Nodaļa 5

UZTICAMĪBAS VEICINĀŠANA DIGITĀLAJAI EKONOMIKAI

Latvijas digitālās drošības politika

Šajā sadaļā ir sniegts plašs apraksts par digitālās drošības politiku Latvijā un tās analīze. Pirmajā *Latvijas kiberdrošības stratēģijā*, kas aptver 2014.-2018. gada periodu, tika novērtēta digitālā transformācija un iezīmēta pāreja uz stratēģiskāku un visas valdības pieeju digitālajai drošībai. Otrajā *Latvijas kiberdrošības stratēģijā*, kas aptver 2019.-2022. gadu, šis ceļš tiek turpināts, vairāk akcentējot risku pārvaldību, noturību, sabiedrības informētību un nepieciešamību līdzsvarot digitālo drošību ar atklātību, labklājību un cilvēktiesībām.

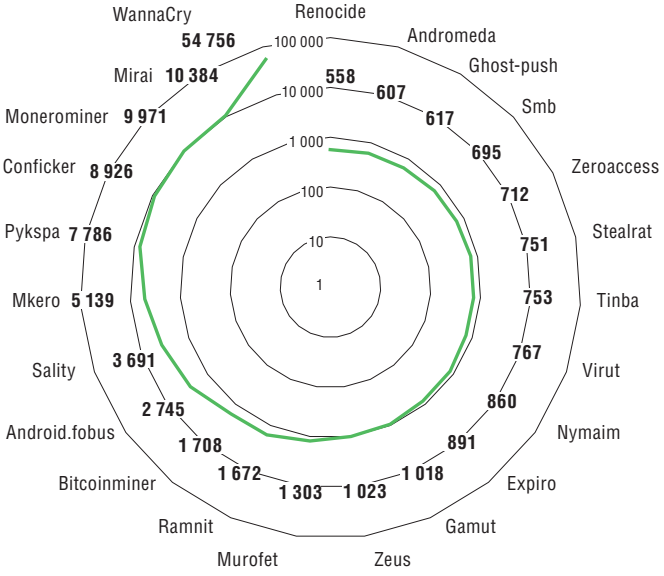
Šīs stratēģijas atspoguļo virzību Latvijas valdības attieksmē pret digitālās drošības politiku. Tomēr šajos dokumentos vai to ieviešanas procesos vēl nav pilnīgi ieviesti digitālās drošības ekonomiskie un sociālie riski. Faktiski Latvijas ģeopolitiskā vide ir likusi valdībai galvenokārt balstīties uz nacionālās drošības konceptuālo struktūru, kas koncentrējas uz kritiskām infrastruktūrām un valsts institūcijām. Varētu nostiprināt daudzu ieinteresēto pušu iesaistīšanos un uz tirgu orientētu politiku, lai pilnībā realizētu digitālās transformācijas potenciālu. Turklāt tas palīdzētu labāk attiecināt digitālās drošības risku uz augstāko vadību organizācijās un uzņēmumos, it īpaši mazajos un vidējos uzņēmumos MVU.

Jaunākās tendences

Uzbrukumi digitālajai drošībai Latvijā

2018.-2019. gadā plašsaziņas līdzekļu uzmanība Latvijā koncentrējās uz politiski motivētu organizāciju uzbrukumiem no valstīm "ar NATO un ES pretēju politisko ideoloģiju" (CERT.LV, 2018. gads). Kā piemērus var minēt darbības, kuru mērķis bija Latvijas Saeimas vēlēšanu process. Tomēr rūpīga analīze liecina, ka Latvija tāpat kā daudzas citas valstis cieta no uzbrukumiem ar globālāku tvērumu, piemēram, WannaCry un Mirai[1] (5.1. attēls). Tomēr šādu uzbrukumu ietekmēto organizāciju skaits Latvijā bija salīdzinoši zems. Digitālās drošības negadījumu galvenie upuri Latvijā bija MVU un pašvaldības (CERT.LV, 2018. gads).

5.1. attēls. Izplatītākie ļaunprātīgā koda uzbrukumi Latvijā, 2018. gads

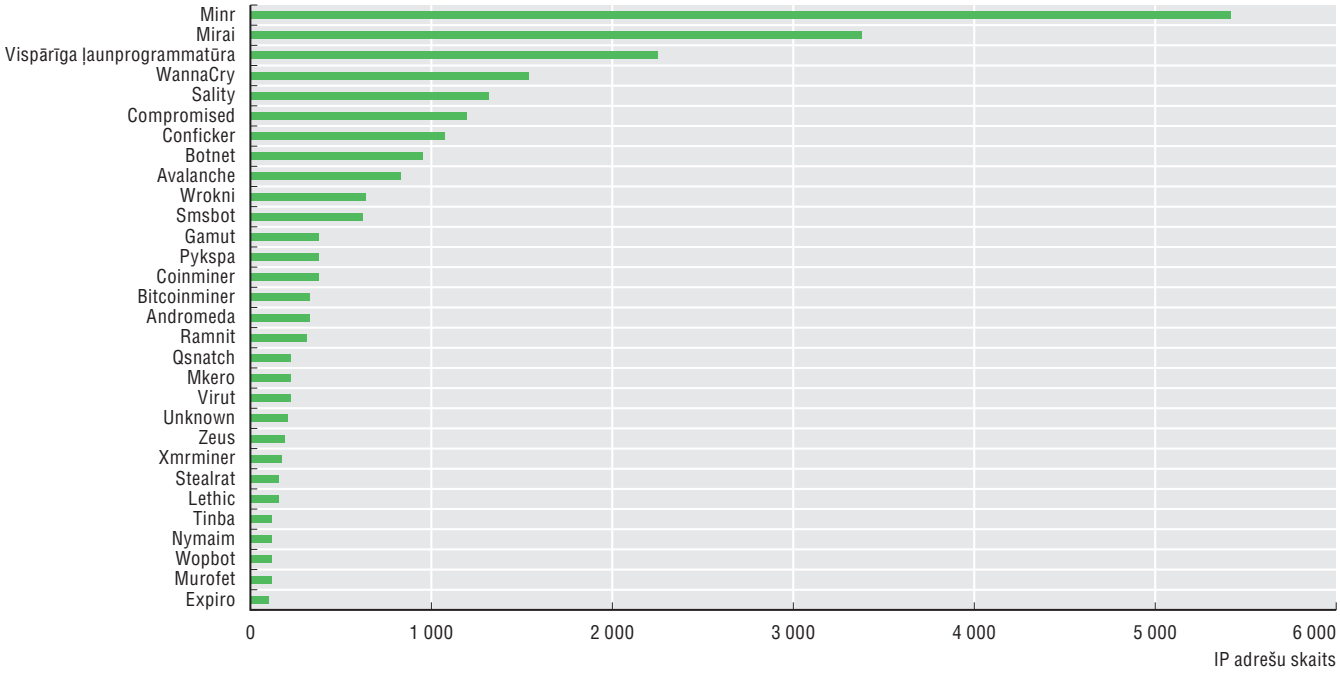


Avots: CERT.LV (2018), *CERT.LV Public Performance Report*, *https://cert.lv/uploads/cert-gada-parskats-2019.pdf*.

