https://doi.org/10.25143/socr.19.2020.1.090-109

Automatizētās datu apstrādes sistēmā esošo datu kontrole (Kriminālprocesa likuma 219. pants): nacionālie un starptautiskie piemērošanas aspekti

Dr. iur. ***Uldis Ķinis***
ORCID: 0000-0002-5573-9887
Rīgas Stradiņa universitāte, Latvija
uldis.kinis@rsu.lv

Mg. iur. ***Ņikita Sinkevičs***
ORCID: 0000-0001-5997-1379
Rīgas Stradiņa universitāte, Latvija
nikita.sinkevics@gmail.com

Kopsavilkums

Raksta tapšanas ideja ir saistīta ar Valsts policijas iesniegto priekšlikumu Tieslietu ministrijas Kriminālprocesa ekspertu pastāvīgajai darba grupai par grozījumiem Kriminālprocesa likuma 219. panta otrajā daļā. Kriminālprocesa likuma 219. pants "Automatizētās datu apstrādes sistēmā esošo datu kontrole" būtībā ir analogs Kibernoziegumu konvencijas 19. pantam, kas uzliek dalībvalstīm pienākumu pieņemt tādus tiesību aktus, kas atvieglotu to teritorijā esošo sistēmu pārmeklēšanu. Priekšlikuma būtība: atteikties pantā no nacionālās teritoriālās piemērošanas klauzulas, jo tā ierobežojot policijas iespējas iegūt pierādījumus, ja no pārmeklējamās sistēmas ir iespējams likumīgi piekļūt datiem, kas glabājas sistēmās, kas atrodas ārpus Latvijas Republikas teritorijas. Citiem vārdiem sakot, idejas būtība ir mainīt panta piemērošanas jurisdikciju no nacionāli teritoriālās uz pārrobežu.

Diskusija par to, vai vienai dalībvalstij ir tiesības veikt datu sistēmu pārmeklēšanu citā dalībvalstī, notiek jau kopš Kibernoziegumu konvencijas pieņemšanas. Turklāt tā turpināsies vismaz līdz Konvencijas otrā Papildprotokola pieņemšanai, kur būtu jāatrisina jautājumi ar pārrobežu sistēmu pārmeklēšanu un datu izņemšanu. Rakstā tiks analizēts, vai un kā situācija, īpaši saistībā ar jurisdikciju kriminālprocesā, pēc Kibernoziegumu konvencijas un Kriminālprocesa likuma pieņemšanas ir mainījusies, un tiks sniegti priekšlikumi, kā efektīvāk būtu risināma problēma, kuru aktualizējusi Valsts policija.

Atslēgvārdi: datu kontrole, automatizētā datu apstrādes sistēma, Kibernoziegumu konvencija, pierādījumi kriminālprocesā, suverenitāte, krimināljurisdikcija, datu pārmeklēšana un izņemšana.

Ievads

Kriminālprocesa likuma (turpmāk – KPL) 219. pants "Automatizētās datu apstrādes sistēmā esošo datu kontrole" sastāv no četrām daļām (Kriminālprocesa likums, 2005). Pirmajā daļā sniegta automatizētās datu apstrādes sistēmā (turpmāk – ADAS) esošo datu kontroles legāldefinīcija, otrajā daļā reglamentēta subjektīvās jurisdikcijas teritoriālās piemērošanas klauzula, trešajā daļā paredzētas procesa virzītāja tiesības pieprasīt nodrošināt pārmeklējamo datu veselumu un nepieejamību citām personām. Savukārt ceturtajā daļā ir noteikta izņemto datu juridiskā kontrole un kārtība.

2020. gadā Valsts policija (turpmāk – VP) vērsās ar priekšlikumu veikt grozījumus Kriminālprocesa likuma 219. panta "Automatizētās datu apstrādes sistēmā esošu datu kontrole" otrajā daļā: "Ja ir pamats uzskatīt, ka meklētie dati (informācija) tiek uzglabāti citā Latvijas teritorijā esošā sistēmā, kurai var piekļūt autorizēti, izmantojot izmeklēšanas tiesneša lēmumā minēto sistēmu, jauns lēmums nav nepieciešams." VP lūdz izslēgt no panta daļas vārdus "Latvijas teritorijā esošā". Priekšlikuma iesniedzēji pēc būtības lūdz izslēgt no normas subjektīvās teritoriālās jurisdikcijas piemērošanas klauzulu. Pēc priekšlikuma autoru viedokļa, tieši šī teritoriālās jurisdikcijas piemērošanas klauzula liedzot policijai veikt pienācīgas kvalitātes procesuālās darbības elektronisko pierādījumu iegūšanā no kratīšanai pakļautajām ierīcēm, ja piekļuve attālinātiem datiem neatkarīgi no to ģeogrāfiskās atrašanās vietas būtu iespējama bez speciālu drošības līdzekļu izmantošanas.

Krimināltiesību pētnieku vidū diskusija par šo jautājumu jau norit, kopš internets, uzsākot pasaulē savu uzvaras gājienu, radīja globālo informācijas telpu, kas tiek aktīvi izmantota arī dažādu nelikumīgu darbību veikšanai. 1989. gadā tika pieņemta Eiropas Padomes Rekomendācija Nr. 89(9) par datorsaistītiem noziegumiem (*Council of Europe*, 1990) un 1995. gada Rekomendācija R(95)13 par kriminālprocesuālo likumu piemērošanas problemātiku saistībā ar informācijas tehnoloģijām (*Council of Europe*, 1995). Turpinot šo darbu, 1997. gadā Eiropas Padome uzsāka darbu pie Kibernoziegumu konvencijas, kas noslēdzās ar 2001. gada 23. novembrī Budapeštā parakstīto Kibernoziegumu konvenciju (turpmāk – KNK) (*Council of Europe*, 2001), kurai Latvija pievienojās 2007. gadā. KNK līdz šim ir vienīgais starptautiskais līgums, kurš reglamentē kibernoziegumu apkarošanas materiālos, procesuālos, nacionālos un starptautiskās sadarbības aspektus krimināllietās. KNK 19. pants "Uzglabāto datu pārmeklēšana un pārņemšana" ir tiešs priekštecis Kriminālprocesa likuma 219. pantam. Tāpēc tas tika izstrādāts, lai atbilstu KNK 19. pantā izvirzītajām prasībām.

Kopš KNK pieņemšanas ir pagājuši vairāk nekā 19 gadi, tāpēc raksta mērķis ir izpētīt, vai straujā informācijas tehnoloģiju attīstība ir mainījusi to KNK normu, kas saistīta ar elektroniskās vides pārmeklēšanu un tās piemērošanas jurisdikciju. Vai pasaulē

mainījusies izpratne par jurisdikcijas pamatiem? Kā KNK dalībvalstis gan Austrumos, gan arī Rietumos regulē šo procesuālo instrumentu, un kādas ir šī instrumenta piemērošanas robežas? Vai, ieviešot šo priekšlikumu, tiktu sasniegts tā mērķis: veikt no kratīšanai pakļautās sistēmas ar sistēmā pieejamiem identifikatoriem piekļuvi attālinātiem datiem neatkarīgi no to fiziskās vai virtuālās atrašanās vietas?

Lai izvērtētu šī priekšlikuma būtību, rakstā tiek analizēta tikai Kriminālprocesa likuma 219. panta pirmā daļa – ADAS pārmeklēšanas legāldefinīcija – un šī panta otrā daļa, kas satur tās piemērošanas teritoriālo klauzulu, jo tieši minētās normas ir svarīgas, lai izvērtētu ar VP priekšlikumu saistīto problemātiku un iespējamās sekas. Raksta sagatavošanā analizēti arī citi KNK dalībvalstu kriminālprocesa likumi par ADAS pārmeklēšanu un tās piemērošanas robežām. Tāpat pētījuma sagatavošanā izmantoti citi juridiskās literatūras avoti un ES normatīvie akti. Raksta nobeigumā izvirzīti priekšlikumi šī procesuālā instrumenta efektīvākai piemērošanai.

Raksta sagatavošanā izmantota salīdzinošā tiesību metode un tiesību normu interpretācijas metodes: vēsturiskā, gramatiskā, sistēmiskā un teleoloģiskā metode.

KPL 219. panta vēsturiskā attīstība

> "(1) Automatizētās datu apstrādes sistēmas (tās daļas), tajā uzkrāto datu, datu vides pārmeklēšanu un piekļuvi tai, kā arī izņemšanu bez šīs sistēmas vai datu īpašnieka, valdītāja vai turētāja ziņas kriminālprocesā veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka konkrētajā sistēmā esošā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem.
> (2) Ja ir pamats uzskatīt, ka meklētie dati (informācija) tiek uzglabāti citā Latvijas teritorijā esošā sistēmā, kurai var piekļūt autorizēti, izmantojot izmeklēšanas tiesneša lēmumā minēto sistēmu, jauns lēmums nav nepieciešams."

KPL tika pieņemts 2005. gada 21. aprīlī un stājās spēkā 2005. gada 1. oktobrī, un tajā bija iekļauts 219. pants "Elektroniskajā informācijas sistēmā esošo datu kontrole" . Savukārt ar 2009. gada 12. marta likumu par Grozījumiem Kriminālprocesa likumā minētais pants tika definēts kā "Automatizētās datu apstrādes sistēmā esošo datu kontrole" (Kriminālprocesa likums, 2005). Tomēr, izņemot elektroniskas informācijas sistēmas aizstāšanu ar automatizētu datu apstrādes sistēmu, citi grozījumi panta pirmajā un otrajā daļā netika veikti.

