentārijs kibernoziegumu definēšanai.[8] Dokumentā sniegta šāda piekļuves tehniskā definīcija: *"Piekļuve aptver jebkuru darbību, kas nodrošina ieiešanu sistēmā; sistēmā glabāto informācijas resursu apskati, parādīšanu, koriģēšanu un cita veida apstrādi; datu izgūšanu, kopēšanu,*

[2] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 123.lpp
[3] Turpat 124.lpp
[4] Turpat 124.lpp
[5] Ķinis U. Nodarījumi pret informācijas sistēmu drošību, Jurista Vārds, 27.09.2011. Nr. 39 (686) http://www.juristavards.lv/doc/236587-bnodarijumi-pret-informacijas-sistemu-drosibub/ [aplūkots 20.03.2015]
[6] Turpat.
[7] Turpat.
[8] Turpat

pārvietošanu, papildināšanu, grozīšanu vai dzēšanu; sistēmas resursu vai daļas izmantošanu, veicot jebkuras sistēmas elementa, tajā skaitā datorprogrammu, datoru, datorsistēmu, tīklu un to piederumu, loģiskās un aritmētiskās atmiņas, datu pārraides, datu saglabāšanas, procesoru, datoru atmiņas funkciju komponentu konfigurāciju vai rekonfigurāciju, tieši vai netieši izmantojot šim nolūkam fiziskos vai virtuālos līdzekļus, to skaitā elektroniskos, magnētiskos, audio, optiskos." [9]

No ITU definīcijas var secināt, ka piekļuve aptver jebkuru darbību, kas nodrošina piekļuvi sistēmas resursiem, kā arī Krimināllikuma regulēta patvaļīga piekļuve.[10] Tāpēc, definējot automatizētas datu apstrādes sistēmas (turpmāk – ADAS) piekļuves tiesības, jēdzienam ir jāatbilst šādam kritērijam: piekļuves tiesībām jāattiecas tikai uz autorizētiem lietotājiem, kuriem ir tiesības pieslēgties sistēmas resursiem un iegūt nepieciešamo informāciju vai pieprasīt to.[11] Savukārt piekļuves tiesības sastāv no diviem elementiem: (a) personai piešķirtiem identifikatoriem un to identifikācijas un (b) sistēmas spējas pēc šiem identifikatoriem atpazīt lietotāju, to autorizēt un dot piekļuvi attiecīgiem sistēmas resursiem. [12]

Šādi personai piešķirtie identifikatori varētu būt, lietotāja vārds, personīgais atpazīšanas kods (PIN), parole, viedkarte u.c.[13] To sarežģītības pakāpe atkarīga no sistēmā esošās informācijas klasifikācijas pakāpes.[14] Ja sistēmā tiek apstrādāta konfidenciāla informācija, tad personai piešķirtie identifikatori ir stingrāki.[15] Ja sistēma neapstrādā tādu informāciju, kuras atklāšana vai sabojāšana var radīt draudus citiem lietotājiem, tad piešķirtie identifikatori ir primitīvāki.[16] Šie identifikatori dod iespēju tām personām, kurām ir atļauja, piekļuvi sistēmai un aizsargā no neautorizētas piekļuves, personām, kurām nav šādas tiesības . Vēl tiek pieskaitīta lietotājam deleģētās tiesības lietot sistēmā esošos resursus, ievadīt jaunu

[9] Ķinis U. Nodarījumi pret informācijas sistēmu drošību, Jurista Vārds, 27.09.2011. Nr. 39 (686) http://www.juristavards.lv/doc/236587-bnodarijumi-pret-informacijas-sistemu-drosibub/ [aplūkots 20.04.2015]
[10] Turpat.
[11] Turpat
[12] Turpat.
[13] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 126.lpp
[14] Turpat
[15] Turpat.
[16] Turpat.

informāciju, apstrādāt to, īstenot piekļuvi konkrētiem informācijas apgabaliem u.c.[17]

ADAS piekļuves tiesiskais raksturojums ir arī atkarīgs no tā, kam pieder šī informācijas sistēma.[18] Ja ADAS turētājs ir valsts vai pašvaldība, tad piekļuves kārtību reglamentē normatīvie akti.[19] Ja ADAS īpašnieks vai tiesiskais valdītājs ir komersants vai privātpersona, tad piekļuves tiesību saturu reglamentē iekšējās kārtības noteikumi.[20]

Definējot patvaļīgās piekļuves nosacījumus, likumdevējam nepieciešams vadīties no lietotāju piešķirto tiesību apjoma.[21] Šis tiesību saturs ietver: 1) tiesības reģistrēties kā ADAS lietotājam, izmantojot sev piešķirtos identifikatorus. Šīs tiesības vēl nekādā gadījumā nedod pilnīgas pieejas tiesības visiem sistēmas resursiem; 2) tiesības pēc reģistrēšanās sistēmā iegūt pieeju un izmantot tikai tos ADAS resursus, kurus tiem atļāvis lietot sistēmas īpašnieks vai viņa pilnvarotā persona; 3) lietot šos resursus likumīgs lietotājs var tikai tādā veidā un kārtībā, kā to pilnvarojis sistēmas īpašnieks vai viņa pilnvarotā persona.[22]

1.2 Automatizēta datu apstrādes sistēma

Viens no krimināatbildības nosacījumiem ir patvaļīgas piekļūšanas saistība ar datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšanu, kas var izpausties kā to apiešana vai salaušana. Ar šiem aizsardzības līdzekļiem saprot informācijas un programmatūras aizsardzības līdzekļus, kas nodrošina informācijas sistēmas lietotāju identitātes un piekļuves tiesību pārbaudi, pasargā informāciju no tīšas vai nejaušas grozīšanas (bojāšanas) vai dzēšanas (iznīcināšanas).[23] Izstrādājot Krimināllikuma 241.panta jauno redakciju (2005. gada 28. aprīļa redakcija), U.

[17] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 126.lpp
[18] Ķinis U. Nodarījumi pret informācijas sistēmu drošību, Jurista Vārds, 27.09.2011. Nr. 39 (686) http://www.juristavards.lv/doc/236587-bnodarijumi-pret-informacijas-sistemu-drosibub/ [aplūkots 20.03.2015]
[19] Turpat
[20] Turpat.
[21] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 127.lpp
[22] Turpat.
[23] Ķinis U. Nodarījumi pret informācijas sistēmu drošību, Jurista Vārds, 27.09.2011. Nr. 39 (686) http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 17.03.2015]

Ķinis ieteica izmantot terminu "automatizētu datu apstrādes sistēmu (ADAS)", argumenti, kāpēc tika izvēlēts minētais termins ir šādi[24]:

1) termins precīzi apzīmē to, ka Krimināllikuma 241.-244.pantā nodarījuma priekšmets ir tikai tā sistēmas, kas veic automatizētu datu apstrādes procesu, tas ir, šo datu apstrādes procesu vada un organizē fiziska persona, pamatojoties uz programmu, kura spējīga veikt automātisko datu apstrādi;
2) jebkurā ADAS ir savstarpēji saistīti jeb integrēti informācijas un tehniskie resursi, tātad, nodalāmi no nodarījumiem pret informācijas sistēmu drošību piekļūšanu publiski pieejamām mājas lapām vietās, kur to funkcionēšanu nodrošina atbalsta tehnoloģijas nolūkā tās sabojāt vai izmantot citos noziedzīgos nolūkos, piemēram, krāpniecisku darbību veikšanai, goda un cieņas aizskaršanai, huligānisku darbību izdarīšanai u.c.;
3) termins "automatizētu datu apstrādes sistēma" ietver gan individuālo datoru, datorsistēmas, gan mobilās un stacionārās telekomunikācijas iekārtas, gan arī elektroniskos tīklus;
4) tas ir tehnoloģiski neitrāls, tā saturu nevar ietekmēt modernie zinātnes sasniegumi tiktāl, ciktāl vien pastāvēs automatizēts datu apstrādes process. Konstruējot Krimināllikumā noziedzīgā nodarījuma sastāvus pret informācijas sistēmu drošību, jāievēro divi faktori, pirmkārt, šiem nodarījumiem nereti ir starptautisks raksturs.

Konstruējot šos noziedzīgo nodarījumu sastāvus, tie ir jāveido, lai tos varētu piemērot arī pret personām, kuras uzbrūk Latvijas esošām ADAS veicot no citu valstu teritorijām .[25]

Automatizēts

Latvijas Zinātņu akadēmijas Terminoloģijas komisija ir noteikusi, ka automatizēts ir tāds (mehānisms, ierīce), kura darbojas bez tiešas cilvēku līdzdalības.[26] Tas var būt pilnīgi jebkas, kā piemēram, automātiskā lidojumu vadības sistēma, kura nodrošina automātisku lidmašīnas vadību gaisā, bez pilota iejaukšanās, no tā brīža, kad pilots ieslēdz šo sistēmu. Kā arī, sakaru torņi, tajos atrodas tehniskās ierīces, kuras nodrošina sakaru nodrošinājumus cilvēkiem, un vēl

[24] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 225.lpp
[25] Turpat. 226.lpp
[26] Terminu un svešvārdu skaidrojošā vārdnīca, vārds - automātisks. http://www.letonika.lv/groups/default.aspx?r=1107&q=autom%C4%81tisks&id=993817&g=1 [aplūkots 17.03.2015]

var minēt, automatizētās ierīces industriālās rūpnīcās, kuras saliek kopā detaļas produktiem, lai darbi tiktu pastrādāti efektīvāk.

Datu apstrāde

Organizētas darbības ar datiem. Piemēri: aritmētiskas vai loģiskas darbības ar datiem, datu saplūdināšana vai sašķirošana, programmu asamblēšana vai kompilēšana un tādas operācijas ar tekstu kā rediģēšana, šķirošana, saplūdināšana, noglabāšana, ieguve, parādīšana uz ekrāna un drukāšana.[27]

Datu apstrādes sistēmas

Apstrādes metožu, programmatūras un aparatūras kopums, kas sadarbībā ar apkalpojošo personālu nodrošina automatizētu datu apstrādi.[28] Kā piemēru var ņemt, persona ievada datorprogrammā skaitļus, kurus tai ir nepieciešams atrisināt vai apkopot, ievadot šos skaitļos un norādot tajā programmatūra, nepieciešamās funkcijas kuras jāveic, tajā brīdi, kad persona ir apstiprinājusi funkciju darbības izpildi, dators vai serveris, veic visas nepieciešamās darbības šo funkciju izpildīšanai.

1.3 Aizsardzības līdzekļi

Par aizsardzības līdzekļiem KL 241.panta izpratnē var minēt, ugunsmūrus. Ugunsmūris tiek uzstādīts datorā, lai to pasargātu no citu lietotāju attālinātas nesankcionētas piekļuves jūsu datoram un tajā esošajai informācijai[29]. Ugunsmūri var lietot, lai bloķētu vīrusus un surogātpastu, un tas ir vērtīgs rīks, lai aizsargātu bērnus tiešsaistē.[30]

Ugunsmūris var pasargāt: no vīrusiem; no spiegprogrammatūras un reklāmprogrammatūras; no surogātpasta; no uznirstošajiem logiem; no nevēlamas

[27]Terminu un svešvārdu skaidrojošā vārdnīca, vārds - automātisks. http://www.letonika.lv/groups/default.aspx?r=1107&q=datu%20apstr%C4%81de&id=2635837&g=1 [aplūkots 17.03.2015]
[28]Terminu un svešvārdu skaidrojošā vārdnīca, vārds-datu apstrādes sistēma. http://www.letonika.lv/groups/default.aspx?cid=967984&r=1107&lid=967984&g=1&q=datu%20apstr%C4%81de&h=6145 [aplūkots 17.03.2015]
[29] Ugunsmūris http://drossinternets.lv/page/72 [aplūkots 21.03.2015]
[30] Turpat.

piekļuves personiskajai informācijai.[31] Līdz ar to dators tiek aizsargāts no šiem draudiem, ar šo programmatūras palīdzību.

Bet ne vienmēr ugunsmūris spēj pasargāt no šiem draudiem, jo hakeri[32] atrod jaunas iespējas un paņēmienus kā apiet ugunsmūra aizsardzību. Pie aizsardzības līdzekļiem vēl ir pieskaitāmi pretvīrusa programmas. Šīs programmatūras pārbauda datoru (parasti, to ieslēdzot), atrodot vīrusus un atbrīvo no tiem. Pretvīrusu programmatūra var pasargāt no personisko datu zuduma, datora bojāšanas, personas identitātes zādzībām, krāpšanas.[33]

Līdz ar to, patvaļīgas piekļuves jēdziens, Krimināllikumā ar skaidri definēts un ir saprotams, ar ko to likumdevējs ir vēlējies regulēt. Kibernozieguma konvencijas[34] 2. pantā definētais patvaļīgas piekļuves skaidrojums un salīdzinot to ar Krimināllikuma doto regulējumu, tad tie ir salīdzinoši vienādi.