Jaunāki dati (5.2. attēls) apstiprina, ka pret Latvijas organizācijām mērķtiecīgi vērstās ļaunprogrammatūras galvenās formas atbilst šādām formām citās valstīs, un Mirai un WannaCry ir attiecīgi otrā un ceturtā izplatītākā ļaunprogrammatūra 2020. gada pirmajā ceturksnī. Minr kā izplatītākā ļaunprātīgā koda dominējošā pozīcija Latvijā šajā periodā ilustrē kriptovalūtu graujošās ļaunprogrammatūras globālo tendenci.

5.2. attēls. Izplatītākie ļaunprātīgā koda uzbrukumi Latvijā, 2020. gadā (1. cet.)

Ļaunprātīgā koda apdraudēto unikālo IP adrešu skaits, 2020. g. 1. cet.



Avots: CERT.LV (2020), *CERT.LV reģistrētie incidenti no 01.01.2020. līdz 31.03.2020*, *https://cert.lv/lv/2020/04/pieejama-statistika-par-2020-gada-1-ceturksni*.

Digitālās drošības politikas svarīgākie datumi Latvijā

Digitālā drošība nav jauna politikas joma Latvijā. Pirms 2012. gada Latvijas pieeja digitālajai drošībai galvenokārt koncentrējās uz tehniskajiem aspektiem un infrastruktūru. Satiksmes ministrija (SM) bija iestāde, kas atbild par digitālās drošības politikas vispārēju koordināciju .

2010. gadā Latvija pieņēma Informācijas tehnoloģiju drošības likumu ("IT drošības likumu"), kas stājās spēkā 2011. gadā un kalpo kā digitālās drošības galvenā juridiskā struktūra (skatiet sadaļu šeit: Tiesiskais regulējums). Tā rezultātā, *inter alia*, tika izveidota:

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV[2] ir Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienība, kas Informācijas tehnoloģiju drošības likumā noteiktās tiesības un pienākumus pilda Aizsardzības ministrijas pakļautībā atbilstoši normatīvajiem aktiem.
- Nacionālā informācijas tehnoloģiju drošības padome (NITDP) — organizācija, kas tiekas vismaz vienreiz četros mēnešos un sastāv no ministriju un citu digitālās drošības politikā iesaistītu publisku organizāciju pārstāvjiem.

2013. gadā Latvijas Ministru kabinets apstiprināja *Informācijas sabiedrības attīstības pamatnostādnes* (2014.-2020. g.) (VARAM, 2014. gads), kas kalpo kā nacionālā digitālā stratēģija. Pamatnostādņu pieņemšana atspoguļoja perspektīvas maiņu līdz ar atziņu, ka digitalizācija ietekmē visas sabiedrības daļas. Digitālās drošības riski ir kļuvuši par stratēģisku valsts politikas jautājumu, kurā ir nepieciešama daudzu ministriju iesaistīšanās, izmantojot visu valdības struktūru pieeju.

Šīs izmaiņas tika apstiprinātas 2014. gadā, pieņemot *Latvijas kiberdrošības stratēģiju (2014.-2018. gadam)*, kurā ir norādīts: "Priekšstatu, ka IKT ir tikai šauras profesionāļu grupas interešu sfērā, pakāpeniski aizstāj izpratne, ka ar IKT lielākā vai mazākā mērā ir saistīta visa sabiedrība" (AM, 2014. gads). Loģiski, ka stratēģijas pirmais mērķis bija skaidras pārvaldības struktūras izveide digitālajai drošībai Latvijā. Šī jaunā pārvaldības struktūra tika izveidota ap NITDP. Aizsardzības ministrijas (AM) pārņēma informācijas tehnoloģiju drošības politikas veidošanas un īstenošanas koordinēšanu.

2016. gadā AM sadarbībā ar citām ministrijām un NITDP veica stratēģijas īstenošanas vidusposma pārskatu, pēc tam 2019. gadā Latvijas Ministru kabinets apstiprināja ziņojumu par stratēģijas ieviešanu,

kurā ir secināts, ka lielākā daļa mērķu ir sasniegti vai atrodas izpildes procesā. Tomēr ziņojumā tika atzīti arī atsevišķu mērķu sasniegšanas šķēršļi, it īpaši šie: 1) digitālā drošība ne vienmēr ir lēmumu pieņēmēju prioritāte; 2) digitālās drošības prasmju trūkums; 3) digitālās drošības finansējuma trūkums.

Pamatojoties uz šiem elementiem, Latvijas Ministru kabinets 2019. gadā apstiprināja otro *Latvijas kiberdrošības stratēģiju (2019.-2022. gadam)*. Šajā dokumentā, ko AM sagatavoja sadarbībā ar citām ministrijām un NITDP, ir izklāstītas Latvijas digitālās drošības politikas nacionālās prioritātes un noteikti gaidāmie izaicinājumi. Jaunās stratēģijas galvenais mērķis ir nostiprināt un uzlabot digitālās drošības iespējas, palielinot noturību pret uzbrukumiem un uzlabojot sabiedrības informētību par apdraudējumiem kibertelpā.

Tas atspoguļo pozitīvu evolūciju Latvijas attieksmē pret digitālo drošību. Divu kiberdrošības stratēģiju attīstība un AM vadošā loma kopš 2013. gada ir padarījusi digitālo drošību par stratēģisku prioritāti Latvijā. Tomēr nacionālā drošība ir izvirzīta priekšplānā uz citu aspektu, it īpaši ekonomiskās un sociālās labklājības, rēķina (skatiet 5.3. attēlu). To ir apstiprinājusi analīze par definīciju kopu (saistītu ar digitālo drošību), kas ir iekļauta Latvijas politikas dokumentos (skatiet zemāk).

Digitālā drošība un ar to saistītie termini Latvijas politikā

Latvijas politikas dokumentu pamatā ir jēdzieni "kiberdrošība", "informācijas tehnoloģiju drošība" un "informācijas drošība" (AM, 2014. gads; VARAM, 2014. gads).