Nepieciešamību ietvert Kriminālprocesa likumā šādu normu noteica gan nacionālā procesuālā nepieciešamība, gan arī Eiropas Padomes Rekomendācijas, kā arī 2001. gadā pieņemtā Kibernoziegumu konvencija un tās protokols. Minētie dokumenti rekomendēja dalībvalstīm Kriminālprocesa likumā ieviest instrumentus, kas efektivizētu valstu cīņu pret kibernoziegumiem un tai pašā laikā garantētu aizsardzību pret personu pamattiesību nepamatotu ierobežošanu. Par pirmo starptautisko avotu saistībā ar elektroniskās vides pārmeklēšanu uzskatāma jau minētā Eiropas Padomes Rekomendācija R(95)13 (*Council of Europe*, 1995), kur pirmo reizi starptautiskas vadlīnijas formā tika definēts jauns kriminālprocesuālais instruments – sistēmā uzglabāto datu meklēšana un pārņemšana

(angļu val. *search and seizure*). Tās saturs definēts Rekomendācijas Pielikuma 1. punkta 2. apakšpunktā, kur norādīts, ka kriminālprocesa likumiem ir jāatļauj izmeklēšanas iestādēm veikt datorsistēmu pārmeklēšanu un datu izņemšanu līdzvērtīgi tradicionālajai. Turklāt 1.3. punktā uzsvērts, ka "izmeklēšanas iestādēm ir tiesības paplašināt pārmeklēšanas objektus un pakļaut tai arī citas savstarpēji tīklā savienotas to jurisdikcijā esošas datorsistēmas". Tomēr Eiropas Padome secināja, ka dalībvalstis nav visai aktīvas šo rekomendāciju ieviešanā, tāpēc tika nolemts uzsākt darbu pie Kibernoziegumu konvencijas. 1996. gadā tika izveidota Eiropas Padomes Kibernoziegumu ekspertu komiteja. Tās uzdevums bija izstrādāt KNK, kas tika parakstīta 2001. gada 23. novembrī Budapeštā (*Council of Europe*, 2001). Vienlaikus ar KNK tika pieņemts Kibernoziegumu konvencijas Paskaidrojošais ziņojums (turpmāk – KNK PZ) (*Council of Europe*, 2001). Līdz šim brīdim tas ir arī vienīgais saistošais starptautiskais līgums kibernoziegumu apkarošanai, un Latvija tam pievienojās 2007. gadā. Jānorāda, ka arī Eiropas Savienībā Konvencijas pieņemšanas brīdī, izņemot Komisijas politikas dokumentu (*European Commission*, 1996), šajā jomā nebija speciāla regulējuma. Tāpēc KNK PZ 8. punktā ir uzsvērts, ka informācijas tehnoloģiju un sakaru pakalpojumu savienojums radījis jaunu kopīgu telpu, kuru sauc par kibertelpu. Tā rada iespēju veikt pārrobežu rakstura nodarījumus, kas nereti nepakļaujas nacionālo tiesību jurisdikcijai. Tādēļ ir nepieciešami starptautiski centieni, lai nostiprinātu Eiropas Padomes Rekomendācijā (89)9 minēto, ka datorsaistītiem noziegumiem ir pārnacionāls raksturs, ka cīņai pret šiem nodarījumiem nepieciešams uzlabot starptautisko tiesisko sadarbību.

Panta pamatā ir vispāratzītā un plaši izmantotā kriminālprocesuālā darbība kratīšana (KPL 179. pants). Tās mērķis ir iegūt materiālus (taustāmus) pierādījumus kriminālprocesā (sk. KNK PZ 186. punktu). Kratīšana ir patstāvīga izmeklēšanas darbība, kurai raksturīga augsta iejaušanās pakāpe personas dzīvē (Meikališa, 2019). Šī iejaukšanās pamattiesību kontekstā saistāma ar personas tiesībām uz privātumu. KNK izstrādātā panta mērķis ir panākt elektroniskās vides pārmeklēšanai tādu pašu efektivitāti, kā to var sasniegt, pārmeklējot mājokļus un izņemot taustāmus pierādījumus savā nacionālās valsts teritorijā situācijās, kad iesaistīti vietējie sakaru pakalpojumu sniedzēji (sk. KNK PZ 188. punktu). Kāpēc bija jāveido jauns regulējums?

Galvenais iemesls ir tas, ka pastāv divu veidu dati: 1) dati, kas ir saglabāti ADAS un atrodas pārmeklējamā ierīcē, un 2) attālināti pieejamie dati, kuri ir savienoti ar sistēmu, bet atrodas citā ģeogrāfiskajā vietā esošā ADAS. ADAS saglabātos datus var iegūt kratīšanas procesā, izņemot dažādus datu nesējus, taču nevar attālināti iegūt datus no sistēmām, kas atrodas ārpus valsts jurisdikcijas, jo procesa virzītājs ir tiesīgs rīkoties tikai nacionālās valsts teritorijā. Kaut arī kratīšana un darbības pēc juridiskās kontroles līmeņa un piemērošanas principiem ir līdzīgas, tomēr elektroniskās vides pārmeklēšana ir daudz sarežģītāka darbība, jo galvenais šīs aktivitātes uzdevums ir iegūt lietā nepieciešamos elektroniskos pierādījumus, kas var atrasties dažādos datu nesējos. Tradicionālajā kratīšanā tiek pārmeklēta fiziska telpa, objekti, savukārt elektroniskās vides pārmeklēšana nav saistīta tikai ar dažādu datu nesēju pārmeklēšanu un izņemšanu, bet arī ar

attālināti pieejamo datu iegūšanu no pārmeklējamās datorsistēmas. Turklāt elektroniskie pierādījumi ir viegli gaistoši, tādēļ to iegūšana un saglabāšana procesa virzītājiem nereti ir ļoti darbietilpīgs un tehniski sarežģīts process. Eiropas Padomes dalībvalstis pārstāv dažādas tiesību sistēmas, līdz ar to arī krimināprocesuālais regulējums ir atšķirīgs. Tāpēc KNK 19. panta mērķis bija panākt, lai dalībvalstis, izmeklējot kibernoziegumus, padarītu šī procesuālā līdzekļa piemērošanu efektīvu nacionālās valsts teritorijā, proti, ar vienu kompetentas amatpersonas lēmumu par ADAS pārmeklēšanu un datu izņemšanu to attiecinātu uz jebkuru valsts teritorijā esošu ADAS, ja šādiem datiem var likumīgi piekļūt no pārmeklējamās ADAS. Jābūt iespējai nekavējoties paplašināt meklēšanu vai līdzīgi piekļūt otrai sistēmai un iegūt tajā glabātus datus. Tāpēc KPL 219. panta mērķis ir tieši un nesaraujami saistīts ar KNK 19. pantā sniegto definīciju, jo šī norma KPL esošajā redakcijā tika iekļauta ar mērķi, lai Latvija varētu pievienoties KNK, jo tikai pēc normatīvā regulējuma attiecīgo grozījumu Krimināllikumā un KPL pieņemšanas Latvija 2007. gada 14. aprīlī pievienojās KNK. Tāpēc, lai noskaidrotu šajā pantā reglamentēto darbību mērķi un piemērošanas robežas, ir nepieciešams to analizēt kopsakarā ar KNK 19. pantu "Uzglabāto datu meklēšana un pārņemšana".

Tā kā pantam ir četras daļas, tiks atzīmētas galvenās panta juridiskā kodola sastāvdaļas:

1) normatīvie akti, kas pilnvaro tās kompetentās institūcijas pārmeklēt vai līdzīgi piekļūt ADAS vai tās daļai, kas atrodas tās teritorijā;
2) piekļuve citas puses teritorijā esošai ADAS vai tās daļai, ja no pārmeklējamās ADAS ir iespējams meklētajiem datiem likumīgi piekļūt vai arī tie jau ir pieejami (respektīvi, ar vienu tiesas lēmumu var paplašināt meklēšanu uz jebkuru valsts teritorijā esošu ADAS);
3) jāuzliek par pienākumu atbildīgajām personām nodrošināt šo datu aizsardzību;
4) juridiskā kontrole – lēmumu var pieņemt tikai tiesnesis.