[31] Ugunsmūris http://drossinternets.lv/page/72 [aplūkots 21.03.2015]
[32] Hakeris- Cilvēks, kas interesējas par datoriem, programmēšanu.
[33]Pretvīrusu programmatūra http://drossinternets.lv/page/64 [aplūkots 21.03.2015]
[34] Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. Pieejams - http://likumi.lv/doc.php?id=146481 [aplūkots 16.04.2015]

2. Patvaļīgas piekļūšanas automatizētai datu aizsardzības sistēmai sastāva analīze

KL 241.panta skaidrojumā nav dots sīkāks paskaidrojums, kas tad ir šī panta objekts, ir zināms grupas objekts - vispārējā drošība un sabiedriskā kārtība. Bet ko tieši KL 241.pants aizsargā? Jo panta pirmajā daļā ir norādīts, ka tiek sodīta par to, ka patvaļīgi piekļūst datu apstrādes sistēmas resursiem, pārvarot sistēmas aizsardzības līdzekļus. Kas tad būtu šie sistēmas resursi? Vai nebūtu vienkāršāk šo pašu noziedzīgo nodarījumu aptvert ar KL 177.[1] pantu? Augstākās tiesas Krimināllietu departaments lietā SKK – 349/2014, ir norādījis, kaut arī KL 177.[1] pants norāda uz tādu pašu nodarījumu kā KL 241.pants, tas būtu pret automatizētām datu apstrādes sistēmām, bet KL 177.[1] panta noziedzīgā nodarījuma objektīvā puse ļauj nošķirt no citiem līdzīgiem noziedzīgiem nodarījumiem.[35] U.Ķinis rakstā „Krāpšana automatizētā datu apstrādes sistēmā" norādījis, ka termins „automatizēta datu apstrādes sistēma" ietver datorsistēmu, tīklu, tehnisko un informācijas resursu kompleksu, kam ir lietotāju pieeja. Tādējādi par automatizētu datu apstrādes sistēmu Krimināllikuma izpratnē atzīstama jebkura ierīce, kuras primārais mērķis ir automatizēta datu apstrāde. Turklāt automatizētu datu apstrādes sistēma ir integrēta ar elektroniskiem tīkliem un tai ir lietotāju pieeja, piemēram, mobilais telefons, ar tīklu savienots dators, planšete u.c.[36]

Augstākā tiesa arī atzina, ka par automatizētu datu apstrādes sistēmu nav atzīstamas sadzīves elektroniskās ierīces, spēļu, biļešu, kafijas u.c. automāti, kuru galvenais uzdevums ir par samaksu sniegt konkrētai personai mantisku tiesību vai konkrētu mantu, jo to primārā funkcija nav automatizēta datu apstrāde. Datu ievadīšana automatizētu datu apstrādes sistēmā var notikt tikai tad, ja tā var ietekmēt automatizētu datu apstrādes sistēmā esošo datu apstrādes procesu. Datu ievadīšana ir normāla automatizētu datu apstrādes sistēmas datu apstrādes funkcija. Dati ir saistāmi ar simboliem, burtiem, lielumiem, kas sagatavoti apstrādei automatizētās datu apstrādes ierīcē. Automatizētu datu apstrādes sistēma datu apstrādes procesā var tikt izmantota gan kā rīks, ar kuru dati tiek ievadīti, gan kā

[35] LR Augstākā tiesa Krimināllietu departaments 2014. gada 27.augusta lēmums Lietā Nr. SKK-349/2014 4.lpp [aplūkots 16.04.2015]
[36] Turpat 5.lpp

objekts, kas glabā datus, gan arī kā medijs datu pārraidei. Taču nekādas saistības ar datu apstrādi nav personu darbībām, kas saistītas ar fizisku darbību pret konkrēto apdraudējuma priekšmetu – sišana, speršana, monētu, kuponu iemešana automātos, ierīču atslēgšana no strāvas padeves.[37] Līdz ar to, darba autors sīkāk izpētīs KL 241.panta sastāva analīzi un noskaidros panta mērķi.

2.1 Objekta analīze

KL 241. panta aizsargājamais objekts būs, tiešais objekts, tas ko tieši aizkars, šis noziedzīgais nodarījums. Tiešais šo noziedzīgo nodarījumu apvienojošais objekts ir tiesiskās intereses realizēt informācijas drošību, tas ir, nodrošināt informācijas sistēmu resursu pieejamību, integritāti un konfidencialitāti.[38]

Tātad par informācijas sistēmas drošību tiek uzskatīta specifiski aizsargājamas intereses, kuru mērķis ir nodrošināt informācijas sistēmas resursu uzturēšanu normālā darba kārtībā, lai sistēmas informācijas resursi saglabātu savu integritāti, lai varētu tai piekļūt visi reģistrētie lietotāji. [39] Tas ir, ka šai piekļuvei jābūt nepārtrauktai un informācija, kas glabājas, tiktu nodrošināta pret iespējām sistēmā iekļūt un iegūt šo informāciju. Tā ir informācija, kuru persona glabā kādā datu glabātuvē, uz datora, datu nesējā, vai telefonā. Līdz ar to šis aizsargājamais objekts ir jāskatās šaurāk, tādā ziņā, ka tas neskar gadījumus, kad tiek sabojāti šie datu nesēji, kur tiek uzglabāta informācija, ja bojājums ir radies mēģinot iegūt šos datus.

Aizsardzība iestājas brīdi, kad nodarījumi ir saistīti ar informācijas sistēmas datu un resursu traucēšanu, programmu bojāšanu, galvenokārt ir vērsti pret sistēmas īpašnieka, vai tiesiskā valdītāja vai informācijas resursu īpašnieku interesi saglabāt sistēmā esošo informāciju nemainīgā stāvokli, uzturēt tās veselumu.[40] Šie nodarījumi nav vērsti, lai tiktu bojāti materiāli taustāmi objekti, bet gan nemateriāli priekšmeti, tādi, kas atrodas arī kibertelpā[41]. Tā būtu uzskatāma vieta, kura nav

[37] LR Augstākā tiesa Krimināllietu departaments 2014. gada 27.augusta lēmums Lietā Nr. SKK-349/2014
[38] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g., 109.lpp
[39] Latvijas Universitātes raksti. Juridiskā zinātne. Nr. 667. U. Ķinis."patvaļīga piekļūšana datorsistēmai"(KL241.pants) priekšmeta kvalifikācijas problēmas 17.lpp
[40] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g., 110.lpp
[41] Cyberspace definition http://www.thefreedictionary.com/cyberspace [aplūkots 09.04.2015]

sasniedzama cilvēka ķermenim, un tā radusies, laikā gaitā attīstoties datortehnoloģijām. Kibertelpas galvenā iezīme ir internets un cilvēks, un mijiedarbība starp abām šīm lietām. Bet ne visa informācija un dati, kas atrodama ir pieslēgta internetam, piemēram, persona A glabā visus savus dokumentus, bildes, video datorā, kurš nav pieslēgts interneta savienojumam. Tad, kādā veidā persona varēs, kurai ir vēlme, iegūt šo informāciju. Autors uzskata, ka nav nepieciešams obligāts internets, lai varētu pārkāpt sistēmas drošību. Ar to domājot, ka pietiek pieslēgt citu sistēmu klāt otrai, tādā veidā, kā ar vadiem saslēdzot, bet visas darbības persona veiktu caur savu rīku, kas varētu būt, planšete, telefons, dators. Bet šajā gadījumā, personai vajadzētu atrasties fiziski klāt vienā telpā ar informācijas sistēmu, bet fiziski neiedarbojoties uz to. Tikai pieslēgties sistēmas iekšējam tīklam, ja tāds pastāv.

Bet kā pats galvenais, tiek uzsvērts uz to, ka noziedzīgais nodarījums vērsts uz šo informācijas sistēmu. Tādēļ darba autors uzskata ka visas darbības ir vērstas uz to, lai iegūtu to informāciju, kas tiek glabāta personas sistēmā. Tādējādi, personai nemaz nebūtu nepieciešams piekļūt šai sistēmai, pārvarot visus aizsardzības līdzekļus, ja tur neatrastos nekāda informācija. Tāpēc šis pants būtu jāpārveido, lai radītu materiālu sastāvu, nevis formālu.

Kas tad, KL 241.panta izpratnē ir uzskatāms par priekšmetu, ja par priekšmetu parasti uzskata sataustāmas lietas. Piemēram, telefons, dators, krēsls, tad kā, mēs varam sataustīt informāciju, kas atrodas datu glabātuvē? Kā tiesību zinātnieki ir norādījuši, ka šī panta analizējamais priekšmets ir telekomunikāciju sistēma - strukturizēts informācijas tehnoloģiju un datu bāzu kopums.[42] Šajā gadījumā ir U. Ķiņa viedoklis, ka informācija un vieta, kur tā informācija atrodas ir jāskatās saistīti. Tādā ziņā, ka informācija tukšā gaisā nevar atrasties, tai ir kaut kur jāglabājas, lai būtu pieejamai personai lietošanai. Ja informācija glabājas attiecīgās informācijas sistēmas datu nesējā, tad tā kļūst par šīs sistēmas informācijas resursu neatņemamu sastāvdaļu un uzskatāma par materiālas kustamas mantas (informācijas sistēmas tehnisko resursu) kā galvenās lietas piederumu, un gadījumos, ja persona nelikumīgi iekļūst telpā, kur atrodas datorsistēmā, un fiziski piekļūst šīs sistēmas resursiem, tad šāda darbība ir kvalificējama pēc KL 175.p 3.

[42] Krastiņš U., V. Liholaja, A, Niedre. Krimināllikuma zinātniski praktiskais komentārs, sevišķā daļa 3, Rīga, 2007.g. 251.lpp

daļas kā zādzība, kas saistīta ar iekļūšanu telpā.[43] Bet ja šī darbība ir veikta attālināti, fiziski neaizskarot datu sistēmu, tad tā ir kvalificējama kā kibernoziegums.[44]

Bet problemātiskākais varētu būt jautājums, kā kvalificēt, ja informācija neatrodas uz datu nesēja, datora, bet gan *mākonī* (cloud) vai mākoņdatošana.[45] Jo visa *mākoņa* būtība ir tāda, ka informācija, kas pieder cilvēkam, bet lai tā neaizņemtu daudz vietas uz datora noglabā *mākonī.* Tas ir, ka tiek pirkta no pakalpojuma sniedzēja, datu glabāšanai nepieciešamā atmiņa. Iegūstot šo vietu mākonī, persona var glabāt datus un tiek piešķirts identifikators, kurš var sastāvēt no lietotāja vārda un paroles.

Darba autors uzskata, ka ja arī personas informācija ir noglabāta mākonī, tā ir saistīta ar šo personu, tādā ziņā, ka tajā atrodas viņam piederoša, personīga informācija. Tas ir gadījumos, ja ir strīdi par to, kam pieder tie dati, pakalpojuma sniedzējam vai lietotājam, kurš glabā tos datus. Un kā ir noteikts Fizisko personu datu aizsardzības likuma 14.panta 1.daļā, ka persona noslēdz rakstveida līgumu, ar datu apstrādes pārzini. Līdz ar to šis noslēgtais līgums norāda saistību ar mākonī esošo informāciju un personu, kurai tā pieder. Un līgumā būtu vēlams norādīt, ka visi dati pieder personai, nevis pakalpojuma sniedzējam, ja gadījumā, pakalpojuma sniedzējs bankrotē.[46]

2.2 Objektīvā puse

Noziedzīgā nodarījuma objektīvo pusi raksturo obligātās pazīmes un papildpazīmes. Pie obligātajam pazīmēm, kas raksturo nozieguma objektīvo pusi, pieder darbība vai bezdarbība, un to rezultātā nodarītais kaitējums un cēloņsakarība starp personas aktīvo prettiesisko uzvedību un sekām, bet papildpazīmes var būt vieta, laiks, izdarīšanas vieta, nozieguma izdarīšanas rīks u.c.[47]

---

[43] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 113.lpp
[44] Turpat.
[45]DATU VALSTS INSPEKCIJA. Rekomendācija «Personas datu apstrādes drošība» http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Rekomendacija_PDA_drosiba_2014.pdf [aplūkots 09.04.2015]
[46]Cloud Storage: 4 Legal Issues You Need to Know http://www.inc.com/samuel-wagreich/the-4-things-you-must-have-in-your-contract-with-your-cloud-provider.html [aplūkots 09.04.2015]
[47] Ķinis U. Kibernoziegumi, Rīga, 2007, 116.lpp

KL 241.panta atbildība noteikta par patvaļīgu (bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības) piekļūšanu automatizētai datu apstrādes sistēmai vai tās daļai, kas sodāma ar nosacījumu: 1) ja tas saistīts ar datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšanu; 2) ja ar to radīts būtisks kaitējums (materiāls sastāvs).[48]

Nozieguma objektīvo pusi veido aktīva darbība – piekļūšana ADAS, kas ir patvaļīga, tas ir, iekļūstot tur bez atļaujas vai izmantojot citai personai piešķirtas tiesības.[49]

Aplūkosim nosacījumu, ja tas ir saistīts ar datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšanu. Kā jau darba sākumā norādīju, tad ir šādi aizsardzības līdzekļi, ugunsmūris, antivīruss u.c.