Savās 2015. gada *Rekomendācijās par digitālās drošības risku pārvaldību ekonomiskās un sociālās labklājības labā*, šeit un turpmāk "2015. gada rekomendācijā" (ESAO, 2015. gads) ESAO izmanto terminu "digitālā drošība", nevis "kiberdrošība", "informācijas drošība" vai "IT drošība". ESAO definē "digitālo drošību" kā tādu ekonomisko un sociālo risku pārvaldību, kuri izriet no informācijas un komunikācijas tehnoloģiju (IKT) un datu pieejamības, integritātes un konfidencialitātes (PIK). Šī definīcija atspoguļo virzību no 2002. gada ESAO *Informācijas sistēmu un tīklu drošības pamatnostādnēm* ("Drošības pamatnostādnes"), kas galvenokārt koncentrējās uz tehniskajiem aspektiem, nevis uz digitālās drošības risku pārvaldību attiecībā uz ekonomiskajām un sociālajām aktivitātēm, kuru pamatā ir IKT izmantošana.

Tomēr nav vispārpieņemtas terminoloģijas, kas aptvertu digitālās drošības dažādās šķautnes jebkurā kontekstā. Termini dažādās valstīs atšķiras un atspoguļo dažādu valstu kultūru un vēsturi: nav "pareizas" vai "nepareizas" terminoloģijas. 2015. gadā ESAO valstis deva priekšroku terminam "digitāls", nevis "kiber-", jo pēdējais no šiem bieži asociējās ar tādām koncepcijām kā "kiberkarš", "kiberaizsardzība" vai "kiberietekme". Turklāt termins "kiber-" netiek lietots ekonomikas aprindās, kas parasti vairāk izmanto digitālo semantiku: digitālā ekonomika, digitālā transformācija, digitalizācija utt. Vārds "digitāls" sekmē "digitālās drošības" kā ekonomikas jautājuma atzīšanu no politikas veidotāju un uzņēmumu vadītāju puses. "Informācijas drošība" tika atstāta malā kā tehniskās pārvaldības termins, kas primāri atspoguļo tehniskās kopienas viedokli (piemēram, ISO/IEC 27000 "Informācijas drošības pārvaldes sistēmas" standartus). Turklāt termins "Informācijas drošība" ir neskaidrs starptautiskajā kontekstā, jo tam ir atšķirīgs tvērums tādās valstīs kā Ķīnas Tautas Republikā un Krievijas Federācijā, kuras tajā iekļauj arī pret dezinformāciju, ietekmi un informācijas manipulācijām vērstu politiku. Dezinformācija, ietekme un kaitīga satura izplatīšana ir svarīgi jautājumi, ko saasina digitālā transformācija. Tie dažkārt var pārklāties ar digitālo drošību, piemēram, ja digitālās drošības uzbrukumus izmanto, lai mainītu datu integritāti, manipulējot ar sabiedrisko viedokli, vai novērstu piekļuvi valdības pakalpojumiem. Tomēr tie atšķiras no PIK pārkāpumu ekonomisko un sociālo seku pārvaldības, jo ietver atšķirīgus politikas instrumentus un juridiskus apsvērumus saistībā ar runas brīvību un plašsaziņas līdzekļu regulējumu.

Papildus semantikai kopienām, kuras pievēršas katrai digitālās drošības dimensijai (skatiet 5.3. attēls), bieži ir atšķirīgas kultūras un konteksti, un to mērķi var dažkārt saplūst, pārklāties vai konkurēt atkarībā no konteksta un konkrētā jautājuma. Kriptogrāfijas politika (ESAO, 1998. gads) ir tipisks piemērs par konkurējošiem mērķiem, kad uzņēmumi, organizācijas un patērētāji sekmē neregulētu kriptogrāfijas izmantošanu, lai veicinātu uzticamību un atbalstītu e-komerciju, digitālās valdības un inovācijas tiešsaistē, kamēr tiesībaizsardzības un informācijas aģentūras atbalsta regulējumu, kas atvieglo piekļuvi šifrētajiem datiem, lai cīnītos pret kriminālnoziedzniekiem un terorismu.

5.3. attēls. "Kiberdrošības" četras dimensijas

Latvijas politikas dokumentos jēdzieni "kiberdrošība", "IT drošība" un "informācijas drošība" šķietami norāda uz kādu no šīm definīcijām (atkarībā no konteksta):

- tehnisko līdzekļu, piemēram, tīklu, IKT un datu aizsardzība (5.3. attēls aspekts "Tehnoloģija");
- ar tādas IKT izmantošanas saistīto risku pārvaldība, kas nekoncentrējas uz ekonomiskām un sociālām aktivitātēm, bet tā vietā aizskar jautājumus, kas attiecas uz nacionālo drošību ietekmi uz stratēģijām demokrātiskās vēlēšanās un kaitīgu saturu (5.3. attēls aspekti "Nacionālā drošība" un "Tiesībaizsardzība").

Piemēram, *Latvijas kiberdrošības stratēģijā (2014-2018)* kiberdrošība ir definēta kā "instrumentu, politikas, drošības konceptu un vadlīniju, risku vadības, rīcības, apmācības, pieredzes un tehnoloģiju kopums, kuru var izmantot elektroniskās vides, tās organizācijas un lietotāju aktīvu aizsardzībai". Savukārt *Latvijas kiberdrošības stratēģija (2019-2022)* balstās uz to, ka "Kiberdrošības politikas vīzija ir droša, atvērta, brīva un uzticama kibertelpa, kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana un sniegšana un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē". Turklāt šajā dokumentā tiek atzīts, ka "Latvijai ir jāizmanto digitālās vides priekšrocības, lai nodrošinātu ekonomisko un sociālo labklājību, vienlaikus samazinot kiberdrošības risku vispārējo līmeni, nevajadzīgi neierobežojot tehnoloģiju, sakaru un datu plūsmu".

Šīs izmaiņas ir pozitīva attīstība, kur Latvijas valdība šobrīd atzīst, ka digitālā drošība ietekmē citus digitālās ekonomikas aspektus (atvērtību, brīvību), kas liecina, ka ir pamatota uz risku balstīta pieeja un ka ir nepieciešami kompromisi. Stratēģija atzīst arī kiberfizisko sistēmu parādīšanos, kas virtuālo (jeb "kibertelpas") / fizisko divdalījumu padara mazāk nozīmīgu, jo arvien vairāk ekonomisko un sociālo aktivitāšu "kļūst digitālas". Kopumā šī semantiskā evolūcija atspoguļo dziļākas izmaiņas veidā, kā Latvija uztver digitālo drošību, atzīstot to kā digitālās transformācijas instrumentu, nevis autonomu elementu.