KNK 1. pants datus iedala trijos juridiskajos līmeņos: ir plūsmas dati (angļu val. *traffic data*); ar abonentu saistītie dati (angļu val. *subscriber data*) un satura dati (angļu val. *content data*). Katram no šo datu veidiem ir savs juridiskais kontroles līmenis. Uzkrāto datu saglabāšanu reglamentē KNK 16.–17. pants. Savukārt satura datu kontroli – uzglabāto datu meklēšanu un pārņemšanu – reglamentē KNK 19. pants. Latvijas tiesību sistēmā Elektronisko sakaru likuma 1. panta 44^2. punktā tiek izdalīti "noslodzes dati, atrašanās vietas dati un ar tiem saistīti dati, kas nepieciešami, lai identificētu abonentu vai lietotāju" (Elektronisko sakaru likums, 2004), kas atbilst KNK pirmajai un otrajai datu grupai. Šo datu ieguvi reglamentē KPL 191. pants, kur pieprasījumu par datu iesaldēšanu, kas atrodas pie pakalpojumu sniedzēja, veic procesa virzītājs. Savukārt datu izsniegšanai ir nepieciešama juridiska kontrole. Tādējādi KNK izstrādātāji un arī Latvijas likumdevējs ir nošķīris šo divu pirmo datu grupu iegūšanas juridiskās prasības no sistēmā saglabātu datu, kas pēc būtības ir satura dati, kontroles un izņemšanas. Protams, abos gadījumos tiek veikta personu datu apstrāde un ierobežots privātums, taču, piemērojot KPL 219. pantu, šī iejaukšanās privātumā ir daudz būtiskāka, tāpēc lielākajā daļā pasaules valstu lēmumu par datu

kontroli pieņem tiesas amatpersona (Latvijā tas ir izmeklēšanas tiesnesis). A. Lieljuksis norāda, ka ADAS esošo datu kontrole ir speciālā izmeklēšanas darbība, kuras mērķis ir bez īpašnieku, valdītāju vai turētāju ziņas, bet ar izmeklēšanas tiesneša atļauju iegūt ziņas par pierādāmos apstākļos ietilpstošiem faktiem, to izņemšanu un tiesības pieprasīt citiem lietotājiem saglabāt uzkrāto datu veselumu un nodrošināt to nepieejamību (Lieljuksis, 2019). Tādējādi satura datu iegūšana kriminālprocesā tiek īpaši aizsargāta.

KNK PZ 195. punktā ir skaidri definēta normas piemērošanas teritoriālā klauzula, proti, ka šo normu "nevar izmantot, lai veiktu pārrobežu pārmeklēšanu, iegūstot elektroniskos pierādījumus no sistēmām, kas atrodas citu valstu teritorijās". Tomēr kopš KNK pieņemšanas ir pagājuši vairāk nekā 19 gadi, līdz ar to ir svarīgi noskaidrot, kā tiek iedzīvināta KNK un vai ir mainījusies šī panta teritoriālās jurisdikcijas piemērošanas klauzula. Tādēļ ir svarīgi saprast, kāpēc Eiropas Padomes Kibernoziegumu komitejas eksperti vienojās un dalībvalstis atbalstīja tieši šādu KNK 19. panta tekstu. Tāpēc ir jāapskata KNK definētā jurisdikcija un tās piemērošanas interpretācija.

Jurisdikcija un diskusijas par tās piemērošanas robežām

Termins "jurisdikcija" ir cēlies no latīņu vārda "jurisdictio". Romiešu tiesībās ar to apzīmēja juridisku varu – tiesību noteikt, regulēt un piemērot likumus savas valsts teritorijā (Ķinis, 2015). Attīstoties krimināltiesību zinātnei, Hārvarda Universitātē 1935. gadā tika izstrādāta paplašinātā teritoriālā krimināljurisdikcijas doktrīna, kas balstīta uz pieciem kritērijiem: 1) teritoriālo jurisdikciju (objektīvo, subjektīvo); 2) objektīvo personālo jurisdikciju; 3) aizsardzības principu; 4) seku jurisdikciju (pasīvo personālo jurisdikciju) un 5) universālo jurisdikciju. Kaut arī šīs doktrīnas sagatavošana palika tikai projekta līmenī, tomēr tā ir atstājusi milzīgu iespaidu uz krimināljurisdikcijas attīstību visā pasaulē (*Svantesson*, 2015).

Jau KNK ekspertu grupā par jurisdikcijas pamatiem, principiem un robežām notika ļoti sarežģītas diskusijas, kuru rezultātā eksperti vienojās, ka kibernoziegumu jurisdikcijas regulējumā ir ietverami visi iepriekšminētie Hārvarda Universitātes projekta jurisdikcijas principi. Jāuzsver, ka arī 2000. gadā bija internets un globālie informācijas pakalpojumu sniedzēji, kuru pakalpojumi tika sniegti jebkurā vietā, kur pieejams internets. Šajās diskusijās tika izvērtēti visi iepriekšminētie jurisdikcijas kritēriji un atzīts, ka kibernoziegumu jurisdikcijas pamats ir teritoriālā jurisdikcija un ka jurisdikciju (noteikt, piemērot, iztiesāt) var piemērot tiktāl, ciktāl tā nepārkāpj citu valstu suverēnās tiesības uz jurisdikciju. Savukārt, ja būtu izvirzīti citi jurisdikcijas principi, darbs pie KNK, visticamāk, tiktu pārtraukts un beigtos bez rezultāta. Tādējādi KNK jurisdikcijas kodols ir teritoriālās (subjektīvās un objektīvās, jeb paplašinātās) jurisdikcijas princips, kura neatņemama sastāvdaļa ir dalībvalstu suverenitāte.

Saskaņā ar KNK 22. pantu dalībvalstij ir jāpieņem tāds regulējums, lai paredzētu jurisdikciju par KNK pirmajā nodaļā noteiktajiem kibernoziegumiem savas valsts

teritorijā Savukārt, piemērojot paplašinātās jurisdikcijas doktrīnu, attiecināt to arī uz 1) karoga principu (kuģi, lidmašīnas); 2) personas principu; 3) dubultās kriminalitātes principu; 4) ārpus jebkuras valsts teritoriālās jurisdikcijas principu. Tomēr, kā ir uzsvērts juridiskajā literatūrā, neviena dalībvalsts rīcība nedrīkst pārkāpt citas valsts teritoriālo jurisdikciju (Ķinis, 2015) jeb, citiem vārdiem sakot, suverenitāti (*Koops*, 2006). Taču raksts nesasniegtu savu mērķi, ja netiktu analizēti arī citu KNK dalībvalstu kriminālprocesuālie regulējumi saistībā ar ADAS pārmeklēšanu un datu izņemšanu. Proti, vai dalībvalstis paredz procesa virzītājam tiesības veikt datu pārmeklēšanu un izņemšanu no ārpus valsts teritorijas esošām sistēmām.

Automatizētās datu apstrādes sistēmā esošo datu kontroles regulējuma salīdzinošā kriminālprocesuālā analīze

Šajā raksta daļā tiek veikta atsevišķu valstu, kuras ir ratificējušas KNK (*Council of Europe*, 2020) – Austrijas, Bulgārijas, Francijas, Igaunijas, Polijas, Lietuvas, Norvēģijas, Vācijas, Ukrainas, Rumānijas, Slovēnijas, Slovākijas, Portugāles, Zviedrijas un Spānijas –, kriminālprocesuālo regulējumu un pieeju attiecībā uz datu kontroli ārvalstu ADAS salīdzinošā analīze.

Austrija. No Kriminālprocesuālā kodeksa izriet, ka nav atsevišķas normas, kurā būtu norādīts, ka kodekss darbojas tieši un tikai valsts iekšienē. Atbilstoši šī kodeksa 25. panta pirmajai daļai, ja noziedzīgā nodarījuma izdarīšanas vieta atrodas ārpus valsts vai šo vietu nevar noteikt, tad izšķirošā nozīme ir vietai, kur noziedzīgā nodarījuma sekas iestājās vai tām vajadzēja iestāties. Savukārt no šī panta septītās daļas izriet: ja noziedzīgais nodarījums bija noticis vai tam bija jānotiek citā Eiropas Savienības dalībvalstī, prokuratūrai ir pienākums nekavējoties par to paziņot citai dalībvalstij, izņemot gadījumus, kad likumpārkāpumu regulē nacionālā jurisdikcija. Kriminālprocesuālā kodeksa 115. panta pirmā daļa regulē priekšmetu izņemšanu un netiek paredzēts, ka šiem priekšmetiem būtu jāatrodas tieši valsts teritorijā. Jāatzīmē, ka no kodeksa 111. panta otrās daļas izriet, ka katrai personai, kas ir tiesīga rīkoties ar datu nesēju, ir pienākums sniegt pieeju datiem (*Rechtsinformationssystem des Bundes*, 2020).

Bulgārija. No Bulgārijas Kriminālprocesa kodeksa 172. panta pirmās daļas izriet, ka kriminālprocesa izmeklēšanā var tikt piemērota speciālā datu pārbaude. Savukārt atbilstoši šī panta trešajai daļai likumā noteiktajos gadījumos datoru un informācijas pakalpojumu sniedzējiem ir pienākums sniegt atbalstu tiesai un pirmstiesas izmeklēšanas iestādēm datu vākšanā un reģistrācijā, izmantojot speciālos tehniskos līdzekļus (*Наказателно-процесуален кодекс*, 2020).

Francija. Kriminālprocesa kodeksa pants "706-102-1" paredz iespēju bez ieinteresēto personu piekrišanas piekļūt datoru datiem, tos reģistrēt, glabāt un pārsūtīt. (*Legifrance*, 2020). Tāpat arī šajā pantā nav norādes par konkrētu teritoriju, kur datoram vai tā datiem jāatrodas. Ja ir noteikts, ka informācijas sistēma atrodas ārvalstī, tad datus

no šīs sistēmas var iegūt, ievērojot starptautiskajās saistībās ietvertos nosacījumus (*Legicoop*, 2020).

Igaunija. No Kriminālprocesa kodeksa 126.^{7} panta izriet, ka kriminālprocesa ietvaros var veikt informācijas pārtveršanu vai apskati publiskajos elektroniskajos sakaru tīklos. Šajā normā nav norādes uz teritoriju, kurā jāatrodas elektroniskajam sakaru tīklam (*Riigi Teataja*, 2020). Ja datu meklēšanas vai datora ekspertīzes laikā no esošās sistēmas var likumiski piekļūt citai sistēmai bez šīs sistēmas uzlaušanas vai drošības nosacījumu pārkāpuma, tad tiesībaizsardzības iestādes var turpināt un paplašināt meklēšanu konkrētajā sistēmā (*Legicoop*, 2020).