Aizsardzības līdzekļu pārvarēšanai ir nepieciešama aktīva, kaitīga un prettiesiska darbība, kas vērsta pret vienu vai vairākiem informācijas sistēmu drošības elementiem (konfidencialitāti, integritāti vai pieejamību), tad jābūt kaitīgajām sekām, kas var izpausties gan materiāli, morāli, politiska vai organizatoriska kaitējuma radīšanā un visbeidzot, cēloņsakarība, ka jebkura kaitīgā darbība, kas vērsta pret informācijas sistēmu drošību, likumsakarīgi un nepieciešami rada citu parādību.[50] Kā redzams no objektīvās puses pazīmes, tad likumdevējs neatzīst par noziedzīgu nodarījumu patvaļīgu piekļuvi sistēmai, ja tā nebūs nodrošināta ar attiecīgiem aizsardzības līdzekļiem. Tāpēc ADAS drošības parametriem jābūt tādiem, lai šai personai būtu pilnīgi un nepārprotami skaidrs, ka viņas pieslēgšanai ADAS vai tās daļai ir patvaļīga un neatļauta. Ja persona, zinādama to, ka viņai nav tiesību piekļūt ADAS resursiem, izmanto speciālās metodes un salauž vai apiet loģiskās aizsardzības līdzekļus, tad, ja ir iestājušās attiecīgās sekas, persona saucama pie krimināatbildības pēc KL 241.panta.[51]

Grūtāk ir noteikt no kurienes šīs darbības ir uzsāktas, jo nereti, personas, kuras veic šos noziedzīgos nodarījumus neveic kopā, tas ir, atrodoties vienā vietā, bet gan dažādās, iespējams katra savā valstī. Tādējādi jāskatās katras valsts

[48] Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724) http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 09.04.2015]
[49] Turpat.
[50] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g., 122.lpp
[51] Turpat 230.lpp

regulējums atsevišķi. Kā piemēru var ņemt, 2013.gada Novembra sākumā, kad Latvijas teritorija notika NATO militārās mācības "Steadfast Jazz 2013", ir bijuši veikti vairāki mēģinājumi ielauzties un radīt problēmas civilo, valsts un institūcijas sistēmā, kā norādīts ziņojumā, tad tas nav noticis no valsts teritorijas, bet gan no ārienes.[52] Jo tehnoloģijām attīstoties, arī personas, kuras veic šos uzbrukumus ir grūtāk notvert. Par patvaļīgu piekļūšanu var atzīt, tikai tādu darbību, ja uzbrucējam ir bijis nepieciešams pārvarēt datu aizsardzības līdzekļus, ja šādi līdzekļi nav bijuši izstrādāti, tad tā nav uzskatāma par patvaļīgu piekļūšanu ADAS. Tikai persona, kurai pieder sistēma, var atzīt, ka darbība, kas ir veikta ir bijusi patvaļīga vai nē.[53] Jo tikai sistēmas īpašnieks un pārvaldītājs var noteikt vai persona, kura ir iekļuvusi sistēmā ir bijusi pielaide. Tas vairāk sarežģi iespēju noteikt vai ir bijis pārkāpums. Ja arī personai ir bijusi pielaide sistēmai, tad ir jānoskaidro cik liela pielaide sistēmai ir bijusi personai.[54] Tādējādi, vērtējot nosacījumu, vai darbība veikta bez atļaujas vai izmantojot citai personai piešķirtas tiesības, krimināprocesā svarīgi būtu arī izvērtēt apstākļus, kā pārkāpējs ir ieguvis citam lietotājam piešķirtus identifikatorus.[55]

KL 241.panta 2.daļā ir kvalificētais sastāvs, kurā noteikts, ja šo noziedzīgo nodarījumu izdara mantkārīgā nolūkā. Tas būtu, ja persona vēlas gūt mantisku vai citāda rakstura labumu sev vai citai personai.[56] Attiecīgi uz KL 241.panta nodarījumu, varētu būt gadījums, ja persona patvaļīgi piekļūstot citas personas datoram, kur atrodas informācija par biržu akcijas cenām, kuras būtu ieteicams pirkt un kuras nē, līdz ar to, ja vainīgā persona izmantotu šādu informāciju, lai gūtu sev materiālu labumu, būtu saucama pie atbildības pēc KL 241.p 2.daļas noziedzīgo nodarījumu.

Obligāta objektīvās puses pazīme ir nodarījuma sekas – būtisks kaitējums, tāpēc jākonstatē, ka patvaļīgas piekļūšanas automatizētai datu apstrādes sistēmai

[52] Militāro mācību "Steadfast Jazz 2013" laikā notikušie kiberuzbrukumi bijuši "ārējas izcelsmes" http://www.focus.lv/latvija/viedokli/militaro-macibu-steadfast-jazz-2013-laika-notikusie-kiberuzbrukumi-bijusi-arejas-izcelsmes [aplūkots 10.04.2015]

[53] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g., 122.lpp

[54] Ķinis U Nodarījumi pret informācijas sistēmu drošību Jurista Vārds27.09.2011. Nr. 39 (686) https://defense.lv/wp-content/uploads/2011/09/uldis_kinis_kriminallikuma_piemerosanas_problemas.pdf [aplūkots 10.04.2015]

[55] Turpat.

[56] Krastiņš U., V. Liholaja, A, Niedre. Krimināllikuma zinātniski praktiskais komentārs, sevišķā daļa 3, Rīga, 2007.g. 252.lpp

rezultātā ir vai nu nodarīts ievērojams mantiskais zaudējums un apdraudētas vēl citas ar likumu aizsargātās intereses un tiesības, vai arī šāds citu ar likumu aizsargātu interešu un tiesību apdraudējums ir ievērojams.[57] Kā skaidrots likuma "Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību" 23. panta otrajā daļā[58], par ievērojamu mantisko zaudējumu atzīstams mantiskais zaudējums, kas nodarījuma izdarīšanas brīdī pārsniedz piecu tajā laikā Latvijas Republikā noteikto minimālo mēnešalgu kopsummu, kas, piemēram, pēc U. Ķiņa ieskata, varētu tikt aprēķināts, ņemot vērā 1) zaudējumus, kas saistīti ar sistēmas dīkstāvi; 2) izdevumus, kas saistīti ar bojātās informācijas atjaunošanu vai tās aizstāšanu; 3) izdevumus, kas saistīti ar jaunu programmatisku resursu instalēšanu, kas paredzēti sistēmas drošības funkciju atjaunošanai; 4) izdevumus, kas saistīti ar sistēmas lietotāju piekļuves tiesību korekciju; 5) neiegūto peļņu, ja sistēma sniedz maksas informācijas pakalpojumus.[59] Par būtisku kaitējumu var būt ne tikai, tādi nodarījumi, kuros ir konstatēti lieli materiāli zaudējumi, bet arī tādi, kuros konstatē lielu apdraudējumi aizsargātajām interesēm.[60] KL 241.panta noziedzīgajā nodarījumā, par šādu kaitējumi varētu uzskatīt, patvaļīga iekļūšana valsts iestāžu datu sistēmās, nenodarot materiālus zaudējumus. Šāda piekļuve valsts iestāžu sistēmai var radīt draudus, personu un valsts drošībai, jo tajā var atrasties personīga informācija, personas kodi un dzīvesvietas adrese un cita informācija, bet otrs gadījums, ja tajos atrodas valsts informācija, kura nav paredzēta publiskai apskatei. KL 241.panta 3.daļā ir norādīta uz ADAS, kas apstrādā, kā apstrādāt informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību. Šī panta daļa tika grozīta pamatojoties uz Direktīvu Nr. 2013/40/ES, kur tiek norādīts,

[57]Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724) http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 10.04.2015]

[58] Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību. Pieejams - http://likumi.lv/doc.php?id=50539 [aplūkots16.04.2015]

[59] Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724) http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 10.04.2015]

[60] Liholaja V Hamkova D. Būtisks kaitējums izpratne: likums, teorija, prakse. Jurista Vārds, 10.01.2012., Nr. 2. (701).
Pieejams - http://www.juristavards.lv/doc/242455-butiska-kaitejuma-izpratne-likums-teorija-prakse/ [aplūkots 08.05.2015]

ka Eiropas Savienībā pastāv vairākas kritiskas infrastruktūras, ja gadījumā tiktu iegūta informācija no šīm sistēmām, tas varētu apdraudēt Eiropas Savienību.[61]

Pēdējā laikā Latvijas tiesu praksē par KL 241.panta 3.daļas noziedzīgu nodarījumu skandalozāko ir bijusi I. Poikāna lieta, kurā faktiskie apstākļi norāda uz to, ka viņš esot nopludinājis no VID EDS sistēmas iegūtos vairāku valsts uzņēmumu algu sarakstus.[62] Analizējot I. Poikāna veiktās darbības un publiski izskanējušo informāciju par tām, zvērināts advokāts Mārtiņš Birks uzskata, ka Elektroniskās deklarēšanas sistēmas datu masveida lejupielādēšanai I. Poikāns izmantojis operētājsistēmas "Linux" standarta programmu "curl", kas ir publiski pieejams produkts datu lejupielādēšanai un pēc būtības nav nelikumīgs automatizētas datu apstrādes sistēmas resursu nelabvēlīgas ietekmēšanas līdzeklis.[63]

Tādējādi jāpieņem, ka I. Poikāns tikai izmainīja vienoto resursu vietrādi (URL), kas ir standartizēta resursa (kā dokuments vai bilde) adrese internetā, konkrētajā gadījumā, interneta adresi globālā tīmekļa (Web) pieteikumā, mainot tikai numerāciju adresēs uz sava datora.[64]

Apmeklējot tīmekļa vietni internetā (mājaslapā), dokumenti tiek lejuplādēti no datora sistēmas (tīmekļa vietnes servera) un īslaicīgi novietoti lietotāja datora atmiņā, kā arī parādīti lietotāja tīmekļa vietnes meklētājā. Izvēloties pieprasīt konkrēto tīmekļa vietni, ikviens var ieiet meklētājā ierakstītajā tīmekļa adresē (URL), noklikšķinot uz saites, kas ved uz konkrēto tīmekļa vietni, kas ir atrasta, vai arī tā tiek automātiski lejuplādēta ar citu tīmekļa adresē kodētu dokumentu.[65]

Katra tīmekļa adrese attiecīgajā tīmekļa programmā ietver skaitli, kas ir identifikācijas numurs lietotāja pieprasītajam dokumentam. Mainot šos numurus (par pamatu ņemot, piemēram, savu elektroniskās deklarēšanas sistēmas

[61] Eiropas parlamenta un padomes Direktīva 2013/04/ES, par uzbrukumiem informācijas sistēmām, un kuru aizstāj Padomes pamatlēmumu 2005/222/TI. Pieejams - http://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32013L0040&qid=1431336947563&from=LV [aplūkots 11.05.2015]
[62] Aiz Neo vārda, iespējams, slēpies LU pētnieks Ilmārs Poikāns http://www.delfi.lv/news/national/criminal/aiz-neo-varda-iespejams-slepies-lu-petnieks-ilmars-poikans-1744.d?id=31832311 [aplūkots 11.04.2015]
[63]Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724 http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 10.04.2015]
[64] Turpat.
[65] Turpat.