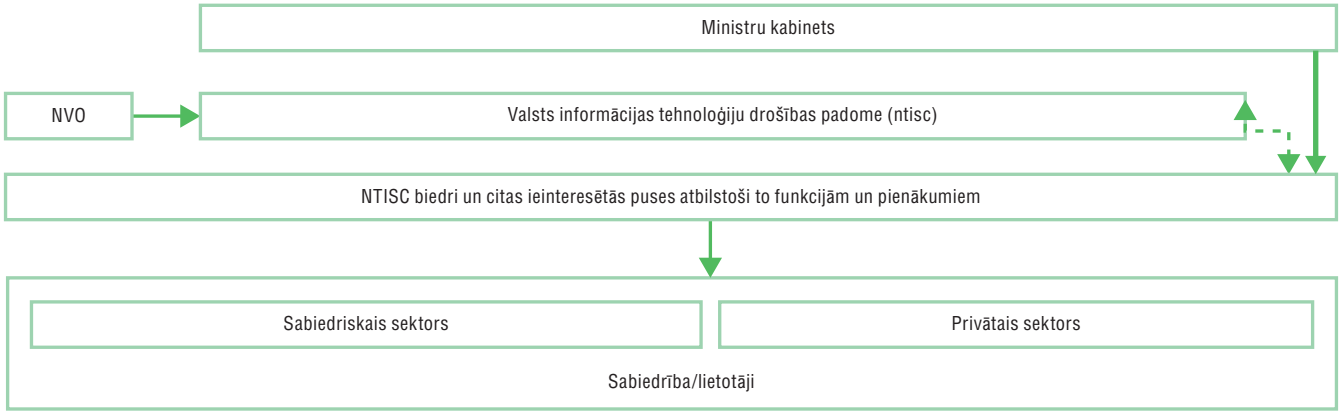
Pārvaldība

Digitālās drošības politikas vispārējā pārvaldības struktūra Latvijā

Kopš 2013. gada AM ir koordinējusi digitālās drošības politikas attīstību un īstenošanu, iesaistot daudzas Latvijas valdības ministrijas.[3]

Lai koordinētu ar informācijas tehnoloģiju drošību saistītās politikas izstrādi, kā arī attiecīgu uzdevumu un pasākumu plānošanu un īstenošanu, tika izveidota NITDP. NITDP vada AM, parasti valsts sekretāra līmenī. Tā tiekas vismaz vienreiz četros mēnešos un sapulcina pārstāvjus no dažādām institūcijām, tostarp ministrijām un tiesībsargājošajām institūcijām. Citas ieinteresētās puses ir uzaicinātas dalībai uz ad-hoc bāzes,[4] jo NITDP galvenā funkcija ir koordinēt ar informācijas tehnoloģiju drošību saistītās politikas izstrādi. 5.4. attēls ir vizuāli attēlota digitālās drošības valdības struktūra Latvijā (2019. g.).

5.4. attēls. Digitālās drošības vadības struktūra Latvijā (2019.-2022. g.)



Piezīme: NVO = Nevalstiska organizācija.

Avots: AM (2019), *Latvijas kiberdrošības stratēģija (2019.-2022. g.)* [Cyber Security Strategy of Latvia (2019-2022)], *https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf*.

NITDP nav piešķirts atsevišķs budžets, un administratīvo atbalstu nodrošina AM. AM Nacionālās kiberdrošības politikas koordinācijas nodaļa (NKPKN) nodrošina NITDP atbalstu sekretariāta vārdā. Turklāt AM nodrošina Elektroniskās identifikācijas uzraudzības komitejas darbu.

Ārlietu ministrija (ĀM) ko-ordinē ar digitālo drošību saistīto starptautisko sadarbību ar AM iesaistīšanos digitālās drošības jautājumos, kas ir saistīti ar NATO un ES.

Vides aizsardzības un reģionālās attīstības ministrija (VARAM) ir atbildīga par valsts informācijas sistēmām un koordinē sabiedrisko pakalpojumu digitalizāciju. Valsts reģionālās attīstības aģentūra (VRAA) nodrošina valsts IKT koplietošanas risinājumu darbību un izstrādi, ieskaitot valsts eID un digitālā paraksta platformu, valsts eIDAS vārteju, publisko iepirkumu sistēmu un sabiedrisko pakalpojumu portālu "Latvija.lv", kā arī e-adreses oficiālo risinājumu. Turklāt VARAM vada arī digitālās un informācijas sabiedrības politikas vispārējo attīstību, un VARAM valsts sekretāra vietnieks ir NITDP priekšsēdētāja vietnieks.

Iekšlietu ministrija (IeM) un Valsts policija (VP) īsteno tiesību aktu ieviešanas politikas, lai apkarotu kibernoziegumus.

CERT.LV nodrošina atbalstu valsts iestādēm, atklājot digitālās drošības incidentus. CERT.LV atbild arī par reaģēšanu digitālās drošības incidentu gadījumā, iekļaujot krīzes pārvaldību. Tā uzrauga un analizē attīstību digitālās drošības jomā, veido statistiku par incidentiem un reaģē uz tiem, kā arī koordinē to novēršanu, veic izpēti, organizē izglītības pasākumus un apmācību, kā arī uzrauga likumā norādīto saistību ieviešanu attiecībā uz Informācijas tehnoloģiju drošību. Papildus savai primārajai misijai, atbalstīt publiskā sektora institūcijas, CERT.LV atbalsta arī uzņēmējus un fiziskas personas. CERT.LV budžets pēdējo gadu laikā ir ievērojami pieaudzis no apmēram 120 000 EUR 2011. gadā līdz 882 000 EUR 2015. gadā un 1 328 000 EUR 2019. gadā, atspoguļojot Latvijas valdības apņemšanos paaugstināt digitālās drošības spējas.

Satversmes aizsardzības birojs (SAB), valsts izlūkošanas un drošības aģentūra uzrauga kritisko infrastruktūru aizsardzību. Turklāt SAB aktīvi iesaistās sadarbības iniciatīvās starp Baltijas valstīm un Amerikas Savienotajām Valstīm, nodrošinot kompetenci un vadību enerģētikas kritiskās infrastruktūras jomā. SAB un CERT.LV strādā kopā, lai pārbaudītu informācijas tehnoloģiju kritisko infrastruktūru noturību un sniegtu norādes šādu infrastruktūru publiskajiem un privātajiem operatoriem.