Polija. No Kriminālprocesa kodeksa 241. panta izriet, ka kriminālprocesā var tikt veikta datu kontrole (*Kancelaria Sejmu*, 2020), taču šajā pantā nav norādes uz informācijas sistēmas teritoriālo piekritību. Likumā nav regulēti jautājumi, kuri ir saistīti ar datu pārmeklēšanu ADAS (*Legicoop*, 2020).

Lietuva. Atbilstoši Kriminālprocesa kodeksa 154. pantam kriminālprocesa ietvaros var tikt veikta datu kontrole elektroniskajos sakaru tīklos. Šajā normā nav atsevišķas norādes uz teritoriju, kur jāatrodas datiem un elektroniskajam sakaru tīklam. Savukārt saskaņā ar kodeksa 4. panta otro daļu neatkarīgi no tā, kur noziedzīgais nodarījums tika izdarīts, kriminālprocess Lietuvas Republikas teritorijā notiek saskaņā ar Lietuvas Republikas Kriminālprocesa kodeksu (*Lietuvos Respublikos Seimas*, 2020).

Norvēģija. Saskaņā Kriminālprocesa likuma 216. pantu tiesa var atļaut veikt publiski nepieejamās informācijas (datu) nolasīšanu datorsistēmā vai lietotāja kontā, kas paredzēts tīkla sakaru un glabāšanas pakalpojumiem un pieder aizdomās turētajam, vai var tikt pieņemts, ka viņš vēlas tos izmantot. Tāpat datu nolasīšana ietver sakarus, elektroniski saglabātus datus un citu informāciju par datorsistēmas vai lietotāja konta izmantošanu. Atbilstoši šī likuma 4. pantam likuma noteikumus piemēro ar ierobežojumiem, kas ir atzīti starptautiskajos tiesību aktos vai izriet no līguma ar ārvalsti (*LOVDATA*, 2020).

Vācija. Atbilstoši Kriminālprocesa kodeksa 100.b panta pirmajai daļai bez attiecīgās personas ziņas var iejaukties viņas izmantotajā informācijas tehnoloģiju sistēmā un no tās var apkopot datus (veikt meklēšanu tiešsaistē). Tāpat no šī kodeksa otrās nodaļas izriet, ka šī kodeksa ietvaros veicamās izmeklēšanas darbības ir veicamas tieši Vācijas Federatīvās Republikas teritorijā (*Bundesministeriums der Justiz und für Verbraucherschutz*, 2020). Gadījumā, ja dati glabājas informācijas sistēmā, kura atrodas ārvalstī, un Vācijas varas iestādes piekļūst šiem datiem no Vācijas teritorijas, tad tas tiktu uzskatīts par ārvalsts suverēno tiesību pārkāpumu. Taču tas neattiecas uz tādiem ārvalstī esošajiem datiem, kuri ir publiski pieejami vai par kuriem ir saņemta labprātīga personas, kurai ir tiesības datus izņemt un veikt to pārraidi sistēmā, piekrišana. Citos gadījumos jāizmanto tiesiskās palīdzības lūguma mehānismi (*Legicoop*, 2020).

Ukraina. Saskaņā ar Ukrainas Kriminālprocesa kodeksa 264. panta pirmo punktu var tikt veikta informācijas sistēmā vai tās daļās esošo ziņu meklēšana un fiksācija, nodrošināta pieeja informācijas sistēmai vai tās daļām, kā arī ziņu iegūšana bez īpašnieka vai valdītāja piekrišanas, ja ir informācija par datu, kuriem ir nozīme pirmstiesas izmeklēšanā,

esamību informācijas sistēmā vai tās daļā. Savukārt šī kodeksa pirmā panta pirmais punkts nosaka, ka kriminālprocess Ukrainas teritorijā tiek noteikts tikai ar Ukrainas kriminālprocesa normatīvajiem aktiem (*Уголовный процессуальный кодекс*, 2020).

Rumānija. Atbilstoši Kriminālprocesuālā kodeksa 168. panta astotajai daļai gadījumā, ja, pārmeklējot informācijas sistēmu, tajā tiek konstatēta cita informācijas sistēma un dati, kuriem var piekļūt no šīs sistēmas, tad prokurors nekavējoties pavēl datus saglabāt, nokopēt identificētos datus un nekavējoties lūgt pabeigt rīkojuma izpildi. Šajā normā nav norādes, kur dati teritoriāli atrodas. Tas ir saistīts ar to, ka tā ir attālināta operācija attālinātā vietā, un vienīgais, ko var darīt, – saglabāt datu kopiju (*Legicoop*, 2020).

Slovēnija. No Kriminālprocesuālā kodeksa 150. panta izriet, ka atsevišķos ar likumu noteiktajos gadījumos kriminālprocesa ietvaros var tikt veikta elektronisko sakaru kontrole ar noklausīšanos un ierakstīšanu, kā arī visu elektronisko sakaru tīklos pārraidīto saziņas veidu kontrole. Šajā normā nav norādes, kur informācijas sistēmai un datiem jāatrodas (*Pravno-informacijski sistem*, 1995).

Slovākija. Krimināprocesa kodekss nepieļauj iespēju piekļūt datiem, kuri atrodas citas valsts ADAS. Slovākijas varas iestādes norāda, ka piekļūt šāda veida datiem ir iespējams, izmantojot Eiropas izmeklēšanas rīkojumu (*Legicoop*, 2020).

Portugāle. No Kibernoziegumu likuma 15. panta piektās daļas izriet, ka tiesībaizsardzības iestādēm ir tiesības piekļūt attālinātajām datorsistēmām no pārmeklējamā datora, ja pārmeklēšanas laikā tiek konstatēts, ka no šīs sistēmas (kura sākotnēji tika pārmeklēta) var likumiski piekļūt citai datorsistēmai (*Procuradoria-Geral Distrital de Lisboa*, 2009). Šī norma nenorāda, kur sistēmai fiziski jāatrodas – valsts teritorijā, ārzemēs, nezināmā atrašanās vietā (*Legicoop*, 2020).

Zviedrija. Varasiestādēm nav tiesību īstenot savas pilnvaras ārpus Zviedrijas teritorijas, kas nozīmē, ka datu pārmeklēšana nevar tikt īstenota citu valstu teritorijās (*Legicoop*, 2020).

Spānija. Atbilstoši Kriminālprocesuālā kodeksa 588. panta 3. punktam, ja sistēmas pārmeklēšanas laikā rodas pamatoti iemesli uzskatīt, ka meklējamie dati tiek glabāti citā datorsistēmā, meklēšana var tikt paplašināta, ja datiem var tiesiskā veidā piekļūt caur sistēmu, kurā pārmeklēšana notiek. Nav atsevišķu norāžu, kur teritoriāli jāatrodas sistēmai. Tāpat parasta tehnisku ierīču izņemšana nedod tiesības piekļūt šīs iekārtas datiem bez tiesneša sankcijas (*Legicoop*, 2020).

No analīzes secināms, ka valstīm ir atšķirīga pieeja attiecībā uz datu kontroli ārvalstu ADAS.

Krimināltiesiskās jurisdikcijas regulējums Latvijā

Krimināllikuma 4. pantā "Krimināllikuma spēks ārpus Latvijas teritorijas" (Krimināllikums, 1998) ir iestrādāti visi KNK 22. pantā noteiktie jurisdikcijas principi. Krimināllikuma 4. pants ietver gan subjektīvo, gan arī objektīvo (paplašināto) teritoriālo jurisdikciju un no tās izrietošo personas jurisdikciju, karoga jurisdikciju, ārpus

jebkādas jurisdikcijas esošo teritoriju jurisdikciju, aizsardzības un seku jurisdikciju. Krimināllikums neparedz jurisdikcijas piemērošanai dubultās krimināltiesību ierobežojumu, ko paredz lielākā daļa KNK dalībvalstu. Taču tas nekādā veidā nerada priekšrocības noziegumu izmeklēšanā, ja persona, kura pēc Krimināllikuma būs izdarījusi noziedzīgu nodarījumu, atradīsies ārpus valsts robežām, jo lielākā daļa KNK dalībvalstu šo principu gan Krimināllikumā, gan arī Kriminālprocesā joprojām uzskata par pamatu sadarbības izvērtēšanai.

Savukārt KPL 3. pants "Krimināllikuma spēks telpā" paredz: "Kriminālprocesa likums nosaka vienotu procesuālo kārtību visos kriminālprocesos, kurus par Latvijas jurisdikcijā esošiem noziedzīgiem nodarījumiem veic tam pilnvarotas personas" (Kriminālprocesa likums, 2005). Arī KPL komentāru A daļā ir uzsvērts, ka pantā pausts vienots vispārīgs uzstādījums, ka visi kriminālprocesi Latvijas Republikā notiek saskaņā ar vienotu KPL noteiktu kārtību (Strada-Rozenberga, 2019). Taču, tā kā lielākā daļa nodarījumu ir saistīta ar globālu datu apriti, tad starp šiem pienākumiem un tiesībām veidojas paradokss. No vienas puses, valsts paredz krimināltiesību un attiecina to uz jebkuru valsts teritorijā esošu subjektu, bet, no otras puses, apsūdzības pierādīšanai nepieciešamās kriminālprocesuālās darbības valsts ir tiesīga attiecināt tikai uz ADAS, kas atrodas Latvijas valsts teritorijā.