dokumentu) un pieprasot dokumentu no tīmekļa servera ar jaunu tīmekļa adresi, I. Poikāns varēja lejuplādēt jaunu dokumentu no tīmekļa servera.[66]

Visticamāk I. Poikāns automatizēja šo procesu, mainot vienoto resursu vietrādi (adresi internetā), un, apmeklējot tīmekļa vietni, lejuplādēja to uz sava datora, izmantojot nelielu datorprogrammu (skriptu), un, atkārtojot dokumentu numurus, lejuplādēja dokumentus no visdažādākajām adresēm internetā, kas tika saglabātas speciālā vietā datorā, nevis pagaidu kešatmiņā, kurā interneta pārlūkprogramma saglabā dokumentus pēc to parādīšanas.[67]

Tādu darbību rezultātā I. Poikāna datorā nonāca vairāki dati, kurus viņš apkopoja un faktiski atkārtoti publicēja interneta vietnē, kur šī informācija atkal (atkārtoti) bija pieejama jebkuram interneta lietotājam – gluži tāpat kā tajā brīdī, kad to sākotnēji ieguva I. Poikāns.[68] Darba autoram pēc šo apstākļu izklāsta rodas šaubas, vai I. Poikāna darbība būtu uzskatāma par KL 241.panta 3. daļas noziedzīgo nodarījumu, jo nav bijusi objektīvas puses pazīme, patvaļīga piekļūšana pārvarot datu aizsardzības līdzekļus. Jo kā jau iepriekš tika izskatīts, tad ir jābūt pārvarētiem šiem aizsardzības līdzekļiem, un ja šie aizsardzības līdzekļi nav, tad nebūtu pamata inkriminēt pēc KL 241.panta 3. daļas. Kā arī U.Ķiņis norādījis intervijā LTV[69] Denisa Čalovska lietā, un to pašu varētu attiecināt arī uz I. Poikāna lietu, ka tieši attiecībā uz kibernoziegumiem trūkst juridisko datu analīzes,. Darba autors uzskata, tādēļ, ka šāda veida noziedzīgi nodarījumi nav bijuši līdz šim brīdim tik ļoti aktuāli Latvijas tiesu praksē, kamēr tehnoloģijas pasaule attīstās un citu valstu tiesu prakse attīstās, Latvijas tiesu prakse šajos jautājumos nevirzās uz priekšu, nespējot rast risinājumus uz šiem jautājumiem.

Ir iespējami gadījumi, kad krimināltiesības neiestājas par KL 241.panta noziedzīgo nodarījumu. Gadījumā, ja personai nav bijis nodoms patvaļīgi iekļūt ADAS sistēmai, bet gan tikai pārbaudīt ADAS sistēmas drošību pret iespējamiem uzbrukumiem. Bieži vien, lieli IT uzņēmumi un arī bankas, izsludina konkursus

[66] Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724 http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 10.04.2015]
[67] Turpat.
[68] Turpat.
[69] Valdība nolemj izdot Denisu Čalovski ASV; ECT aptur izdošanu https://defense.lv/2013/08/11/valdiba-nolemj-izdot-denisu-calovski-asv-ect-aptur-izdosanu/ [aplūkots 11.04. 2015]

hakeriem, kuri spēs ātrāk ielauzties viņu sistēmās, ar mērķi norādot sistēmas vājos punktus, kur vajadzētu uzlabot aizsardzību pret iespēju ielauzties sistēmā.

2.3 Subjekts, subjektīvā puse

Subjekts.

Juridiskajā literatūrā faktiski pastāv relatīvi liela vienprātība, ka noziedzīgā nodarījuma subjekts ir pieskaitāma, Krimināllikumā paredzētu vecumu sasniegusi persona, kura vainojama noziedzīgā nodarījumā.[70] Tātad, lai personu varētu saukt pie krimināLatbildības, viņai obligāti jāpiemīt šādām pazīmēm: 1) jābūt fiziskai personai; 2) jābūt sasniegušai 14 gadu vecumu (KL 11.pants); 3) jābūt pieskaitāmai, tas ir, jāspēj saprast savas darbības un jāspēj tās vadīt; 4) jābūt tādai, kuras uzvedība ir aizliegta vai ierobežota krimināllikumā. Ja trūkst kāda no šīm pazīmēm, tad persona nevar tikt atzīta par noziedzīgā nodarījuma subjektu.[71]

Subjektīvā puse.

Subjektīvās puses jēdziens aptver subjekta psihisko attieksmi pret sabiedriski bīstamu nodarījumu. Juridiskajā literatūrā noziedzīgā nodarījuma subjektīvā puse definēta kā noziedzīgā nodarījuma sastāva elements, kas dod priekšstatu par iekšējiem psihiskiem procesiem, kas rodas tās personas apziņā, kura izdara noziedzīgu nodarījumu, un ko raksturo konkrēta vainas forma, motīvs, mērķis un emocijas. Respektīvi, noziedzīgā nodarījuma subjektīvā puse atspoguļo saistību starp personas apziņu, gribu un viņas izdarīto nodarījumu. Subjektīvās puses pamatpazīme ir vaina.[72]

Vaina ir personas psihiskā attieksme nodoma vai neuzmanības formā pret viņas izdarīto prettiesisko darbību vai bezdarbību un ar to saistītajām kaitīgajām sekām.[73] No subjektīvās puses Krimināllikuma 241. pantā paredzētais nodarījums ir tīšs noziegums, jo persona apzināti bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības piekļūst automatizētai datu apstrādes sistēmai vai tās

[70] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 117.lpp
[71] Turpat.
[72] Ķinis U. Nodarījumi pret informācijas sistēmu drošību, Jurista Vārds, 27.09.2011. Nr. 39 (686) Pieejams - http://www.juristavards.lv/doc/236587-bnodarijumi-pret-informacijas-sistemu-drosibub/ [aplūkots 20.03.2015]
[73] Krastiņš U. Noziedzīgs nodarījums. Rīga: Tiesu namu aģentūra, 2000.g., 90.lpp

daļai, pārvarot datu apstrādes sistēmas aizsardzības līdzekļus, vēloties radīt būtisku kaitējumu, apzināti pieļaujot tāda kaitējuma rašanos vai arī esot vienaldzīgai pret sava nodarījuma izraisītajām sekām.[74] Bet ko darīt, ja persona, piekļūst datu apstrādes sistēmai, nenojaušot, ka ir pārkāpusi datu aizsardzības līdzekļus. Vai tad vēl joprojām personu būtu sodāma pēc KL 241.panta? Pēc KL 10.panta dots skaidrojums, kad noziedzīgie nodarījumi ir izdarīti aiz neuzmanības. Un tur doti noziedzīgās pašpaļāvības un noziedzīgās nevērības skaidrojumi. Noziedzīga pašpaļāvība Krimināllikuma 10.panta izpratnē ir konstatējama gadījumos, kad persona, kas izdarījusi noziedzīgu nodarījumu, ir paredzējusi savas darbības vai bezdarbības seku iestāšanās iespēju, tomēr vieglprātīgi paļāvusies, ka tās varēs novērst jeb cerējusi, ka tās neiestāsies. Apzināta seku pieļaušana šajā gadījumā nav iespējama.[75] Bet kā U.Ķinis norādījis, ka kibernoziegumus, kas ir arī KL 241.panta noziedzīgs nodarījums, var izdarīt tikai ar tīšu vai netiešu nodomu, tātad KL 241.panta noziedzīgā nodarījuma subjektīvā puse vienmēr izpaudīsies tīšas darbības veidā.[76]

2.4 Kvalifikācijas nošķiršana no citiem kibernozieguma pantiem

Krimināllikumā bez KL 241.panta noziedzīgo nodarījumu par kibernoziegumiem regulē arī KL 243.-245.panti[77]. Jo kā, lai jurists spētu nošķirt tos gadījumus, kad jāpiemēro konkrētā norma. Jo visa darbība notiek kibertelpā, un visi nodarījumi ir pārsvarā vērsti pret sistēmas resursiem, līdz ar to aizskartais objekts neatšķiras no KL 241.panta, tas ir, informācijas sistēmas drošība. Bet vai tā tiešām ir? Tādējādi autors nedaudz aplūkos katru no minētājām normām un salīdzinās ar KL 241.panta regulējumu.

243.pants. Automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju. Jau pantā vērstais noziedzīgais nodarījuma objekts nav vērsts pret pieejamības tiesībām uz sistēmā

[74] Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724) http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 10.04.2015]

[75] LR Augstākās tiesas Krimināllietu departamenta 2009.gada 20.janvāra, lieta Nr. SKK-030/2009 [aplūkots 16.04.2015]

[76] Ķinis U. Kibernoziegumi, Rīga: Turība, 2007.g. 233.lpp

[77] Krimināllikums. LR likums. Pieejams - http://likumi.lv/doc.php?id=88966 [aplūkots 07.04.2015]

esošiem resursiem, kā tas ir KL 241pantā,[78] bet gan uz informācijas integritāti, tas ir, pret sistēmas īpašnieka vai likumīgā valdītāja interesi saglabāt informācijas sistēmas resursu veselumu.[79] Kuras var tikt apdraudētas ar vairākām darbībām.[80] KL 243.panta pirmajā daļā jau ir dotas norādēs, par tā, neatļautām darbībām, tās ir[81]:

Grozīšana – izmaiņu izdarīšana, aizstājot jebkādu tās elementu ar citiem elementiem;

Bojāšana – darbības, kuru rezultātā informācija daļēji zaudējusi savu sākotnējo kvalitāti un paredzēto nozīmi, taču pastāv iespēja to atjaunot;

Iznīcināšana – tāda iedarbība uz informāciju, kuras rezultātā tā vairs nav izmantojama pēc nozīmes un nav atjaunojama sākotnējā stāvokli;

Pasliktināšana – tāda iedarbība uz informāciju, kuras rezultātā tiek sabojāta tās struktūra, neciešot saturiskajam apjomam;

Aizklāšana – jebkura darbība, kas beidz pieeju datorsistēmā vai medijā saglabātiem datiem vai nu tāpēc, ka tie ir nodzēsti un fiziski vairs nepastāv, vai arī tie ir padarīti nepieejami un ekspluatācijai nederīgi.

Noziedzīgais nodarījums ir materiāls, jo nepieciešamas izdarīt šīs darbības, lai iestātos atbildība. Tātad, lai šī panta noziedzīgs nodarījums, tiktu uzskatīts par izdarītu ar šīm darbībām, ir jātiek sabojātai vai iznīcinātai aizsardzības sistēmai. Kā KL 241.pantā noteikts, tad, lai iestātos nodarījuma sekas ir nepieciešams pārvarēt, apejot aizsardzības līdzekļus, bet ne iznīcināt.

KL 243. panta 2. daļā noteiktas, citas darbības, lai iestātos šī panta daļas atbildība, tās ir, *par automatizētas datu apstrādes sistēmas darbības apzinātu traucēšanu, ievadot, pārnesot, bojājot, izdzēšot, pasliktinot, izmainot vai aizklājot informāciju, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma un radīts būtisks kaitējums*.

[78] Krastiņš U., V. Liholaja, A, Niedre. Krimināllikuma zinātniski praktiskais komentārs, sevišķā daļa 3, Rīga, 2007.g. 251.lpp
[79] Turpat. 253.lpp
[80] Krastiņš U., V. Liholaja, A. Niedre, Krimināltiesībās. Sevišķā daļa, Rīga: Tiesu namu aģentūra, 2009.g. 576.lpp
[81] Turpat.

Par katru no šiem darbības veidiem[82]:

Ievadīšana - kā viena no darbībām var būt "drazu pasts", tas ir, kad iesūtot liela apjomu šādu ziņu, tas var negatīvi ietekmēt datu apriti un sistēmas darbību;

Pārnešana –pārvietošana no vienas vietas uz citu;

Bojāšana – tāda iedarbība uz informāciju, kuras gala rezultātā informācija ir daļēji zaudējusi savu nozīmi, taču šo darbību ir iespējams atjaunot;

Izdzēšana – darbība, kas padara informāciju par neatpazīstamu un nelietojamu;

Pasliktināšana – darbība, ar kuru tiek sabojāta informācijas struktūra;

Izmainīšana – informācijas padarīšana par atšķirīgu no oriģināla;

Aizklāšana – darbība, ar kuru sākotnējo saturu padara par neredzamu vai aizslēpj aiz cita satura informācijas.