Labklājības ministrija (LM) īsteno sociālo politiku, kā arī politiku bērnu aizsardzībai tiešsaistē.

Valsts akciju sabiedrība Latvijas Valsts radio un televīzijas centrs (LVRTC) ir vienīgais kvalificētu uzticamības pakalpojumu (piemēram, elektronisko parakstu, zīmogu un identifikācijas formu) nodrošinātājs.

Nacionālie bruņotie spēki (NBS) un Zemessardzes Kiberaizsardzības vienība (ZS KbrAV) nodrošina atbalstu krīžu gadījumos. Kaut arī NBS galvenais uzdevums ir militāro informācijas tehnoloģiju un sakaru sistēmu un tīklu attīstīšana un nostiprināšana, NBS ir būtiska nozīme arī vispārējo kiberaizsardzības spēju uzlabošanā.

Ceļā uz "visu valdības struktūru" un vairāku ieinteresēto pušu pieeju

Lai digitālās drošības stratēģijas būtu sekmīgas, nepieciešama efektīva iesaistīšanās ar visiem attiecīgajiem dalībniekiem visā valdībā *un* plašākā vairāku ieinteresēto pušu kopienā (piemēram, pētnieki, uzņēmumi un pilsoniskā sabiedrība). Kaut arī daudzaās stratēģijaās tiek atzīts šīs divvirzienu pieejas svarīgums ("visu valdības struktūru pieejas" koordinācija un "vairāku ieinteresēto pušu" iesaistīšana), efektīva ieviešana var izrādīties problemātiska, jo tai ir nepieciešami atbilstoši resursi, uzticamība un reizēm pārmaiņas kultūrā.

Pašreizējā vadības struktūra Latvijas digitālās drošības politikā, kas aprakstīta iepriekšējā sadaļā, daļēji atbilst "visu valdības struktūru" pieejai, un to var raksturot kā "daļēji centralizētu" (AM, 2014. gads). Šīs struktūras izveide un ieviešana 2012.-2014. gadā iezīmēja pagrieziena punktu Latvijas pieejā: digitālā drošība vairs netika uzskatīta tikai par tīkliem atbildīgo institūciju tehnisku problēmu (Satiksmes ministrijai), bet kļuva par publiskās politikas lietu, kurai ir nepieciešama visu valdības struktūru iesaistīšanās.

Līdz šim šajā struktūrā Latvijas pieeju ir veidojusi valsts drošības aspektu uzsvēršana, un tas ir palīdzējis digitālās drošības risku pacelt nozīmīga politikas jautājuma līmenī un līdzsvarot resursus valdībā. Piemēram, NITDP vada AM valsts sekretārs, kas savukārt uzrauga CERT.LV.

Kaut arī šī pieeja ir sniegusi nenoliedzamus ieguvumus, tai ir arī daži trūkumi. Ja pieeja digitālajai drošībai veidojas galvenokārt caur nacionālās drošības ietvaru, tas var ierobežot ieinteresēto pušu iespēju pilnībā iesaistīties un identificēt sevi ar digitālās drošības risku, jo nacionālā drošība tiek bieži saistīta ar valsts lietām. Piemēram, industrijas un pilsoniskās sabiedrības ieinteresētās puses parasti tiek aicinātas uz NITDP sanāksmēm uz *ad-hoc* pamata un nepiedalās stratēģijas izstrādē un ieviešanā. Kaut arī ieinteresētās puses ir aicinātas piedalīties stratēģijas izstrādes procesā ar publiskiem komentāriem, reālā dalība parasti ir zemā līmenī. Šāda ierobežota iesaistīšanās var rasties ilgtermiņa, uz uzticību balstītas un ilgtspējīgas vairāku ieinteresēto pušu partnerību trūkuma dēļ, kas ir būtiski jēgpilnas un efektīvas dalības nodrošināšanai (ESAO, 2015. gads). Tas var būt arī nepietiekami koordinētas un strukturētas vairāku ieinteresēto pušu kopienas rezultāts. Uzmanība uz nacionālo drošību var arī ierobežot citu valdības institūciju pieeju digitālajai drošībai kā ekonomiskai iespējai (piemēram, pētījumiem, inovācijām, kvalificētai uzņēmējdarbībai). Ja sadarbība ar ministrijām, kuras ir atbildīgas par ekonomikas attīstību un nozaru koordināciju, un to iesaistīšanās ir nepietiekama, pastāv arī risks, ka šīs ministrijas neattīstīs nepieciešamās tehniskās prasmes un izpratni par saistītajām problēmām, lai piedalītos digitālās drošības stratēģijas izstrādē un ieviešanā.

Kopsavilkumā var teikt, ka pašreizējā pieeja Latvijā (5.5. attēls) ir strukturēta ap nacionālās drošības ietvaru (NITDP), kas balstās uz spēcīga tehniskā pamata (CERT.LV). Tomēr ekonomiskā un sociālā dimensija ir šķietami mazāk iesaistīta, un politika parasti tiek īstenota caur tehnisku (izmantojot CERT.LV) vai nacionālās drošības objektīvu.

Vairākums valdību ir cīnījušās par atbilstīgas pārvaldības struktūras izveidošanu digitālajai drošībai, jo ir grūti sasniegt pareizo līdzsvaru starp ekonomikas un sociālajiem jautājumiem, nacionālo drošību, tiesībaizsardzību un tehniskajiem aspektiem (5.3. attēls). Nav modeļa, kas atbilstu visiem gadījumiem, un pārvaldības struktūras un koordinācijas mehānismi dažādās ESAO valstīs ievērojami atšķiras, atspoguļojot valstu vēsturi, ģeopolitisko kontekstu, vadības stilu un briedumu šajā jomā.

Daudzās ESAO valstīs digitālās drošības pārvaldības ietvara veidošanas process bieži sākas ar nacionālo drošību, kibernoziegumu (piemēram, tiesību aktu par kibernoziegumiem pieņemšanu) vai tehnoloģisku dimensiju, koncentrējoties uz pieaugošajām tehniskās reakcijas iespējām, piemēram, veidojot Informācijas tehnoloģiju drošības incidentu novēršanas institūciju (CERT). Pēc tam process pakāpeniski izvēršas, iekļaujot ekonomisko un sociālo labklājību. Tomēr dažas valstis ir nonākušas pie vienošanās par to, ka uz nacionālo drošību orientētās aģentūras nav vislabākajā pozīcijā, lai izstrādātu un ieviestu ekonomikas un sociālo politiku, to pamatojot ar argumentu, ka tā nav viņu galvenā misija; šīm aģentūrām ir bieži vērojams caurskatāmības un vairāku ieinteresēto pušu iesaistīšanās trūkums, kas ir svarīgs, lai veidotu ilgtspējīgas partnerības uz uzticamības pamata.