Lai arī spēkā ir vispārējie noteikumi par jurisdikcijas teritoriālo darbību, valsts cenšas noregulēt tiesiskās attiecības, kuras ir saistītas ar tiesisko kārtību, – arī tajos gadījumos, kad šīs attiecības veidojas ārpus tās robežām (*Тамариновв*, 2019). Tāpēc KPL ir arī C daļa, kas tieši paredzēta starptautiskajai sadarbībai krimināltiesiskajā jomā un to reglamentē. Turklāt Kriminālprocesa likuma 673. panta pirmās daļas 4. punkts paredz arī sadarbību procesuālās darbības izpildē ārvalstīs (piemēram, izmantojot tiesiskās palīdzības lūgumus). Latvijas Republikas gadījumā atbilstoši Kriminālprocesa likuma 674. pantam Latvijas Republika var lūgt ārvalsti, izpildot krimināltiesiskās palīdzības lūgumu, piemērot Latvijas Republikā noteikto kriminālprocesuālo kārtību vai atsevišķus tās principus (Kriminālprocesa likums, 2005). Jāmin, ka atsevišķas valstis, piemēram, Vācija un Slovākija, norāda: lai piekļūtu ārvalstu ADAS datiem, nepieciešams izmantot starptautisko tiesību instrumentus, piemēram, jau minēto tiesiskās palīdzības lūgumu vai Eiropas rīkojuma orderi. Līdzīgi ir arī citās valstīs.

Suverenitāte un digitālā suverenitāte – teorētiska diskusija

Suverenitāte ir starptautisko tiesību fundamentāls princips. *Tallinn Manual* pētnieki ir atzinuši, ka uz valsts teritorijā esošu kiberinfrastruktūru, ko veido valsts teritorijā esošās komunikācijas, ADAS, tīkli, kabeļi, ir attiecināma nacionālās valsts suverēnā vara un no teritoriālās jurisdikcijas izrietošais suverenitātes princips (*Schmitt*, 2017). Tāpat *Tallinn Manual* eksperti norāda, ka valsts suverenitāte pār kiberinfrastruktūru rada divas sekas: 1) infrastruktūra tiek sargāta pēc nacionālās valsts likumiem; 2) valsts suverenitāte

savā teritorijā aizsargā visu kiberinfrastruktūru neatkarīgi no tā, vai tā pieder personai vai valstij, un neatkarīgi no mērķa, kāpēc infrastruktūra pastāv. *Tallinn Manual* eksperti, turpinot pētīt jautājumu par suverenitāti kibertelpā, atzina, ka valsts suverenitāte tiek iedalīta iekšējā un ārējā suverenitātē (*Schmitt*, 2017) un kiberinfrastruktūra attiecināma uz iekšējo suverenitāti. Tādēļ uz visu to, kas notiek attiecīgajā infrastruktūrā, valstij ir tiesības attiecināt savu jurisdikciju.

Turklāt suverenitāte attiecināma uz visiem kibertelpas līmeņiem, tostarp fizisko, loģisko un sociālo. Fizisko līmeni veido fiziskie tīkla elementi, ierīces, kabeļi, rūteri, serveri, datori. Loģisko – dati un protokoli, kas izmantojami, lai dati krustotos ar fizisko līmeni. Kibertelpas sociālo līmeni veido lietotāji, kas sniedz un izmanto informācijas pakalpojumus (*Schmitt*, 2017). Savukārt ārējā suverenitāte izriet no valsts suverenitātes, jo saskaņā ar ANO Hartas 2(1) pantu valstis ir tiesībās vienlīdzīgas (*Charter of the United Nations*, 1948). No tā izriet, ka dalībvalstīm ir tiesības veikt aktivitāti kibertelpā ārpus tās teritorijas, ievērojot starptautiskās tiesības. Taču tās rīcības metodes nedrīkst pārkāpt citu valstu suverenitāti (*Schmitt*, 2017). Kiberaktivitāšu kontekstā par teritoriālās suverenitātes pārkāpumu uzskatāma darbība, kuru viena valsts *ex officio* veic citas valsts teritorijā esošiem objektiem vai personām (*Schmitt*, 2017). Turklāt vairums *Tallinn Manual* rokasgrāmatas sastādīšanā iesaistīto ekspertu uzskata, ka valstij nav suverenitātes pār datiem, kas atrodas ārpus valsts robežām, izņemot starptautiskās tiesībās noteiktus gadījumus (*Schmitt*, 2017).

Var piekrist I. Ziemelei, ka šobrīd var runāt par suverenitātes paradoksu: suverenitāte kā a) augstākā vara pār konkrēto sabiedrību, b) absolūtā ārējā neatkarība, c) pilnīga tiesībspēja starptautiskās attiecībās (Ziemele, 2019). Jāpiekrīt arī Francijas Valsts padomes loceklei K. Bazī-Malorijai, ka valstis globālajā interneta pārvaldības procesā ir tikai viens no procesa partneriem (*Bazy-Malaurie*, 2018). Paradokss veidojas arī starp diviem valsts pienākumiem. No vienas puses, katras valsts pienākums ir apkarot kibernoziedzību, bet, no otras puses, tās pienākums ir arī ievērot starptautiskās tiesības un pienākumus, nepārkāpt citu valstu suverenitāti. Rezultātā kibernoziegumu apkarošana ir iespējama līdz zināmam brīdim, iekams darbība nenotiek vai arī netiek plānota cita starptautiska subjekta jurisdikcijā. Tāpēc svarīga ir *Tallinn Manual* ekspertu atziņa, ka suverenitāte ne vien piešķir tiesības, bet arī uzliek par pienākumu rīkoties (angļu val. *due diligence*) apzinīgi un apturēt un novērst noziedzīgus nodarījumus, kas tiek veikti no valsts teritorijas (*Schmitt,* 2017). Tomēr ir jānorāda, ka līdz šim visi pūliņi radīt efektīvāku starptautisko noregulējumu šajā jomā ir beigušies neveiksmīgi (*Henriksen*, 2019).

Jautājums par suverenitāti kibertelpā ir ļoti sarežģīts, tāpēc ne visi piekrīt *Tallinn Manual* ekspertu viedoklim. Piemēram, profesors Dans Svantesons (*Svantesson*, 2017) uzskata, ka jurisdikcijas jēdzienā teritorialitāte kā suverenitātes komponente ir jānodala no valstiskuma (angļu val. *statehood*) tiesībām noteikt jurisdikciju. D. Svantesons uzskata, ka būtu nepieciešams atteikties no teritorialitātes kā kiberjurisdikcijas kodola. Turklāt, pēc viņa domām, jurisdikcijas piemērošana būtu jāsaista ar apstākli, ka valsts tiesai, kas piemēro jurisdikciju, būtu jākonstatē un jāpamato būtiska saikne (angļu val. *substantial*

connection) un leģitīma interese (angļu val. *legitimate interest*) jurisdikcijas piemērošanā (*Svantesson*, 2017). Tas dotu iespēju dalībvalstī veikt arī pārrobežu pārmeklēšanu, nepārkāpjot valstu suverenitātes robežas. Tomēr 2016. gada OCTOPUS konferencē viņa idejas neatbalstīja lielākā daļa konferences dalībnieku, tostarp nacionālo valstu kibernoziegumu eksperti, diplomāti un lielāko globālo informācijas pakalpojumu sniedzēju pārstāvji. Turklāt, apspriežot Kibernoziegumu komitejas "*Cloud evidence group*" (*Council of Europe*, 2016), tika atzīts, ka, piemērojot KNK, dalībvalstis vēl pilnā mērā neizmanto 1959. gada 20. aprīļa Eiropas Padomes Konvenciju par savstarpējo palīdzību krimināllietās (*Council of Europe*, 1959) dotās iespējas. Piemēram, nacionālo valstu tiesību aizsardzības iestāžu pārstāvji pietiekami neizmanto tiešo komunikāciju ar globālajiem informācijas pakalpojumu sniedzējiem. Apspriežot šo ziņojumu, tika nolemts arī uzsākt darbu pie KNK Otrā papildprotokola.