Subjektīvā puse - pantā minētās darbības var izdarīt tikai ar tiešu nodomu, pret mantiskajām sekām var būt arī netiešs nodoms, taču nodarīt kaitējumu personai smagu seku gadījumā var tikai aiz neuzmanības.[83] Ir atšķirība no KL 241.panta subjektīvas puses pazīmes, kur noziedzīgo nodarījumu varēja izdarīt ar tīšu nodarījumu. Un nav paredzēta cita iespēja kvalificēt subjektīvo pusi, attiecībā uz nodarījuma sekām, jo persona pilnībā apzinās, ka piekļūst datu sistēmai.

244.pants. Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm. Šī panta objektīvo pusi veido neatļautās darbības ar programmām Panta pirmajā daļā norādīts uz ierīci (arī datorprogrammu), kura paredzēta automatizētas datu apstrādes sistēmas resursu ietekmēšanai.[84] Programmas, kas var kaitīgi ietekmēt ir 1) datorvīrusi – speciāli veidotas datorprogrammas ar mērķi ietekmēt informācijas sistēmas resursus, 2) kaitīgās programmas - "tārps", loģiskās bumbas, Trojas zirgs, speciāli radītas programmas

[82] Krastiņš U., V. Liholaja, A. Niedre, Krimināltiesībās. Sevišķā daļa, Rīga: Tiesu namu aģentūra, 2009.g. 577- 578.lpp
[83] Turpat. 579.lpp
[84] Turpat. 580.lpp

ar mērķi apiet drošības sistēmu un veikt sistēmā konkrētu programmētāja noteiktu darbību.[85] Pēdējais nosacījums, lai varētu personu sodīt pēc šī noziedzīgā nodarījuma panta, ir jāveic vēl neatļautas darbības. Šīs darbības būtu[86]:

To izgatavošana - darbības veids, kā galarezultātā rodas datu komanda vai tehnisku ierīču objektīvs kopums, kas paredzēts datorsistēmas vai datortīkla resursu ietekmēšanai.

Pielāgošana izmantošanai - ierīces īpašību izmainīšana, lai to varētu izmantot datorsistēmas vai datortīklu resursu ietekmēšanai;

Realizēšana – ierīces, līdzekļa, datorprogrammas nodošana konkrētai personai par atlīdzību, bez tās;

Izplatīšana – iepriekš minēto nozieguma izdarīšanas rīku ievadīšana datorvidē, radot tās pieejamību – konkrētas ierīces nosūtīšana citiem lietotājiem vai konkrētai personai, kaitīgas programmas ievadīšana publiskā datu pārraides tīklā;

Glabāšana – jebkādas darbības, kas saistītas ar nozieguma rīka atrašanos vainīgā valdījumā.[87]

Šis noziedzīgais nodarījums ir ar materiālu sastāvu, jo nepieciešams veikt šīs darbības. Subjektīvā puse, šis nodarījums ir tīšs nodarījums, kuru raksturo tiešs nodoms, bet attiecībā pret sekām – netiešs nodoms vai neuzmanība.

Pēc šī panta noziedzīgā nodarījuma būtu skatāms Denisa Čalovska gadījums, ja viņš tiktu tiesāts Latvijā, nevis nodots ASV tiesai, jo kā mēdijos[88] ziņo, tad tiek apgalvots ka viņš ir palīdzējis radīt un izplatīt Gozī vīrusu, kurš esot inficējis vairāk nekā miljonu datoru pasaulē. *"Vīruss ielauzies ap 40 000 datoros ASV, to skaitā 160 ASV kosmosa aģentūras (NASA) datoros un izraisījis miljoniem dolāru lielus zaudējumus, norāda prokuratūra"*. Bet tā kā Latvijas varasiestādes nav varējušas pierādīt, ka Čalovskis ir vainīgs pēc KL 241.[1] panta darbībām, bet ASV FIB jau visus pierādījumus bija savākuši, tādēļ ir pieprasījuši Denisu Čalovski izdot ASV tiesai tiesāšanai. Kā arī Lauris Liepa norādījis, ka "*Krimināprocesa*

[85] Krastiņš U., V. Liholaja, A. Niedre, Krimināltiesībās. Sevišķā daļa, Rīga: Tiesu namu aģentūra, 2009.g. 581.lpp
[86] Turpat
[87] Turpat.
[88] Stāsts par Imantas hakeri http://www.rigaslaiks.lv/Raksts.aspx?year=2013&month=3&article=4 [aplūkots 14.04.2015]

likums paredz, ka Latvijas pilsoņa izdošanu var atteikt, ja noziedzīgs nodarījums pilnībā vai daļēji izdarīts Latvijas teritorijā."[89] Bet kā jau iepriekš darba autors norādījis, Latvijā trūkst zināšanu šādu gadījumu izskatīšanai, jo tiesām iespējams trūkst pieredzes un kvalifikācijas.

244.[1] pants. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām. Šis pants aizsargā to personu intereses, kuru elektronisko sakaru tīkla identificējamās galiekārtas (ierīces, kas paredzētas tiešai vai netiešai pieslēgšanai publiskā elektronisko sakaru tīkla pieslēguma punktiem, piemēram, tālruņa aparāti, faksi, modemi, datu pārraides iekārtas utt., kurām ražotājs piešķīris identifikatoru atpazīšanai elektronisko sakaru tīklā), nolaupītais, pazaudētais vai citādi pret īpašnieka gribu izgājušais no viņa varas.[90] Tas nozīmē, ka mobilo sakaru operatori pēc klienta pieprasījuma, var nobloķēt savu tālruni, ja tas ir pazudis vai nozagts. Taču pastāv iespēja tos izmantot citās valstīs, jo Latvijas mobilo skaru operatori šādas ziņas starptautiskajā datu bāzē nesniedz, kas tiek skaidrots ar to, ka daži mūsmāju operatori pieļauj nolaupītu galiekārtu izmantošanu ārvalstīs .[91]

Noziedzīgā nodarījuma objektīvo pusi veido, elektronisko sakaru tīkla galiekārtu identificēšanai elektronisko sakaru tīkla nepieciešamo datu izmainīšana bez ražotāja vai tā pilnvarotās personas piekrišanas.[92] Tas ir, ka visos telefonos atrodas IMEI kods, kurš ļauj identificēt šo tālruni ar citiem līdzīgiem tālruņiem, jo, pērkot veikalā mobilo tālruni, līgumā un dažreiz un iepakojuma ir norādīts šis IMEI kods, ka gadījumā, ja īpašnieks pazaudē savu tālruni, viņš to ziņo savam sakaru operatoram, nosaucot šo IMEI kodu, tālrunis tiek bloķēts. Bet zinošāki cilvēki, ar īpašam tehniskām dotībām spēj šo IMEI kodu izmainīt, tādējādi, nozagto tālruni pārdot melnajā tirgū iegūstot pelņu no tā. Subjektīvā puse - tīšs noziedzīgs nodarījums, ar formālu sastāvu, tas ir, ka ir jāizdara pantā noteiktās darbības, lai nodarījums tiktu atzīts par pabeigtu.

[89] Stāsts par Imantas hakeri http://www.rigaslaiks.lv/Raksts.aspx?year=2013&month=3&article=4 [aplūkots 14.04.2015]
[90] U. Krastiņš, V. Liholaja, A. Niedre, Krimināltiesībās, sevišķā daļa, Rīga: Tiesu namu aģentūra, 2009. g. 582.lpp
[91]Turpat.
[92] Turpat.

245.pants. Informācijas sistēmas drošības noteikumu pārkāpšana. Kā noteikts Valsts informācijas aprites likuma[93] 1.panta 1.daļā, tad informācijas sistēma ir strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana. Objektīvā puse ir informācijas noteikumu pārkāpšana, kas noveda pie informācijas nolaupīšanas, iznīcināšanas vai bojāšanas, un ja radīts būtisks kaitējums. Pantā noteikts speciālais subjekts, persona, kura ir atbildīga par šo noteikumu ievērošanu. Kā norādīts Valsts informācijas likuma 1.panta 2. un 3 daļa, tad šis speciālais subjekts ir:

valsts informācijas sistēmas pārzinis — valsts institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada valsts informācijas sistēmas darbību;

valsts informācijas sistēmas turētājs — valsts informācijas sistēmas pārzinis vai tā pilnvarota institūcija, kas uztur šīs sistēmas informācijas un tehnisko resursu funkcionalitāti un nodrošina informācijas apriti.

[93] Valsts informācijas sistēmu likums. LR likums. http://likumi.lv/doc.php?id=62324 [aplūkots 16.04.2015]

3. Jurisdikcijas nošķiršana

Kā KL 2.pantā noteikts, persona, kas izdarījusi noziedzīgu nodarījumu Latvijas teritorijā, atbild saskaņā ar šo likumu[94]. Diez gan loģisks risinājums, kad jāskatās, pēc kura likuma sodīt personu. Bet tas nav tik vienkārši ar tiem noziedzīgiem nodarījumiem, kuros tiek iesaistītas datorsistēmas un kibertelpa. Attīstoties informācijas tehnoloģijām, rodas aizvien jauni objekti, kas var kalpot gan kā apdraudējuma avots, gan arī kā apdraudējuma mērķis.[95] Kā piemērs varētu būt mākoņdatošana un dažādas tiešsaistes spēles, kuru serveri atrodas dažādās valstīs, un mākonī ieliktie dati, ne vienmēr atradīsies vienā vietā. Tādējādi uz mākoņdatni attiecināt nacionālās valsts jurisdikcijas ir ļoti problemātiski.[96] Elektroniskās vides, digitālās teritorijas jeb kibertelpas globālais raksturs rada situāciju, ka kibertelpa var tikt vērtēta gan kā ikvienas valsts jurisdikcijai pakļauta kvaziteritorija, gan arī bezjurisdikcijas telpa, uz kuru nepretendē nevienas valsts jurisdikcija.[97] Vienā teritorijā sagatavoti dati var tikt viegli ielādēti web serverī, kas atrodas pavisam otrā pasaules malā, bet, tiklīdz dati ir ielādēti web serverī, tie var kļūt pieejami jebkurā vietā, kur personai ir attiecīgs tehnoloģisks nodrošinājums. Tiesību zinātnieki ir devuši vairākas teorijas, kā skatīt šo jurisdikcijas problemātiku kibertelpā. Darba autors norādīs uz tām jurisdikcijas nošķiršanas teorijām, kuras veiksmīgāk atrisinātu nošķiršanu ar noziedzīgiem nodarījumiem, kuri pastrādāti kibertelpā.

Klātbūtnes doktrīna.

Noziedzīgā nodarījuma klātbūtnes doktrīna ir radusies un tiek plaši piemērota Apvienotās Karalistes un Britu sadraudzības valstu tiesību praksē. Tā dod iespēju noteikt jurisdikciju par ikvienu noziedzīgu nodarījumu, kura izdarīšana saistīta ar valsti, valsts piederīgo, vai valsts teritorijā atrodošos lietu neatkarīgi no tā, vai daļa noziedzīgā nodarījuma elementu ir konstatējams vienas, bet daļa citas valsts teritorijā.[98]

[94] Krimināllikums. LR likums. Pieejams - http://likumi.lv/doc.php?id=88966 [aplūkots 07.04.2015]
[95] Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g, 62.lpp
[96] Turpat. 63.lpp
[97] Turpat. 84.lpp
[98] Turpat 81.lpp

Šīs doktrīnas aptverošie elementi ir:

1. Noziedzīgs nodarījums ir pabeigts teritorijā, kur iestājas nodarījuma sekas. Saskaņā ar šo doktrīnu neatkarīgi no tā, vai noziedzīga nodarījuma sastāva elements parādās vai iestājās kaitīgās sekas, šī teritorija tiek uzskatīta par nozieguma izdarīšanas vietu.[99]

2. Valsts ir tiesīga piemērot savu krimināljurisdikciju gadījumos, ja kāds no nodarījumu sastāva (corpus delicti) elementiem ir saistīts ar konkrēto teritoriju.[100]

Mūsdienu izpratnē klātbūtnes jurisdikciju piemēro visos gadījumos, kad kāds no noziedzīga nodarījuma elementiem ir saistīts ar konkrēto teritoriju.. Līdz ar to klātbūtnes doktrīna garantē valstij visplašāko iespēju piemērot valsts teritoriālo (subjektīvo, objektīvo) jurisdikciju.[101]

Valstīm, kuru pilsoņi vai pastāvīgie iedzīvotāji ir aizdomās turamās personas, ir tiesības vērst pret tiem savu jurisdikciju par jebkura nodarījuma izdarīšanu. Kā to paredz arī Krimināllikuma 4. panta pirmā daļa. Var piekrist profesores V Liholajas apgalvojumam, ka "teritoriālais jurisdikcijas princips Latvijas krimināltiesību teorijā un praksē piemērojams visos gadījumos, kad noziedzīgais nodarījums tiek faktiski pabeigts vai pārtraukts Latvijas teritorijā, neatkarīgi no tā sastāva un konstrukcijas".[102]

Lai varētu skatīt KL 241.panta noziedzīgo nodarījumu ir jāskatās, tā sastāva klasifikācija, šajā gadījumā, noziedzīgā nodarījuma sastāvs ir pieskaitāms pie materiāliem nozieguma sastāviem, jo ir nepieciešams lai iestātos kaitīgās sekas.[103] No tā arī tiesas var vērtēt par noziedzīgā nodarījuma piekritību. Tātad skatot jurisdikcijās problēmu pēc šīs teorijas, KL 241.panta noziegums, piemēram, persona A. no sava datora, Latvijā, mēģina iekļūt citas valsts pilsoņa datorā, kurš atrodas Nīderlandē, iegūstot datus, kas atrodas uz šī nīderlandieša pilsoņa datora, tad, kā skatīt šo gadījumu, ja noziedzīgs nodarījums ir uzsākts Latvijas teritorijā, bet kaitīgās sekas iestāsies citā valsts teritorijā, Nīderlandē. Tad kā to nosaka KL 4.panta 1.daļas būtu saucami pēc Latvijas regulējuma.