5.5. attēls. Digitālās drošības politika Latvijā

Piezīme: Šajā attēlā ir parādīts līmenis, kādā valdība pievērš uzmanību trim no četriem digitālās drošības struktūras komponentiem (kā redzams 5.3. attēls). Latvijas pašreizējā struktūrā iekļautā krimināllikuma īstenošana nav parādīta, jo tā neietilpst šī pārskata ietvaros.

Lai visiem kiberdrošības aspektiem pievērstos nevis fragmentēti, bet holistiski, digitālās drošības stratēģijas ir jāatbalsta augstākajā valdības līmenī (piemēram, valsts vadītājam vai valdības vadītājam) un jāizveido jauni pārvaldības un koordinācijas mehānismi, lai nodrošinātu līdzsvaru starp papildu un reizēm konkurējošiem mērķiem dažādās dimensijās (ESAO, 2015. gads). Tomēr katrai valstij ir jāpieņem savai kultūrai un valdības stilam pielāgots pārvaldības modelis.

Piemēram, Austrālijā, Japānā un Apvienotajā Karalistē politikas koordinācija ir uzticēta premjerministram caur Ministru kabineta biroju. Francija ir izveidojusi nacionālo koordinācijas aģentūru iepriekš pastāvošajā koordinācijas organizācijā, ko pārvalda premjerministrs (ANSSI). Amerikas Savienotās Valstis ir izveidojušas "Kiberdrošības un infrastruktūras drošības aģentūru" (CISA) Valsts drošības departamentā. Kanādā, Vācijā un Nīderlandē galvenā atbildība par digitālo drošību ir uzticēta esošai ministrijai (attiecīgi Sabiedriskās drošības, Iekšlietu, Drošības un Tieslietu ministrijām). Izraēla ir izveidojusi valsts aģentūru, kas atskaitās tieši premjerministram (INCD).

Dānijā atbildība par digitālās drošības stratēģijas vispārējo koordināciju ir sadalīta starp Digitalizācijas aģentūru (FM ietvaros) un Kiberdrošības centru (AM). Aģentūra ir atbildīga par digitālo drošību sabiedriskajā sektorā, kā arī par daudzām uz pilsoņiem vērstām iniciatīvām. Centrs konsultē valsts iestādes un privātuzņēmumus, kas atbalsta kritiskās aktivitātes. Aģentūra vadīja darba grupu, kura izstrādāja digitālās drošības stratēģiju.

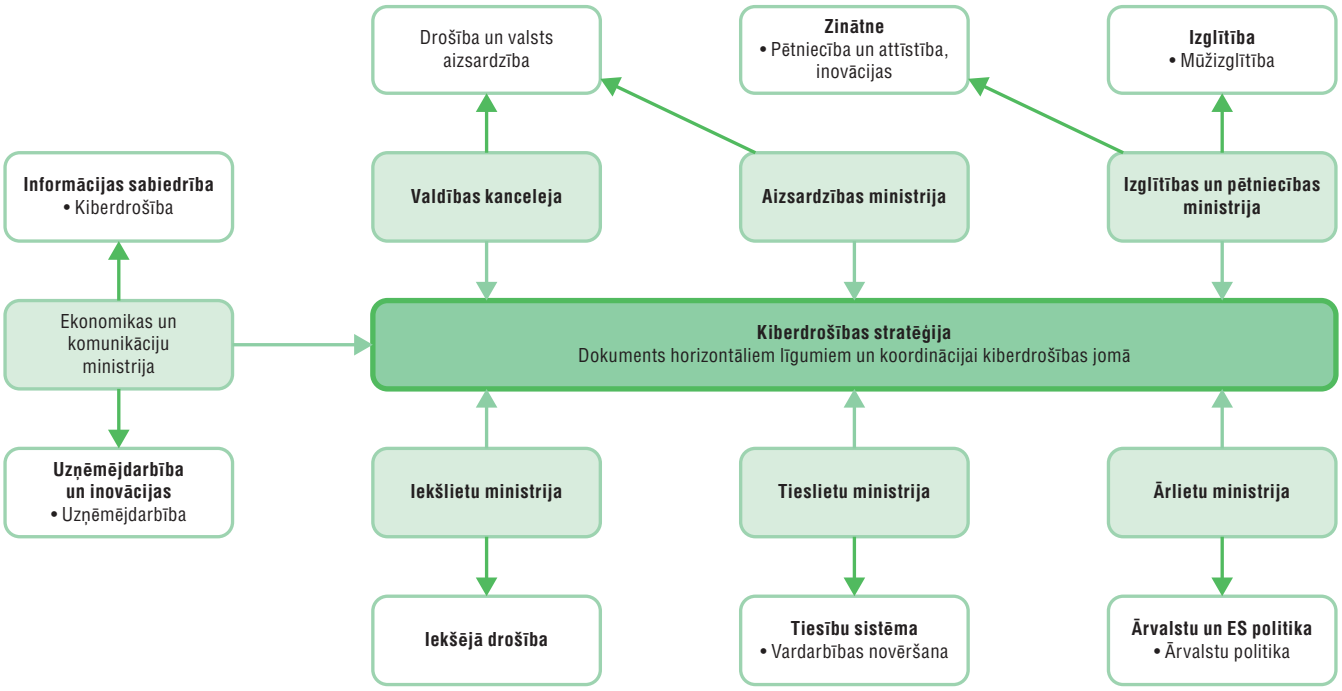
Igaunijā Ekonomikas lietu ministrija ir atbildīga par digitālās drošības politikas izstrādes un ieviešanas koordinēšanu (5.6. attēls). Arī citas ministrijas (piemēram, Aizsardzības, Izglītības un pētniecības, Iekšlietu, Tieslietu) ir pilnībā iesaistījušās savā kompetences jomā.

Visos šajos gadījumos pastāv arī dažādas vienošanās par to, kā konkrēti jāveic vairāku ieinteresēto pušu koordinācija un kur ir valdības operacionālais potenciāls. Tas aptver diapazonu no politikas koordinācijas aģentūras (Francija, Izraēla) līdz pievienotajai apakšstruktūrai vai ziņojumiem ministrijai (Vācija, Nīderlande) vai atsevišķai struktūrai (AK Nacionālais kiberdrošības centrs). Turklāt politikas, kas sekmē kritisko aktivitāšu un infrastruktūras digitālo drošību, rada nepieciešamību iesaistīt nozaru regulatorus (piemēram, telekomunikāciju, veselības, finanšu, transporta un enerģētikas nozarēs) , lai nodrošinātu to, ka saistītajā digitālās drošības regulējumā tiek ņemti vērā esošie tirgus un normatīvie ierobežojumi.