2017. gadā Kibernoziegumu komiteja pieņēma Vadlīniju Nr. 10, kurā daļēji iestrādāta arī D. Svantesona ideja par būtisko saikni un leģitīmo interesi (*Council of Europe*, 2017). Vadlīnija ir oficiālā KNK 18. panta interpretācija. KNK 18. pants noteic: "Puse pieņem tādus normatīvos aktus un veic citus nepieciešamos pasākumus, lai pilnvarotu tās kompetentās institūcijas pieprasīt personai tās teritorijā iesniegt konkrētus datus, kas atrodas personas īpašumā vai kontrolē un kas ir saglabāti datorsistēmā vai datu uzkrāšanas vidē par abonentu." Vadlīnijā skaidrots, ka vietējo procesa virzītāju lēmumi ir attiecināmi arī uz tādiem pakalpojumu sniedzējiem, kuriem nav savas pārstāvniecības nacionālajā valstī, taču **kuru darbība valstī rada ekonomisku efektu**. Tieši šis ekonomiskais efekts arī pamato procesuālas darbības būtisko saikni un leģitimitāti. Taču KNK 18. pants attiecas tikai uz plūsmas un abonentu datu pieprasījumiem un to atklāšanu. Tie ir dati, kurus procesa virzītājs Latvijā var pieprasīt KPL 191. panta kārtībā. Līdz ar to šī Vadlīnija par abonentu datu pieprasīšanu ir piemērojama visiem digitālo platformu un pakalpojumu turētājiem un sniedzējiem, kuru darbība Latvijā rada ekonomisko efektu. Šie pieprasījumi ir attiecināmi arī uz ārvalstu jurisdikcijā esošajām datu glabātuvēm vai mākoņdatnēm. Eksperti, kas uzskata, ka "valstīm nav suverenitātes pār datiem, kas pārraidīti no ārvalstīm vai saglabāti ārvalstīs esošās ADAS, un ka šie dati uzskatāmi par ārpus nacionālās suverenitātes esošiem", arī *Tallinn Manual* ekspertu vidū palika mazākumā (*Schmitt*, 2017).

KNK ir strukturēta trīs nodaļās: 1) termini; 2) pasākumi, kas jāveic nacionālā līmenī (pasākumi, kas jāveic substantīvajās krimināltiesībās, un procesuālie līdzekļi, kuri dalībvalstīm jāievieš saistībā ar KNK), un 3) starptautiskā sadarbība, kur katra no šīm nodaļām sadalīta vairākās apakšnodaļās. KNK19. pants ir ietverts otrās nodaļas 4. apakšnodaļā, kas reglamentē tikai procesuālās darbības dalībvalstu teritorijā. Savukārt KNK 3. nodaļas "Starptautiskā sadarbība" 2. apakšnodaļā "Īpaši noteikumi" reglamentēta savstarpējā palīdzība attiecībā uz pagaidu pasākumiem. Apakšnodaļa paredz šādas procesuālas darbības: 1) sistēmā uzkrāto datu operatīvu saglabāšanu (KNK 29. pants); 2) saglabātās datu plūsmas operatīvu atklāšanu (KNK 30. pants); 3) savstarpēju palīdzību attiecībā uz piekļuvi uzkrātajiem datiem (KNK 31. pants); 4) pārrobežu piekļūšanu

uzkrātajiem datiem ar piekrišanu vai tur, kur tie ir publiski pieejami; 5) savstarpēju palīdzību datu plūsmas vākšanai reālā laikā; 6) savstarpēju palīdzību attiecībā uz satura datu pārtveršanu; 7) 24/7 tīklu.

Savstarpējā palīdzība saistībā ar KPL 219. pantā paredzēto darbību ir reglamentēta KNK 31. pantā. KNK PZ 292. paragrāfā norādīts, ka šis pants piemērojams gadījumos, ja nepieciešama starptautiskā sadarbība. Piemērojot KNK 19. pantu nacionālās valsts robežās, lai pārņemtu un atklātu ADAS saglabātus datus, kas atrodas Saņēmēja puses teritorijā, Puse var lūgt šo darbību veikt citai Pusei. Savukārt KNK 32. pants noteic, ka pārrobežu piekļūšana ADAS uzkrātiem datiem ir pieļaujama citā valstī tikai divos gadījumos: 1) ja uzkrātie dati ir publiski pieejami; 2) ja dati, kas iegūti no citas valsts teritorijas un izsniegti kompetentai iestādei, ir iegūti ar tādas personas atļauju, kurai ir likumīgas tiesības šos ADAS uzkrātos datus izsniegt kompetentai personai. KNK PZ 294. paragrāfā norādīts, ka šāda autorizēta persona varētu būt, piemēram, e-pastu pakalpojumu sniedzējs vai pats datu subjekts.

Tātad var secināt, ka KNK noteic, ka ADAS saglabāto datu pārrobežu pārmeklēšana un izņemšana ir pieļaujama tikai tad, ja tās nodrošināšanā tiek iesaistīta citas puses kompetentā institūcija vai amatpersona. Tādējādi KNK 19. pants uzskatāms par izmeklēšanas darbību, kuru dalībvalsts var veikt tikai nacionālās valsts ietvaros; šāda redakcija ir ietverta arī pašreizējā KPL 219. panta 2. daļas regulējumā. Var piekrist A. Lieljuksim, ka, kaut arī normas darbība attiecas tikai uz Latvijas teritorijā izvietotām ADAS, kas ģeogrāfiski izvietotas dažādās vietās, tomēr to varētu attiecināt arī uz Latvijā reģistrētiem un uzņēmējdarbību veicošiem ārvalstu uzņēmumiem, kuru ADAS veido vienotu tīklu gan Latvijā, gan arī ārpus tās (Lieljuksis, 2019). Savukārt, ja, pārmeklējot šo sistēmu, bez papildu identifikatoriem iespējams piekļūt datiem, kas atrodas citā valstī, tad procesa virzītājam ir jārīkojas KPL 83. nodaļā noteiktā kārtībā un KNK 31. panta kārtībā.

Eiropas Savienības digitālā suverenitāte

Termins "tehnoloģiskā vai digitālā suverenitāte" tiek attiecināts uz pasākumiem, kas nodrošina Eiropas Savienības līderību un stratēģisku autonomiju digitālā jomā, tostarp ekonomikā, kiberdrošībā, kibernoziegumu apkarošanā (*Madiega*, 2020). Eiropas Komisijas prezidente Urzula fon der Leiena norāda, ka digitālā suverenitāte apzīmē Eiropas spēju digitālā vidē veikt savas izvēles un rīcību, balstoties uz saviem likumiem un vērtībām. Ar to EK prezidente uzsvēra, ka Eiropai ir tiesības uz saviem likumiem, kas regulē interneta darbību (*Komaitis*, 2020). Kā norāda pētnieki, galvenais digitālās suverenitātes mērķis ir kontrolēt datu plūsmas un protokolus Eiropas Savienībā (*Floridi*, 2020). Vācijas prezidentūra ES paredz izstrādāt kopīgu Eiropas pozīciju un to pārstāvēt ANO interneta pārvaldības organizācijās un Kibernoziegumu ekspertu komitejā un attīstīt plašu ES diplomātiju ES kibersankciju noteikšanai par ES normatīvo aktu un vērtību pārkāpšanu (*Federal Foreign Office*, 2020). Patiesībā šī diskusija ir tikai loģisks turpinājums Eiropas

vienotās juridiskās, ekonomiskās telpas izveidošanai. Galvenais šīs diskusijas iemesls ir radīt neatkarīgu digitālu vidi, samazinot atkarību no ASV un Ķīnas (*Federal Foreign Office*, 2020).

Protams, ka, izveidojot vienoto tiesisko digitālo Eiropas Savienības telpu, Eiropas Savienība šajā teritorijā spēs daudz efektīvāk risināt arī pārrobežu ADAS pārmeklēšanas problēmu. Tomēr pastāv bažas, ka šādu ADAS pārmeklēšanu, kura fiziski atrodas citā ES dalībvalstī, Latvijas procesa virzītājs varēs veikt bez saskaņošanas ar attiecīgās dalībvalsts amatpersonām. Protams, ka sadarbības metodes var tikt vienkāršotas un process paātrināts, līdzīgi kā tas tiek paredzēts, izpildot jau spēkā esošos ES tiesiskās sadarbības instrumentus krimināllietās, tomēr ir ļoti apšaubāmi, ka dalībvalstis būs gatavas atteikties no savas suverenitātes, lai apkarotu kibernoziedzību, īpaši, ja tā būs saistīta ar būtisku iejaukšanos citu valstu iedzīvotāju pamattiesībās un brīvībās, ko vairāku ES valstu konstitucionālās tiesas ir pasludinājušās par neaizskaramu valsts konstitucionālo kodolu.

Neapšaubāmi, ka ES digitālā suverenitāte nosaka un arī turpmāk noteiks ES prioritātes kibernoziegumu apkarošanā, jo īpaši saistībā ar pārrobežu piekļuvi elektroniskajiem pierādījumiem (COM(2015) 185 final, 2015). Ir uzsākta diskusija par Eiropas Parlamenta un Padomes Regulu "Par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu iegūšanai krimināllietās" (COM/2018/225 final, 2018). Minētajā dokumentā uzsvērts, ka šā priekšlikuma mērķis ir uzlabot juridisko noteiktību iestādēm, pakalpojumu sniedzējiem un iesaistītajām personām, kā arī saglabāt augstus standartus tiesībaizsardzības pieprasījumiem, tādējādi nodrošinot pamattiesību aizsardzību, pārredzamību un atbildību. Minētā Regula paredz ieviest jaunus e-pierādījumu sniegšanas un saglabāšanas rīkojumus, kuri balstīsies uz savstarpējās atzīšanas principiem. Jebkurā krimināllietā ar tiem varēs pieprasīt tikai abonenta un noslodzes datus. Savukārt, lai iegūtu darījuma vai satura datus, rīkojumu tiesa varēs izdot tikai par nodarījumiem, kur soda maksimālais apmērs izdevējvalstī ir ne mazāks par trim gadiem, vai par noziegumiem, kuri saistīti ar terorismu.