[99] Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g, 81.lpp
[100] Turpat. 82.lpp
[101] Turpat 83.lpp
[102] Turpat, 84.lpp
[103] Turpat. 94.lpp

Kibernoziegumi kļūst aizvien komplicētāki, tāpēc nākotnē to izdarīšanas vietas noteikšanai un līdz ar to jautājums par jurisdikcijas tiesībām būs viens no vislielākajiem izaicinājumiem tiesību aizsardzības speciālistiem un digitālajiem ekspertiem. Tomēr ir svarīgi uzsvērt, ka neatkarīgi no tā, kāda tehnoloģija tiek lietota kiberinfrastruktūras apdraudējumam, vienmēr sākotnējās darbības, tas ir, datu ievade ADAS, būs saistīta ar vienu konkrētu teritoriju, un tās valsts, kuras teritorijā šīs sākumdarbības veiktas, arī gūst tiesības saukt personu pie krimināatbildības, ja vien par šādu darbību izdarīšanu paredzēta krimināatbildība.[104] Skatoties no tiesu prakses un faktiskās situācijas, var secināt ka, ja Latvijā šāds nodarījums tiktu konstatēts, tad tas nebūtu Latvijas tiesai pa spēkam un iespējams kompetencē tādu lietu izskatīt. Jo pārsvarā šīs darbības, kuras veic hakeri ir globālas. Apskatot FIB mājaslapā[105] top meklētākajos ir arī Latvijas pilsonis Aleksejs Belans (Alexsey Belan) un Pēteris Sahurovs, tad kā vajadzētu reaģēt Latvijas tiesai, ja Latvija notver pirmā viņus un vēlas iztiesāt pēc Krimināllikuma pantiem. Kā to pieļauj KL 4.panta 1.daļa, ka Latvijas tiesas var sodīt un saukt pie atbildības Latvijas teritorijā saskaņā ar šo likumu. Tātad Latvijas tiesai būtu visas tiesības šo personu notiesāt pēc Krimināllikuma pantiem.

Bet to visu varētu mainīt 2007.gada 13. jūnijā spēkā stājošais likums "Par Latvijas Republikas valdības un Amerikas Savienotās Valstu valdības līgumu par izdošanu"[106] (turpmāk – izdošanas likums), kur pirmajā pantā jau norādīts, līguma puses vienojas izdot personu viena otrai, kuru viena no lūguma pusēm ir apsūdzējušas, varētu būt tāda situācijas, ka ar pašreizējos politisko situāciju Latvijas valdība izdotu šīs personas ASV valdībai, lai uzturētu draudzīgas attiecības. Tad kā izdošanas likuma 2.pantā norādīts, ka drīkst izdot par noziedzīgu nodarījumu, kas ir sodāma ar abu valstu tiesību aktiem, kas ir ilgāks par vienu gadu, vai smagāku sodu. Tātad abos valstu tiesību aktos, jābūt šim noziedzīga nodarījumam regulētam. Bet kā jau Denisa Čalovska lietā, tad tika izvirzītas bažas, ka viņam tur pienāktos 4 reizes lielāks cietumsods nekā, ja viņu tiesātu Latvijā, tad vai tas nebūtu cilvēktiesību pārkāpums, valsts atbildība aizsargāt savus pilsoņus. Bet tas nav šī darba uzdevums apskatīt šos jautājumus.

---

[104] Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g 97.lpp
[105] Cyber's Most Wanted http://www.fbi.gov/wanted/cyber [aplūkots 16.04.2015]
[106] Par Latvijas Republikas valdības un Amerikas Savienoto Valstu valdības līgumu par izdošanu. Pieejams- http://likumi.lv/doc.php?id=158619 [aplūkots 16.04.2015]

Personālā jurisdikcija

Jau darba autors iepriekš norādīja, ka skatīs tos jurisdikcijas skatīšanas teorijas veidus, kas veiksmīgāk nošķirtu KL 241.panta atbildību, tādējādi no personālās jurisdikcijas aplūkos aktīvo personālo jurisdikciju, jo tā ir regulēta KL 4.panta pirmajā daļā.[107] Aktīvajā personālajā jurisdikcijā svarīgi ir noskaidrot likuma pārkāpēja attiecības pret valsti (pilsonis, pastāvīgais iedzīvotājs, nepilsonis, ārvalstnieks ar pastāvīgāks uzturēšanās atļauju vai bez tās).[108] KL 4.panta pirmajā daļā ir norādīta uz tām personām, uz kurām varētu attiecināt šo jurisdikcijas doktrīnu., tie ir:

1. Latvijas Republikas pilsonis – Latvijas Republikas pilsonību var iegūt trijos veidos. Pirmkārt, naturalizācijas (uzņemšana pilsonībā) kārtībā. Otrkārt, reģistrējot Latvijas pilsoņa statusu. Tāpat arī pilsonību var iegūt par īpašiem nopelniem Latvijas labā. Šādu lēmumu pieņem Saeima.[109] Pilsonības likuma 12.pantā noteikti noteikumi, kā var iegūt pilsonību naturalizācijas ceļā. Pilsoņa reģistrēšana būtu gadījumos, kad piedzimst bērns Latvijas teritorijā, un ja viņa pēcnācēji ir latvieši. Pēdējais gadījums būtu, piemēram, ja kādam zinātniekam vai sportistam, kurš ceļ godā Latvijas vārdu pasaulē, Saeima lemj par šādas pilsonības piešķiršanu šādām personām.
2. Nepilsonis – kārtību kā persona iegūst nepilsoņa statusu nosaka likums "Latvijas nepilsoņa statusa noteikšanas kārtība".
3. Pastāvīgais iedzīvotājs – to regulē "Par Eiropas Savienības pastāvīgā iedzīvotāja statusu Latvijas Republikā" likums, kur 1.pantā noteikta kārtībā, kas ir nepieciešama, lai personu varētu atzīt par ārzemnieku ar pastāvīgo uzturēšanos.
4. Ārvalstnieks – persona, kurai ir citas valsts pilsonība.

Kā norādījis U.Ķinis, tad problemātiskākais būtu noteikt, tās personas, pēc kuras jurisdikcijas, kurām ir pastāvīgās uzturēšanās atļaujas, jo tad vēl jāskata saistību ar valsti. Bet kā to norāda Imigrācijas likuma[110] 24. panta pirmā daļa, norāda uz personām kurām ir tiesības uz pastāvīgās uzturēšanas atļauju Latvijas Republikā, bet panta astotajā daļā noteikts, ka persona, kura bijusi ārpus Latvijas

[107] Krimināllikums. LR likums. Pieejams - http://likumi.lv/doc.php?id=88966 [aplūkots 07.04.2015]
[108] Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g 98-99.lpp
[109] Kā iegūt Latvijas pilsonību un kā no tās atteikties http://www.lvportals.lv/visi/skaidrojumi/236290-ka-iegut-latvijas-pilsonibu-un-ka-no-tas-atteikties/ [aplūkots 16.04.2015]
[110] Imigrācijas likums. LR likums http://likumi.lv/doc.php?id=68522 [aplūkots 16.04.2015]

Republikas teritorijas ne ilgāk par sešiem secīgiem mēnešiem vai kopā nepārsniedz vienu gadu. Ir uzskatāma par nepārtrauktu, līdz ar to tās nodarījumi ir skatāmi pēc Krimināllikuma. Sakarā ar kibernoziegumiem, pārsvarā hakeri ir ļoti mobilas personas, tās neuzturas ilgi vienā vietā, tātad ja ārzemnieks, kurš šeit uzturējies ilgu laiku, ieguvis pastāvīgās uzturēšanās atļauju, bet aizceļo uz pāris mēnešiem uz Eiropas valstīm izdarīt noziedzīgus nodarījums, patvaļīgi piekļūstot citu personu datoros, tad Latvija drīkstētu sodīt šo personu, jo tai ir ciešāka saistība ar Latvijas Republiku.

Seku doktrīna

Šī doktrīna ir paredzēta KL 4.panta trešajā daļā, noteikts " *Ārzemnieki, kuriem nav pastāvīgās uzturēšanās atļaujas Latvijas Republikā un kuri izdarījuši citas valsts teritorijā smagus vai sevišķi smagus noziegumus, kas vērsti pret Latvijas Republikas vai tās iedzīvotāju interesēm, neatkarīgi no tās valsts likumiem, kuras teritorijā izdarīts noziegums, saucami pie krimināLatbildības saskaņā ar šo likumu, ja tie nav saukti pie krimināLatbildības vai nodoti tiesai saskaņā ar nozieguma izdarīšanas vietas valsts likumiem."* [111] Tad pantā dotais regulējums, norāda ka personu var saukt pie atbildības par noziedzīgu nodarījumu, kas ir vērst pret Latvijas Republiku vai tās iedzīvotājiem, tātad šeit jāskatās, kāds kaitīgums ir izdarīts aizsargātajām interesēm.[112] Kā KL 241. panta trešajā daļā noradīto panta dispozīciju norādīts, tad personu drīkst saukt pie atbildības, ja panta pirmajā daļa paredzētas darbības ir izdarījušas smagas sekas. Līdz ar to, ja kāda persona izdara noziegumu patvaļīgi piekļūstot ADAS, kur doktrīnā sekas iedala šādās kategorijās[113]:

1) Fiziskās sekas – datu apstrādes sistēmu darbības fiziska sagraušana vai darbības traucēšana;
2) Mantiskas sekas, kas izpaužas konkrētu mantisku zaudējumu nodarīšanā sistēmas īpašniekam vai tiesiskajam valdītājam, vai arī datu subjekta;
3) Nemantiskas sekas, kur kaitējums saistīts ar likumu aizsargātu interešu aizskārumu sistēmas īpašniekam vai tiesiskajam valdītājam, piemēram, reputācija.

[111] Krimināllikums. LR likums. Pieejams - http://likumi.lv/doc.php?id=88966 [aplūkots 07.04.2015]
[112] Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g 112.lpp
[113] Turpat. 177.lpp

Tad ja, tā persona nav Latvijas pilsonis, tādā gadījumā Latvijas valsts varētu lūgt tai valstij, kur atrodas persona, par tās izdošanu. Būtu vērtīgi aplūkot arī Kibernozieguma konvenciju[114], kuru pieņēma 2001.gada novembrī, Budapeštā. Kur 24.pantā noteikts, ka puses var vienoties par izdošanu, kas saistīti konvencijas 2.-11. pantu nodarījumiem, tie būtu:

- 2.pants – patvaļīga piekļūšana;
- 3.pants – patvaļīga pārtveršana;
- 4.pants – datu traucēšana;
- 5.pants – sistēmas traucēšana;
- 6.pants – ierīces ļaunprātīga izmantošana;
- 7.pants – ar datoru saistītas viltošanas;
- 8.pants – ar datoru saistīta krāpšana;
- 9. pants – ar bērnu pornogrāfiju saistītie noziedzīgie nodarījumi;
- 10. pants – ar autortiesību un blakustiesību pārkāpšanu saistītie noziedzīgie nodarījumi;
- 11.pants – mēģinājums un līdzdalība vai kūdīšana.