Daudzās ESAO valstīs ir sāktas uz ekonomiku orientētas un vairāku ieinteresēto pušu virzītas iniciatīvas. Valdības ir atbalstījušas nozaru specifiskās partnerības, kuru mērķis ir informācijas un labākās pieredzes apmaiņa digitālās drošības izaicinājumu jomā, piemēram, caur Informācijas apmaiņas un analīzes centriem (*ISAC*). Kā vēl vienu labu pieredzi var minēt partnerības uzsākšanu ar interneta pakalpojumu sniedzējiem (ISP) un citām ieinteresētajām pusēm, lai atklātu un iztīrītu inficētās savienotās ierīces. Piemēram, Nīderlandes valdība ir veikusi darbības, lai uzraudzītu un uzlabotu savienoto ierīču digitālo drošību, ar publiskas-privātas partnerības starpniecību, kas iekļauj ISP, Ekonomikas lietu ministriju

un Delftas universitāti. Šīs iniciatīvas mērķis ir informācijas apmaiņa starp ražotājiem/pārdevējiem un gala lietotājiem, lai produktu izplatītājus mudinātu apsvērt ietekmēto produktu izņemšanu no pārdošanas un stimulētu patērētājus uzstādīt drošības atjauninājumus vai deaktivizēt produktus kritiskas ievainojamības atklāšanas gadījumā.

5.6. attēls. Digitālās drošības pārvaldības struktūra Igaunijā



Avots: ELKM (2019), *Cyber Security Strategy of Estonia (2019-2022)*, *www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

Latvijā pašreizējā vadības struktūra norāda uz vēlmi veidot sasaisti ar vairāku ieinteresēto pušu kopienu, kaut lai gan varētu uzlabot līdzekļus to efektīvai līdzdalībai. Lai arī NITDP ir aprakstīta *Kiberdrošības stratēģijā* kā "centrālā nacionālā institūcija valsts un privātā sektora informācijas apmaiņai un sadarbībai", šķiet, ka nevalstiskās ieinteresētās grupas (gan no privātā sektora, gan arī no pilsoniskās sabiedrības) tiek uzaicinātas dalībai tikai *ad-hoc* gadījumos. Tās nesniedz pilnu ieguldījumu stratēģijas izstrādē un ieviešanā, kaut arī tiek aicinātas to darīt publisko komentāru. Tas var norādīt uz vairāku ieinteresēto pušu kopienas nepietiekamu strukturizāciju pienācīgai dalībai digitālās drošības politikas veidošanā. Turklāt NITDP tiekas tikai ik reizi četros mēnešos un galvenokārt ir kā kanāls jautājumu pārrunāšanai valdībā, nevis elastīgs un uzņēmējdarbībai vai pilsoniskajai sabiedrībai draudzīgs forums. Tas arī daļēji var izskaidrot, kāpēc uzņēmumu vadītāji Latvijā ne vienmēr uzskata digitālo drošību par savu prioritāti, jo valdības struktūrā tā galvenokārt ir pasniegta kā nacionālās drošības jautājums.

Visbeidzot dažādos politiku dokumentos NITDP ir raksturota kā "konsultējoša" organizācija, "koordinācijas" platforma, varas iestāde, kas uzrauga kiberdrošības stratēģijas "īstenošanu", un organizācija, kas atbild par digitālās drošības politikas īstenošanas novērtēšanu. Pārvaldības struktūra skaidri neatdala digitālās drošības stratēģijas plānošanas, konsultāciju, īstenošanas un novērtēšanas funkcijas, jo šķiet, ka NITDP AM vadībā veic visas šīs funkcijas. Tas var izraisīt ierobežotu ārējo uzraudzību un vērtīgu atsauksmju trūkumu, kas laika gaitā kavētu stratēģijas uzlabošanu.

Tiesiskais regulējums

Digitālās drošības galvenais tiesiskais regulējums ir Informācijas tehnoloģiju drošības likums, kas tika pieņemts 2010. gadā un kopš tā laika ir vairākkārt grozīts. Likums attiecas uz valsts un pašvaldību institūcijām, informācijas tehnoloģiju kritiskās infrastruktūras (ITKI) operatoriem, svarīgāko pakalpojumu operatoriem un digitālo pakalpojumu nodrošinātājiem, kā arī elektronisko sakaru nodrošinātājiem. Tajā ir norādītas svarīgākās organizācijas un to pienākumi digitālās drošības jomā (piemēram, NITDP un CERT.LV).

Valsts informācijas sistēmu likums, kas tika pieņemts 2002. gadā un grozīts 2014. gadā, attiecas uz tīkliem, kurus izmanto un uztur valsts iestādes. Viens no tā nosacījumiem ir vienotās procedūras, pēc kurām tiek izveidotas, reģistrētas, uzturētas, izmantotas, reorganizētas vai atmestas nacionālās informācijas sistēmas, un tas nosaka to digitālās drošības pārvaldību.

Citi svarīgi normatīvie akti:

- Ministru kabineta noteikumi Nr. 422: "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" (2015. gads, atjaunināti 2017. un 2019. gadā), kuru mērķis ir saskaņoti un augstāki drošības līmeņi IKT sistēmās valsts un pašvaldību iestādēs.
- Ministru kabineta noteikumi Nr. 764: "Valsts informācijas sistēmu vispārējās tehniskās prasības" (2005. gads, jaunākie grozījumi 2009. gadā)
- Ministru kabineta noteikumi Nr. 496: "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība" (2010. gads, pēc tam grozīti)
- Ministru kabineta noteikumi Nr. 100: "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība" (2011. gads).

Latvijas institūcijas acīmredzot nav vēl veikušas esošo digitālās drošības jomas likumu un noteikumu un to īstenošanas pilnīgu auditu.

Jaunākās iniciatīvas

Informācijas sabiedrības attīstības pamatnostādnes (2014.-2020. g.)