Īpaši uzsverot, ka Regulas priekšlikums tiek gatavots tā, lai atbilstu KNK, nepieciešams apskatīt arī ES kā organizācijas iesaisti KNK otrā papildu protokola izstrādes procesā. Kaut arī KNK neparedz, ka ES varētu pievienoties šim līgumam, ES piedalās arī Kibernoziegumu konvencijas otrā protokola izstrādes procesā kā novērotāja organizācija, jo no 62 KNK dalībvalstīm 26 ir ES dalībvalstis. Respektīvi, tās dalībnieki ir visas valstis, izņemot Īriju un Zviedriju, kas turpina sarunas par pievienošanos KNK. Eiropas Komisija uzskata, ka saskaņā ar LEZD 3. panta 2. punktu (Līgums par Eiropas Savienības darbību) tās kompetencē ir arī noslēgt starptautisku līgumu "tiktāl, ciktāl līguma slēgšana ietekmē Savienības kopīgos noteikumus vai maina to jomu". Tādējādi darbu pie KNK otrā papildu protokola ES uzskata par tādu, kas nākotnē var būtiski ietekmēt arī ES kopīgos noteikumus. Eiropas Komisijas sarunu mandātā (COM(2019) 71 final, 2019) ir ietverta arī diskusija par starptautiskiem e-pierādījumu sniegšanas rīkojumiem, paplašinātu meklēšanu un piekļuvi, kas iespējama, pamatojoties uz pārmeklējamās sistēmas akreditācijas datiem.

Valsts policijas priekšlikuma satura izvērtējums

VP priekšlikums ir veikt grozījumus KPL 219. panta otrajā daļā, svītrojot vārdus "Latvijas teritorijā esošā" un izsakot normu šādā redakcijā: "Ja ir pamats uzskatīt, ka meklētie dati (informācija) tiek uzglabāti citā sistēmā, kurai var piekļūt autorizēti, izmantojot izmeklēšanas tiesneša lēmumā minēto sistēmu, jauns lēmums nav nepieciešams." Priekšlikuma autori norāda, ka minētā norma nav grozīta kopš 2005. gada un ka likumdevējs, pieņemot šādu normu, nevarēja paredzēt tehnoloģiju un informācijas pakalpojumu transformāciju, proti, ka ADAS vai tās daļa vairs nav saistāma ar konkrētas valsts teritoriju – tā var atrasties jebkurā valstī, bieži vien neidentificētā. Vēl vairāk, izmeklēšanas laikā gandrīz neesot iespējams identificēt un pierādīt, ka noteiktā ADAS daļa, kurai var piekļūt autorizēti, atrodas Latvijas vai citas valsts teritorijā. Turklāt gan procesa virzītājs, gan tiesnesis, gan pat kontrolējamā persona varot arī nezināt, kur fiziski atrodas viņu rīcībā neesošas attālinātas piekļuves automatizētās datu apstrādes sistēmas daļas.

Līdz ar to VP uzskata, ka mūsdienu pasaulē informācijas tehnoloģijas un to risinājumi vairs nav saistāmi ar konkrētu valsts teritoriju, tāpēc, lai efektivizētu KPL 219. panta normas piemērošanu, nepieciešams atteikties no norādes, ka tā attiecināma tikai uz Latvijas teritoriju. Papildu priekšlikuma pamatojumam VP izmanto 2019. gada 28. marta Norvēģijas Augstākās tiesas nolēmumu (*Supreme Court of Norway*, 2019), kur tiesa atzinusi, ka policijai ir tiesības *Oslo Tidal Music AS* ADAS pārmeklēt un izņemt arī datus, kas tiek uzglabāti ADAS ārpus Norvēģijas. Lai izvērtētu minēto spriedumu, būtu nepieciešama plašāka analīze, taču interesants ir apstāklis, ka tiesa, analizējot Kibernoziegumu konvenciju, analizē tikai KNK 18. pantu, kas tiešām nosaka minimumu, kas valstij jāizpilda, pievienojoties Konvencijai, bet neanalizē Konvencijas Starptautiskās sadarbības daļu, konkrēti 32. panta b punktu, kas nevis nosaka minimumu, bet gan strikti reglamentē pieļaujamos pārrobežu pārmeklējamos gadījumus, ja dati pieejami no pārmeklēšanai pakļautās sistēmas. Tādēļ var secināt, ka argumenti, ko tiesa izmantojusi šāda viedokļa taisīšanai, ir vairāk balstīti uz nacionālām interesēm, nevis uz starptautisku avotu analīzi.

No priekšlikuma pamatojuma var izdalīt divas tiesiskās situācijas. Pirmā, kad no pārmeklējamās sistēmas iespējams ar esošajiem identifikatoriem iegūt datus, kuru teritoriālo piederību nav iespējams noskaidrot, piemēram, dati, kas atrodas *Dark web* vai citos šifrētos interneta resursos. Šajā gadījumā var tikt piemērota prezumpcija, ka šie dati atrodas ārpus jebkādas jurisdikcijas, līdz ar to nav pakļauti nevienai jurisdikcijai, un valsts policijai ir likumīga pieeja šiem datiem pat bez speciālu normu grozīšanas. Otrā, kad, pārmeklējot sistēmu, ir skaidrs, ka dati atrodas pie konkrēta pakalpojuma sniedzēja, kurš darbojas un kura infrastruktūra (fiziskā, loģiskā) atrodas citas valsts teritorijā, kas atbilstoši *Tallinn Manual* ekspertu viedoklim ir pakļauti tās valsts, kurā tie atrodas, suverenitātei. Līdz ar to izmeklēšanas darbība ir pieļaujama tiktāl, ciktāl tā neaizskar citu starptautisku tiesību subjektu suverenitāti un tiesības uz jurisdikciju.

Secinājumi

1. Kriminālprocesa likuma 219. pants "Automatizētās datu apstrādes sistēmā esošo datu kontrole" ir ieviests, lai Latvija varētu pievienoties KNK. Līdz ar to tā saturs ir atklājams tikai kopsakarībā ar KNK 19. pantu un KNK Paskaidrojošā ziņojuma tekstu, kas uzskatāms par oficiālu KNK teksta interpretācijas līdzekli. Tā kā nekādi citi starptautiski dokumenti par datu pārmeklēšanu un izņemšanu nav pieņemti, jāsecina, ka pēc būtības nekas šī panta saturā no KNK pieņemšanas brīža nav mainījies, jo arī 2001. gadā bija pārrobežu informācijas pakalpojumu pieejamība.
2. Minētais pants ir iekļauts KNK 2. sadaļā, kur noteikti minimālie pasākumi, kas dalībvalstīm jāveic, lai efektivizētu kibernoziegumu apkarošanu dalībvalsts teritorijā. KNK PZ ir speciāli uzsvērts, ka šo instrumentu nevar izmantot, lai veiktu pārrobežu sistēmu pārmeklēšanu. Savukārt starptautisko sadarbību, tostarp izpildot dalībvalstu lūgumus veikt sistēmu pārmeklēšanu, datu izņemšanu un pārrobežu datu pieejamību, kuri pieejami, izmantojot pārmeklējamā sistēmā esošos identifikatorus, var veikt tikai KNK 31. un 32. pantā noteiktajos gadījumos. Turklāt šis uzskaitījums bez papildu starptautiskās vienošanās nav paplašināms.
3. Kibernoziegumu jurisdikcijas kodolu, kā tas ir noteikts KNK 22. pantā, noteic valstu teritorialitāte un suverenitāte. Turklāt lielākā daļa ekspertu uzskata, ka suverenitāte ir attiecināma arī uz valsts teritorijā esošo kiberinfrastruktūru (tehnisko, loģisko un sociālo līmeni). Taču, kā norādīts iepriekš citētajā *Tallinn Manual 2.0*, suverenitāte uzliek dalībvalstīm arī pienākumus apkarot kibernoziegumus, lai nepieļautu kaitējuma nodarīšanu citu valstu subjektiem un objektiem.
4. Apkopojot salīdzinošā pētījuma rezultātus, var secināt, ka valstīm, kuras ir ratificējušas KNK, ir dažādas pieejas attiecībā uz datu kontroli ārvalstu ADAS. Piemēram, Vācijas, Zviedrijas, Austrijas u. c. valstu normatīvie akti nedod tiesības piekļūt ārvalstu ADAS datiem, savukārt Spānijas, Portugāles un Rumānijas normatīvie akti tādu iespēju pieļauj. Tāpat jāatzīmē, ka atsevišķu valstu krimināltiesiskajos regulējumos nav iestrādāta norāde uz pārmeklējamo datu teritoriālo atrašanās vietu. Tas viss liecina par valstu dažādām pieejām KNK normu interpretācijā.
5. Izvērtējot Valsts policijas priekšlikumu par KPL 219. panta otrās daļas grozīšanu, autori uzskata, ka ir vērtējamas divas juridiskas situācijas: pirmā – kad no pārmeklējamās sistēmas iespējams ar esošajiem identifikatoriem iegūt datus, kuru teritoriālo piederību nav iespējams noskaidrot. Šajā gadījumā var tikt piemērota prezumpcija, ka dati, kas atrodas ārpus jebkādas jurisdikcijas, nav pakļauti nevienai citas valsts jurisdikcijai. Līdz ar to procesa virzītājam ir likumīga pieeja šiem datiem pat bez KPL 219. panta normu grozīšanas. Otrā situācija – ja procesa virzītājam ir zināms, ka dati atrodas citā jurisdikcijā esošā sistēmā, tad procesa virzītājs var piemērot jurisdikciju tiktāl, ciktāl tā nepārkāpj citu starptautisko tiesību subjektu teritorialitāti un suverenitāti.