Kā Kibernozieguma konvencijas 2. pants noteic,*" Katra Puse pieņem tādus normatīvos aktus un veic citus nepieciešamos pasākumus, lai savos nacionālajos normatīvajos aktos kā noziedzīgu nodarījumu noteiktu ar nodomu izdarītu neatļautu piekļūšanu visai datorsistēmai vai daļai no tās. Puse var pieprasīt atzīt par noziedzīgu nodarījumu arī tādu, kas izdarīts laužot drošības pasākumus ar nodomu iegūt datus vai ar citu negodīgu nodomu vai saistībā ar datorsistēmu, kas ir saistīta ar citu datorsistēmu."* Tātad varētu teikt, ka Latvijas regulējums atbilst konvencijas regulējumam. Kā Kibernozieguma konvencijas 22.pants noteic, ka katrai pusei, jāpieņem tāds regulējums, kas nodibina jurisdikciju par Kibernozieguma konvencijas 2.-11.panta noziedzīgiem nodarījumiem. Un Latvijā tie ir noregulēti KL 241.- 245.pantam. Bet tas, ka valsts ir pieņēmusi šādu konvenciju par saistoši nenozīmē, ka tai ir absolūts pienākums to izpildīt. Piemēram, ja Latvijas pilsonis būtu pārkāpis noziedzīgu nodarījumu, kas Latvijas teritorijā būt kvalificējams, kā KL 241.panta nodarījums. Tad cita valsts, kurai ir

[114] Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. http://likumi.lv/doc.php?id=146481 [aplūkots 16.04.2015]

radīts kaitējums ar šīs personas darbībām, varētu lūgt par tās izdošanu. Bet var gadīties situācijas, kad viena puse to var atteikt, ja tā uzskata to par politisku noziedzīgu nodarījumu vai arī par tādu, kas saistīts ar politisku nodarījumu, vai ja tā uzskata, ka lūguma izpildīšana var kaitēt tās suverenitātei, drošībai, sabiedriskajai kārtībai vai citām būtiskajām interesēm.[115] Kā piemēru var minēt ASV un Krievijas gadījumu, kur ASV tika tiesāts Krievijas pilsonis Aleksejs Ivanovs par to, ka bija patvaļīgi piekļuvis datoriem ASV, un kā FIB aģenti ar viltīgām metodēm pierunāja viņu ierasties uz ASV, kur it kā piedāvājot darbu datoru aizsardzības kompānijā. Tas ļāva FIB aģentiem viņu aizturēt, jo viņš bija ASV jurisdikcijā un bija pietiekoši daudz pierādījumi.[116] Šādā veidā tika apieta Krievijas jurisdikcija, jo nebija pamats viņu tiesāt Krievijā, par ASV izdarītiem noziegumiem.

[115] Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g 283.lpp
[116]United States v. Ivanov http://en.wikipedia.org/wiki/United_States_v._Ivanov [aplūkots 16.04.2015]

4. Krimināllatbildība par patvaļīgu piekļūšanu automatizētai datu apstrādes sistēmai regulējums ārvalstu Krimināllikumos

Vācijas Federatīvajā Republikā

Tāpat kā Latvija, tā arī Vācija ir 2009. gadā ratificējusi Kibernozieguma konvenciju.[117] Sodi par kibernoziegumiem ir iezīmēti Vācijas krimināl kodeksā, bet nav tieši pieminēts vai definēts jēdziens kibernoziegums. Skaidra definīcija kibernoziegumiem ir svarīga Vācijas Kiberaizsardzības Stratēģijā, kur Vācijas valdība atzīst, ka kiberuzbrukumi „var ievērojami negatīvi ietekmēt tehnoloģiju sniegumu, uzņēmējdarbību, administrāciju", un atzīst, ka draudi var nākt ne tikai no ārzemēm, bet arī no iekšzemes, tādējādi ir grūti izsekot kiberuzbrukuma pirmavotu.[118] Vācijas Federatīvas Republikas krimināl kodeksa[119] piecpadsmitās sadaļas, 202.a paragrāfs, ziņu izspiegošana ir noteikts, ka (1) „*Kurš prettiesiski iegūst sev vai citai personai tai neparedzētas ziņas, kuras ir īpaši aizsargātas no nelikumīgas pieejas tām, sodāms ar brīvības atņemšanu uz laiku līdz trim gadiem vai arī naudas sodu*." Uz šo regulējumu var skatīties arī tā, ja to izdara caur datoru, patvaļīgie piekļūstot ziņām, kuras varētu tulkot arī kā informāciju, kura glabājas ADAS. Kā uz to norāda regulējuma paragrāfa 2. daļa, „*1.daļas nozīmē par ziņām atzīstamas tikai tādas, kas tiek vāktas vai nodotas elektroniskā, magnētiskā vai citādā, tieši neuztveramā veidā."*

Krimināl kodekss un Kiberaizsardzības Stratēģija velta īpašu uzmanību izspiegošanai un sabotāžai, kuri ir identificēti kā kiberuzbrukuma veidiem Kiberaizsardzības Stratēģijā. Bet Vācija ir vairāk vērsta uz aizsardzību no kiberuzbrukumiem nekā novēršot tos.[120] Līdz ar to varētu teikt, ka Krimināllikumā ir precīzāk regulēts par patvaļīgu piekļūšanu nekā VFR Krimināl kodekss.

---

[117] Country Report: Germany http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Germany.pdf [aplūkots 17.04.2015]

[118] International Comparison of Cyber Crime http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf_21.lpp [aplūkots 17.04.2015]

[119] Vācijas krimināl kodekss Pieejams - http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html [aplūkots 14.04.2015]

[120] Turpat.

Amerikas Savienotajās Valstīs

ASV 2006.gadā ir ratificējusi Kibernozieguma konvenciju. Dažādos juridiskajos, stratēģiskajos un akadēmiskajos dokumentos ASV terminus, kibernoziegums, kiberuzbrukums, datoruzbrukumi, elektroniskie uzbrukumi, un kiberterorisms ir definējuši.[121] Kiberaizsardzības Stratēģija priekš Drošības dienesta (Homeland Security) ir identificējis divas prioritārās jomas priekš kibertelpas aizsardzības nākotnē. Aizsargājot informāciju kas ir kritiska infrastruktūrai un spēcinātu Kiberekosistēmu. [122] ASV kibernoziegumi ir regulēti Amerikas Savienoto valstu kodeksa 18.Sadaļā[123], kas ir krimināl process un krimināl kodekss ASV. Kas nosaka sodus par tiešsaistes identitātes zādzību, hakeru, ielaušanos datorsistēmās, un bērnu pornogrāfiju. ASV Krimināl kodeksa 1030.paragrāfā ir skaidri un plaši izskaidrots, kā tiek saprasta patvaļīgā ielaušanās datu sistēmās un vēl kāda informācija tiek uzskatīta par neatļautu. No tā var secināt, ka ASV ļoti plaši regulē šos kibernoziegumus un aizsardzība pret tiem ir ievērojami liela, kas varētu būt skaidrojams ar tās plašo ietekmi pasaulē un citu valstu centieniem graut tās sabiedrisko drošību un kārtību ar dažādām pretlikumīgām darbībām. Par augsto aizsardzību var secināt no tā, cik daudzas iestādes ir izveidotas kiberaizsardzībai, piemēram, ASV kiberkomanda (CYBERCOM) un ir pakļautībā ASV stratēģiskajai komandai (USSTRATCOM). Kur vēl ietilpst Armijas spēku kiberkomanda (ARFORCYBER), flotes kiber komanda (FLTCYBERCOM) u.c.[124]

[121] International Comparison of Cyber Crime http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf 18.lpp [aplūkots 17.04.2015]
[122] Turpat. 19.lpp
[123] Amerikas Savienoto Valstu Krimināllikums un Krimināl process Pieejams - https://www.law.cornell.edu/uscode/text/18 [aplūkots 14.04.2015]
[124] International Comparison of Cyber Crime http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf 19.lpp [aplūkots 17.04.2015]

Krievijas Federācijā

Autoritātes, kas ir atbildīgas par kibernoziegumiem Krievijā, ir iestāde „K", kas ir Iekšlietu ministrijas pakļautībā. Krievijas teritorijā diezgan plaši pieaug kibernoziegumi, kas tiek skaidroti ar to, ka, pirmkārt, likumdevēja vara cīņai pret kibernoziegumiem ir neefektīva un sodi par šiem noziedzīgiem nodarījumiem ir maigi, sodi ar datoriem saistītos noziegumos ir ļoti īsi vai atcelti. Otrkārt, dažādas hakeru organizācijas cenšas sadarboties viens ar otru, lai iegūtu lielāku peļņu un atbalstītu savus kriminālos uzņēmumus.[125]

Krievijas iestādes bieži izmanto terminu informatizācija savos stratēģiskajos un politiskajos dokumentos. Krievijā vārds „kiber" ir galvenokārt izmantots vienīgi mēdijos un akadēmiskajās publikācijās. Patvaļīga piekļuve Krievijas krimināLkodeksā[126] ir regulēta 28. sadaļā 272. pantā, kurā noteikts, „*Nelegāla piekļuve likumīgi aizsargātai datora informācijai, tas ir, informācija par nolasāmo informāciju, datoros, datoru sistēmām, un to tīkliem, ja šis nodarījums ir nodarījis bojājumus, bloķējis, pārveidojis, vai pārkopējis informāciju, vai radījis traucējumus datora veiktspējai, datorsistēmai vai tās tīklam."* 2010. gadā jaunajā militārajā doktrīnā, kas bija publicēta, un, kur tika uzsvērta informācijas aizsardzības lielā nozīme. No doktrīnas ir saprotams, tas, ka valsts kiberaizsardzība ir uzticēta armijai. Salīdzinot Krievijas un Latvijas regulējumu, tad Krievijas regulējums ir plašāks nekā KL 241.panta dotais, jo krimināLatbildība iestājas par vairākām darbībām nekā Latvijas regulējumā, un tas ir materiāls sastāvs, jo paredz atbildību arī par datu bojājumiem, pārveidojumiem.

[125] International Comparison of Cyber Crime http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf 30.lpp [aplūkots 17.04.2015]

[126] Krievijas Federācijas krimināLkodekss. Pieejams - http://www.russian-criminal-code.com/ [aplūkots 14.04.2015]

KOPSAVILKUMS

1. Kibernoziegumi, kā jaunās tehnoloģijas ēras attīstības procesā, rada jaunus draudus personu drošībai un privātumam. Attīstoties mūsdienu tehnoloģijām, arī valstu regulējumiem jākļūst efektīvākiem un jāseko līdzi tehnoloģijas tendencēm, bet likumdevējs nespēj panākt to, jo likumdevēju spēja grozīt likumu nav vienāda ar to cik ļoti strauji attīstās tehnoloģijas.
2. Ratificējot Kibernozieguma konvenciju, dalībvalstīm bija jāizveido vienots regulējums, lai harmonizētu dalībvalstu normatīvos aktus attiecībā uz šiem noziedzīgiem nodarījumiem, tika arī grozīts KL 241.pants.
3. Salīdzinot ar iepriekšējo KL 241.panta regulējumu, sarežģījumus sagādāja "datorsistēmas" un "automātiskās datu apstrādes sistēmas" jēdzienu maiņa, jo ADAS plašāk regulēja aizsargājamo objektu, kas ir vērtējami pozitīvi, jo "datorsistēmas" apzīmēja tikai datorus, un plašāk tulkot šo terminu bija sarežģīti, bet ieliekot ADAS terminu jaunajā regulējumā, tiek plašāk regulēts objektu loks, kas ieskaita ne tikai datorus, bet jebkuru apstrādes sistēmu, telefonus, planšetes u.c.
4. Vērtējot KL 241.panta objektīvo pusi, tiesību zinātnieki norāda, ka noziedzīgā nodarījuma darbības ir jāizdara attālināti, fiziski neaizskarot datu sistēmu, bet autors to neuzskata par absolūtu risinājumu, jo ir arī datu sistēmas, kuras ir pieslēgtas iekšējam tīklam, tādēļ jāvērtē personas darbība, mēģinot piekļūt tādiem sistēmas datiem, tāpēc būtu jāvērtē arī "attālināti" izpratni regulējamajā pantā.
5. Nošķirt KL 241.p no citiem līdzīgiem noziedzīgiem nodarījumiem, nesagādā problēmas, jo katrā no KL 243.-245.p nodarījumiem ir atšķirīgas objektīvās puses pazīmes, tādējādi ir saprotams, kuru Krimināllikuma pantu piemērot.
6. KL 241.panta nošķiršana no KL 177.[1] panta ir iespējama analizējot objektīvo pusi un kopīgi skatīt terminu "automatizēta datu apstrādes sistēma", tāpēc, ka KL 177.[1] panta nodarījums arī vērsts pret ADAS, tāpēc ir jāskatās šaurāk šī noziedzīgā nodarījuma priekšmets, nekā KL 241.panta dotais priekšmets, KL 177.[1] panta aizsargātais priekšmets būtu tikai spēļu automāti.
7. Gandrīz katru dienu notiek vairāki kiberuzbrukumi datu sistēmām, un tie notiek ne tikai iekšzemē, bet arī nāk no ārvalstīm, tādējādi rodas problemātika pēc

kuras valsts regulējuma saukt pie atbildības vainīgās personas, Latvijas tiesām ir dotas vairākas izvēles iespējas, kā saukt personu pie krimināatbildības, kura ir izdarījusi šos noziedzīgo nodarījumu, ņemot vērā Krimināllikuma 4.pantu.