Control of Data Located in Automated Data Processing Systems: National and International Application Aspects

Abstract

The article "Control of Data Located in Automated Data Processing Systems: National and International Application Aspects" is the result of the idea initiated by the proposal submitted by the Latvian State Police, to the Permanent Working Group of Criminal Procedure Experts of the Ministry of Justice regarding the amendment of Section 219, Paragraph 2 of the Criminal Procedure Law. Article 219 of the Criminal Procedure Law "Control of Data in an Automated Data Processing System" is essentially analogous to Article 19 of the Cybercrime Convention, which obliges Member States to adopt such legislation as to facilitate the search of data in systems located within their territory.

The essence of the proposal is to renounce the national territorial application clause in the Article, as it restricts the police operability to obtain evidence in criminal proceedings in situations where data stored in another computer systems are located outside of the territory of Latvia but are legally accessible from searchable system via Internet. In other words, to change the scope of jurisdiction of search and seizure to transborder search and seizure.

The debate on whether one Member State is entitled to search and capture data in a system located in the territory of another Member State, is not new. It has been running since the adoption of the Convention and it is believed it will continue at least until the adoption of the Second Additional Protocol to the Convention, which should address issues related to cybercrime investigations.

In the article, the authors will analyse what and how the situation has fundamentally changed since the adoption of the Cybercrime Convention and the Criminal Procedure Law, especially regarding the understanding of jurisdiction in the application of criminal procedural instruments. The authors also aim to provide their solutions for solving problems in relation with the proposal submitted by the State Police.

Keywords: control of data, automated data processing systems, cybercrime convention, evidence in criminal proceedings, sovereignty, criminal jurisdiction, data search and seizure.

Avoti un literatūra

1. Bazy-Malaurie, C. 2018. The digital world: what relationship between the jurisdictions? In: *The Role of Constitutional Courts in the Globalised World of the 21st Century. Proceedings of the 2018 Conference of the Constitutional Court of the Republic of Latvia*. Rīga: Latvijas Republikas Satversmes tiesa.

2. Bundesministeriums der Justiz und für Verbraucherschutz. 03.12.2020. *Strafprozeßordnung*. Iegūts no: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html
3. EUR-Lex. 2015. Eiropas Drošības programma – COM(2015) 185 final. Iegūts no: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=LEGISSUM:230801_2
4. EUR-Lex. 2019. *Eiropas Komisija. Ieteikums. Padomes lēmums, ar ko pilnvaro piedalīties sarunās par otro papildu protokolu Eiropas Padomes Konvencijai par kibernoziegumiem (Eiropas Padomes līgumu sērija Nr. 185)*. Iegūts no: https://eur-lex.europa.eu/resource.html?uri=cellar:8d1e03fe-2939-11e9-8d04-01aa75ed71a1.0016.02/DOC_1&format=PDF
5. EUR-Lex. 2018. *Priekšlikums. Eiropas Parlamenta un Padomes Regula. Par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu gūšanai krimināllietās*. Iegūts no: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018PC0225&from=LV
6. Council of Europe. 1959. European Convention on Mutual Assistance in Criminal Matters. *ETS No.030*. Strasbourg.
7. Council of Europe. 1990. *Computer-Related Crime. Recomendation No. R (89) 9 on computer-related crime and final report of the European Committe on Crime Problems.* Iegūts no: http://www.oas.org/juridico/english/89-9&final%20Report.pdf
8. Council of Europe. 1995. *Recommendation R(95)13 concerning problems of criminal procedure law connected with information technology*. Iegūts no: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76
9. Council of Europe. 2001. *Convention on Cybercrime.* Iegūts no: https://rm.coe.int/1680081561
10. Council of Europe. 2001. *Explanatory Report to the Convention on Cybercrime.* Iegūts no: https://rm.coe.int/16800cce5b
11. Council of Europe. 16.09.2016. *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Final report of the T-CY Cloud Evidence Group*. Iegūts no: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e
12. Council of Europe. 2017. *T-CY Guidance note # 10 Production orders for subscriber information.*
13. Council of Europe. 21.12.2020. *Chart of signatures and ratifications of Treaty 185*. Iegūts no: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zCdleT3v
14. Elektronisko sakaru likums: Latvijas Republikas likums: pieņemts 28.10.2004. un stājās spēkā 01.12.2004. *Latvijas Vēstnesis. 183*, 17.11.2004.
15. European Commission. 1996. *Illegal and harmful content on the Internet.* Iegūts no: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF
16. Federal Foreign Office. 2020. *Digital Sovereignty*. Iegūts no: https://erstelesung.de/wp-content/uploads/2020/10/20-10-14_Germany_EU_Digital-Sovereignty.pdf
17.Federal Foreign Office. 2020. *Expanding the EU's digital sovereignty*. Iegūts no: https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828
18. Floridi, L. 12.08.2020. *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*. Iegūts no: https://link.springer.com/article/10.1007%2Fs13347-020-00423-6
19. Henriksen, A. 22.01.2019. The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity. 5*(1). Iegūts no https://doi.org/10.1093/cybsec/tyy009
20. Kancelaria Sejmu. 2020. *Kodeks postępowania karnego*. Iegūts no: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970890555/U/D19970555Lj.pdf

21. Komaitis, K. 07.09.2020. Europe's pursuit of digital sovereignty could affect the future of the Internet. *TECH.EU*. Iegūts no: https://tech.eu/features/32780/europe-digital-sovereignty/
22. Koops, B. J. (ed). 2006. *Cybercrime and jurisdiction*. T. M. C. Asser Press.
23. Krimināprocesa likums: Latvijas Republikas likums: pieņemts 21.04.2005. un stājās spēkā 01.10.2005. *Latvijas Vēstnesis. 74*, 11.05.2005.
24. Ķinis, U. 2015. *Kibernoziedzība, kibernoziegumi un jurisdikcija*. Rīga: Jumava.
25. Legicoop. 2020. https://www.gip-jci-justice.fr/en/projects/intra-european/legicoop-network-for-legislative-cooperation-between-the-ministries-of-justice-of-the-european-union
26. Legifrance. 2020. *Code de procédure pénale*. Iegūts no: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006167524/#LEGISCTA000038311671
27. Lieljuksis, A. 2019. 219. pants. Automatizētās datu apstrādes sistēmā esošu datu kontrole. No: Strada-Rozenberga, K., red. *Krimināprocesa likuma komentāri. A daļa*. Rīga: Latvijas Vēstnesis.
28. Lietuvos Respublikos Seimas. 19.12.2020. *Baudžiamojo proceso kodeksas*. Iegūts no: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr#part_7ca4d122f6c8443f8d18e908c735dcde
29. LOVDATA. 04.12.2020. *Straffeprosessloven*. Iegūts no: https://lovdata.no/dokument/NL/lov/1981-05-22-25/*#&#x2a
30. Madiega, T. 2020. Digital sovereignty for Europe. *European Parliamentary Research Service*. Iegūts no: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
31. Meikališa, A. 2019. 179. pants. Kratīšana. No: Strada-Rozenberga, K., red. *Krimināprocesa likuma komentāri. A daļa*. Rīga: Latvijas Vēstnesis.
32. 32. Pravno-informacijski sistem. 01.01.1995. *Zakon o kazenskem postopku*. Iegūts no: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362#
33. Procuradoria-Geral Distrital de Lisboa. 15.12.2009. *Lei do Cibercrime*. Iegūts no: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis
34. Rechtsinformationssystem des Bundes. 21.12.2020. *Strafprozeßordnung 1975*. Iegūts no: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326
35. Riigi Teataja. 07.05.2020. *Kriminaalmenetluse seadustik*. Iegūts no: https://www.riigiteataja.ee/akt/119032015022?leiaKehtiv#para126b7
36. Schmitt, M. N. (ed). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
37.Strada-Rozenberga, K. 2019. 3. pants. Krimināprocesa spēks telpā. Strada-Rozenberga, K., red. *Krimināprocesa likuma komentāri. A daļa*. Rīga: Latvijas Vēstnesis.
38. Supreme Court of Norway. 28.03.2019. *HR-2019-610-A (case no. 19-010640STR-HRET), criminal case*. Iegūts no: no https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf
39. Svantesson, D. J. 2015. *A new jurisprudential framework for jurisdiction: beyond the Harvard Draft*. Iegūts no: https://core.ac.uk/download/pdf/205332442.pdf
40. Svantesson, D. J. 2017. *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press.
41. United Nations. 1948. *Charter of the United Nations*. Iegūts no: https://www.un.org/en/sections/un-charter/chapter-i/index.html

42. Ziemele, I. 2019. Constitutional courts as lock-gates in the globalized world. In: *The Role of Constitutional Courts in the Globalised World of the 21st Century*. Iegūts no: https://www.satv.tiesa.gov.lv/other/2019-ST-Referati-2018-atverumos.pdf
43. *Наказателно-процесуален кодекс*. 2020. Iegūts no: https://www.lex.bg/laws/ldoc/2135512224
44. Татаринов, М. 2019. Пространственное действие уголовной юрисдикции. *Международное право*. Iegūts no: https://nbpublish.com/library_read_article.php?id=29545 [sk. 20.12.2020.].
45. *Уголовный процессуальный кодекс*. 21.07.2020. Iegūts no: http://continent-online.com/Document/?doc_id=31197178#pos=5;-142