8. Jāņem vērā arī valstu valdības noslēgtie starptautiskie līgumi, kā viens no tiem varētu būt starp ASV un Latviju, "Par Latvijas Republikas valdības un Amerikas Savienoto Valstu valdības līgumu par izdošanu", kur citā noziedzīgā nodarījumā, bet attiecībā uz to pašu noziegumu grupu, kibernoziegumi, ir Denisa Čalovska gadījums.
9. Vērtējot katras valsts regulējumus attiecībā uz kibernoziegumiem, ir vēl jāskatās pastarpināti politiskā attieksme un valsts rīcība pret šiem noziedzīgiem nodarījumiem pārsvarā visā Eiropas Savienībā un atsevišķās valstīs ir ratificēta Kibernozieguma Konvencija, kur dalībvalstīm jau ir nostiprinātas vadlīnijas, kādai jābūt minimālai aizsardzībai pret šiem nodarījumiem, kuras ir dotas tās pašas konvencijas tekstā.
10. Salīdzinot Vācijas Krimināl kodeksu un Krimināllikuma regulējumus par patvaļīgu piekļūšanu automatizētām datu apstrādes sistēmām, var saskatīt līdzību pantu sastāvos, tikai ir atšķirība terminos, Krimināllikumā ir dots jēdziens "pārvarot sistēmas aizsardzības līdzekļus", bet Vācijas Krimināl kodeksā dots jēdziens " iegūstot informāciju, kura ir īpaši aizsargāta", tādējādi jāvērtē, kā izpaužas šī aizsardzība Vācijas Krimināl kodeksā, autors uzskata, ka Krimināllikumā ir dots plašāks jēdziens, saistībā uz aizsardzību, jo ir saprotami, kas ir šie aizsardzības līdzekļi.
11. ASV Krimināl kodeksa regulējums par patvaļīgu piekļūšanu datu sistēmām ir plašāk regulēts nekā Krimināllikuma 241.pants, kurā ir uzskaitītas darbības, kuras ir uzskatāmas par pretlikumīgām. Lai spētu kontrolēt šīs darbības, ir iesaistīta armijas palīdzība, tās apakšvienības, kuras specializējas, lai apturētu kiberuzbrukumus.
12. Krievijas Krimināl kodeksā ir dots plašāks regulējums nekā Krimināllikumā, tādā ziņā, ka atbildība iestājas arī par datu bojājumiem un pārveidojumiem, tad šajā ziņā, ir jāvērtē vai Krievijas regulējums nav haotisks, jo Krimināllikumā par bojājumiem un pārveidojumiem ir paredzēti atsevišķi panti, līdz ar to, Latvijas regulējuma uzbūve, būtu veiksmīgāka, jo atļauj nošķirt no līdzīgiem nodarījumiem pret datu sistēmām.

LITERATŪRAS SARAKSTS

Literatūra

1. Krastiņš U., V. Liholaja, A, Niedre. Krimināllikuma zinātniski praktiskais komentārs, sevišķā daļa 3, Rīga, 2007.g.
2. Krastiņš U., V. Liholaja, A. Niedre, Krimināltiesībās. Sevišķā daļa, Rīga: Tiesu namu aģentūra, 2009.g.
3. Ķinis U. Kibernoziegumi, Rīga, 2007.g.
4. Ķinis U., Kibernoziegums un jurisdikcija, Jumava, 2013.g
5. Birks M. "Neo lieta" – noziedzīgs nodarījums vai "ziņotāja" apklusināšana, Jurista Vārds 19.06.2012. Nr. 25 (724) Pieejams - http://www.juristavards.lv/doc/249232-bneo-lietab-noziedzigs-nodarijums-vai-zinotaja-apklusinasana/ [aplūkots 17.03.2015]
6. Ķinis U Nodarījumi pret informācijas sistēmu drošību Jurista Vārds 27.09.2011. Nr. 39 (686) Pieejams - https://defense.lv/wp-content/uploads/2011/09/uldis_kinis_kriminallikuma_piemerosanas_problemas.pdf [aplūkots 10.04.2015]
7. Ķinis U. Nodarījumi pret informācijas sistēmu drošību, Jurista Vārds, 27.09.2011. Nr. 39 (686) Pieejams - http://www.juristavards.lv/doc/236587-bnodarijumi-pret-informacijas-sistemu-drosibub/ [aplūkots 20.03.2015]
8. Latvijas Universitātes raksti. Juridiskā zinātne. Nr. 667. U. Ķinis."Patvaļīga piekļūšana datorsistēmai"(KL241.pants) priekšmeta kvalifikācijas problēmas
9. Liholaja V Hamkova D. Būtisks kaitējums izpratne: likums, teorija, prakse. Jurista Vārds, 10.01.2012., Nr. 2. (701). Pieejams - http://www.juristavards.lv/doc/242455-butiska-kaitejuma-izpratne-likums-teorija-prakse/ [aplūkots 08.05.2015]
10. Aiz Neo vārda, iespējams, slēpies LU pētnieks Ilmārs Poikāns Pieejams - http://www.delfi.lv/news/national/criminal/aiz-neo-varda-iespejams-slepies-lu-petnieks-ilmars-poikans-1744.d?id=31832311 [aplūkots 11.04.2015]
11. Cloud Storage: 4 Legal Issues You Need to Know Pieejams - http://www.inc.com/samuel-wagreich/the-4-things-you-must-have-in-your-contract-with-your-cloud-provider.html [aplūkots 09.04.2015]

12. Country Report: Germany. Pieejams - http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Germany.pdf [aplūkots 17.04.2015]
13. Cyber's Most Wanted. Pieejams - http://www.fbi.gov/wanted/cyber [aplūkots 16.04.2015]
14. Cyberspace definition. Pieejams - http://www.thefreedictionary.com/cyberspace [aplūkots 09.04.2015]
15. DATU VALSTS INSPEKCIJA. Rekomendācija «Personas datu apstrādes drošība» Pieejams - http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Rekomendacija_PDA_drosiba_2014.pdf [aplūkots 09.04.2015]
16. International Comparison of Cyber Crime. Pieejams - http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf_21.lpp [aplūkots 17.04.2015]
17. Kā iegūt Latvijas pilsonību un kā no tās atteikties. Pieejams - http://www.lvportals.lv/visi/skaidrojumi/236290-ka-iegut-latvijas-pilsonibu-un-ka-no-tas-atteikties/ [aplūkots 16.04.2015]
18. Militāro mācību "Steadfast Jazz 2013" laikā notikušie kiberuzbrukumi bijuši "ārējas izcelsmes" Pieejams - http://www.focus.lv/latvija/viedokli/militaro-macibu-steadfast-jazz-2013-laika-notikusie-kiberuzbrukumi-bijusi-arejas-izcelsmes [aplūkots 10.04.2015]
19. Pērn Latvijā reģistrēti aptuveni 400 kibernoziegumi Pieejams - http://www.tvnet.lv/tehnologijas/internets/553247-pern_latvija_registreti_aptuveni_400_kibernoziegumi [aplūkots 18.04.2015.]
20. Pretvīrusu programmatūra. Pieejams - http://drossinternets.lv/page/64 [aplūkots 21.03.2015]
21. Stāsts par Imantas hakeri. Pieejams - http://www.rigaslaiks.lv/Raksts.aspx?year=2013&month=3&article=4 [aplūkots 14.04.2015]
22. Terminu un svešvārdu skaidrojošā vārdnīca, vārds – automātisks. Pieejams - http://www.letonika.lv/groups/default.aspx?r=1107&q=autom%C4%81tisks&id=993817&g=1 [aplūkots 17.03.2015]

23. Terminu un svešvārdu skaidrojošā vārdnīca, vārds- datu apstrāde. Pieejams - http://www.letonika.lv/groups/default.aspx?r=1107&q=datu%20apstr%C4%81de&id=2635837&g=1 [aplūkots 17.03.2015]
24. Terminu un svešvārdu skaidrojošā vārdnīca, vārds-datu apstrādes sistēma. Pieejams - http://www.letonika.lv/groups/default.aspx?cid=967984&r=1107&lid=967984&g=1&q=datu%20apstr%C4%81de&h=6145 [aplūkots 17.03.2015]
25. Ugunsmūris. Pieejams - http://drossinternets.lv/page/72 [aplūkots 21.03.2015]
26. United States v. Ivanov. Pieejams - http://en.wikipedia.org/wiki/United_States_v._Ivanov [aplūkots 16.04.2015]
27. Valdība nolemj izdot Denisu Čalovski ASV; ECT aptur izdošanu Pieejams - https://defense.lv/2013/08/11/valdiba-nolemj-izdot-denisu-calovski-asv-ect-aptur-izdosanu/ [aplūkots 11.04. 2015]

Normatīvie akti

28. Par Latvijas Republikas valdības un Amerikas Savienoto Valstu valdības līgumu par izdošanu. Pieejams- http://likumi.lv/doc.php?id=158619 [aplūkots 16.04.2015]
29. Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. Pieejams - http://likumi.lv/doc.php?id=146481 [aplūkots 16.04.2015]
30. Eiropas parlamenta un padomes Direktīva 2013/04/ES, par uzbrukumiem informācijas sistēmām, un kuru aizstāj Padomes pamatlēmumu 2005/222/TI. Pieejams - http://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32013L0040&qid=1431336947563&from=LV [aplūkots 11.05.2015]
31. Krimināllikums. LR likums. Pieejams - http://likumi.lv/doc.php?id=88966 [aplūkots 07.04.2015]
32. Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību. Pieejams - http://likumi.lv/doc.php?id=50539 [aplūkots16.04.2015]

33. Imigrācijas likums. LR likums. Pieejams - http://likumi.lv/doc.php?id=68522 [aplūkots 16.04.2015]
34. Pilsonības likums. LR likums Pieejams- http://likumi.lv/doc.php?id=57512 [aplūkots 11.04.2015]
35. Valsts informācijas sistēmu likums. LR likums. Pieejams - http://likumi.lv/doc.php?id=62324 [aplūkots 12.04.2015]
36. Amerikas Savienoto Valstu Krimināllikums un Kriminālprocess Pieejams - https://www.law.cornell.edu/uscode/text/18 [aplūkots 14.04.2015]
37. Krievijas Federācijas kriminālkodekss. Pieejams - http://www.russian-criminal-code.com/ [aplūkots 14.04.2015]
38. Vācijas kriminālkodekss Pieejams - http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html [aplūkots 14.04.2015]

Tiesu prakse

39. Latvijas Republikas Augstākās tiesas Krimināllietu departamenta 2009.gada 20.janvāra, lieta Nr. SKK-030/2009 [aplūkots 16.04.2015]
40. Latvijas Republikas Augstākā tiesa Krimināllietu departaments 2014. gada 27.augusta lēmums Lietā Nr. SKK- 349/2014 [aplūkots 16.04.2015]

Dokumentārā lapa

Bakalaura darbs "Kriminālatbildība par patvaļīgu piekļūšanu automatizētai datu apstrādes sistēmai (Krimināllikuma 241.pants)" izstrādāts LU Juridiskajā fakultātē.

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

Autors: Einārs Janukovičs _____ 18.05.2015

Rekomendēju/nerekomendēju darbu aizstāvēšanai
Vadītāja: Doc,. Dr.iur. Diāna Hamkova _____18.05.2015

Recenzents: _____

Darbs iesniegts Krimināltiesisko zinātņu katedrā 18.05.2015

Dekāna pilnvarotā persona: _____

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē
2015.g. ____._____un novērtēts ar atzīmi - _____

Komisijas sekretāre: _____