Informācijas sabiedrības attīstības pamatnostādnes (2014.-2020. g.) ir kā Latvijas nacionālā digitālā stratēģija. To galvenais mērķis: "nodrošinot iespēju ikvienam izmantot IKT sniegtās iespējas, veidot uz zināšanām balstītu ekonomiku un uzlabot kopējo dzīves kvalitāti, sniedzot ieguldījumu publiskās pārvaldes efektivitātes, valsts konkurētspējas, ekonomiskās izaugsmes paaugstināšanā un darbavietu radīšanā". Tomēr pamatnostādnes galvenokārt koncentrējas uz IKT piekļuves un izmantošanas uzlabojumiem, kā arī e-valdības pakalpojumiem, piemēram, tiešsaistes identitāti un valsts IKT.

Pamatnostādņu darbības virziens 5.7 ir saistīts ar "Uzticēšanos un drošību", bet īpaši (sadaļā 5.7.1) ar "IKT drošību", konkrēti uzsverot iespēju veidošanu.

Kopumā Pamatnostādnes šķiet ierobežotas attiecībā uz sasaisti ar citiem digitālās drošības politikai nozīmīgiem politikas dokumentiem (piemēram, Kiberdrošības stratēģiju), norādot, ka digitālā drošība Latvijā tiek galvenokārt uzskatīta par nacionālās drošības jautājumu. Šī uztvere nav raksturīga tikai Latvijai. Daudzās ESAO valstīs dažādi digitālo stratēģiju pamatelementi darbojas izkaisīti ar nelielu koordināciju vertikālajos laukos.

Kiberdrošības stratēģija

Galvenā digitālās drošības politikas iniciatīva Latvijā ir Latvijas kiberdrošības stratēģija (2019.-2022. gadam), kas aizstāj Latvijas kiberdrošības stratēģiju (2014-2018. gadam).

Iepriekšējās stratēģijas visaptverošais mērķis bija sasniegt "drošu un uzticamu kibertelpu, kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana". Šī stratēģija attiecās uz valdību, ieskaitot valsts un pašvaldību administrācijas, privāto sektoru un fiziskas personas. Tās pamatā bija četri principi (attīstība, sadarbība, atbildība un atvērtība) un pieci prioritāri rīcības virzieni:

- kiberdrošības pārvaldība un resursi;
- tiesiskums kibertelpā un kibernoziedzības mazināšana;
- gatavība un rīcībspēja krīzes situācijās;
- sabiedrības izpratne, izglītība un pētniecība;
- starptautiskā sadarbība.

Jaunā stratēģija (2019.-2022. gadam), šķiet, nedaudz atšķiras, atspoguļojot dažu pēdējo gadu laikā gūtās mācības. Kaut arī tās vīzija sākas tādā pašā veidā (sasniedzamais mērķis ir "droša, atvērta, brīva un uzticama kibertelpa, kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana un sniegšana"), tiek ņemta vērā arī nepieciešamība, ka "indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē". Tā ir pozitīva attīstība, kas atzīst konkurējošos mērķus, kuri bieži ir dienaskārtībā, izstrādājot digitālās drošības politiku (piemēram, privātums un valsts drošība). Jaunajā stratēģijā tiek atzīta arī kiberfizisko sistēmu attīstība un nepieciešamība virzīties tālāk par virtuāli-fizisko divdalījumu.

Kas attiecas uz prioritārajiem rīcības virzieniem, tad pēdējie četri būtībā ir tādi paši, izņemot "rīcībspēja krīzes situācijā", kas ir aizstāta ar šo: "IKT izturētspēja, sabiedrībai kritiski svarīgu IKT un pakalpojumu nodrošināšanas stiprināšana". Pirmais rīcības virziens no "pārvaldības" ir izaudzis līdz šim: "kiberdrošības veicināšana, digitālās drošības risku mazināšana". Tas šķietami norāda, ka digitālās drošības pārvaldības struktūras veidošanas process Latvijā, kas bija sākotnējās stratēģijas pirmais mērķis, tagad ir vismaz daļēji sasniegts, un izaicinājums Latvijas varas iestādēm izmantot šo esošo struktūru, lai visas ieinteresētās puses pilnībā iesaistītu digitālās drošības riska pārvaldībā. Tas ir pozitīvs solis un norāda, ka Latvijas varas iestādes ir atzinušas nepieciešamību iziet ārpus "visu valdības struktūru" pieejas uz "visaptverošas sabiedrības" pieeju, kas it īpaši iekļauj ekonomiskajā un sociālajā labklājībā iesaistītos dalībniekus un kopienas. Šīs izmaiņas satur arī risku pārvaldības pieejas integrāciju. Faktiski jaunā stratēģija atzīst, ka IKT "nav absolūti drošas un var tikt pakļautas uzbrukumiem. Uzbrukuma draudus IKT nevar pilnībā novērst, bet uzbrukuma risku var ievērojami mazināt, lai netraucētu sabiedrības ekonomisko un sociālo attīstību, nenodarītu zaudējumus ekonomikai un gūtu labumu no IKT gan valsts pārvaldē, gan privātajā sektorā".

Tomēr šīs jaunās Kiberdrošības stratēģijas pozitīvās izmaiņas joprojām ir jāievieš praksē. Latvijas valdībai viens no izaicinājumiem būs iesaistīt visas attiecīgās ieinteresētās puses iesaistīšana un pievērsties digitālās drošības riskiem visā ekonomikā, iesaistot vadošās institūcijas, kuru galvenā auditorija ir vai nu IT komandas (CERT.LV), vai militāristi (AM). Lai gūtu panākumus, var būt nepieciešamas kultūras pārmaiņas, kā arī dziļāka iesaistīšanās un/vai atbalsts no citu institūciju, piemēram, VARAM, Ekonomikas ministrijas (EM) vai premjerministra, puses, kuru darbības joma pēc būtībasir vairāk horizontāla.

Citas iniciatīvas

Latvijas valdība ir organizējusi citas iniciatīvas digitālās drošības jomā, piemēram, "drošāka interneta dienu", "e-prasmju nedēļu" un "kiberdrošības mēnesi", kura mērķis ir uzlabot informētību un dalīties labajā praksē. Turklāt digitālās drošības krīzes vingrinājumi tiek veikti ar valsts iestādēm CERT.LV un AM vadībā atbilstoši stratēģijai.

CERT.LV ir rādījusi piemēru, publicējot savu ievainojamību atklāšanas politiku. CERT.LV pieņem ziņojumus par ievainojamību saviem resursiem, kā arī jebkurai citai organizācijai Latvijā. Pēdējā gadījumā CERT.LV rīkojas kā koordinators iesaistīto pušu starpā (piemēram, starp drošības pētniekiem un organizācijām).

CERT.LV nodrošina arī apmācību un informāciju par digitālās drošības riskiem IT profesionāļiem un sabiedrībai. Piemēram, tas publicē regulāru informāciju par tiešsaistes vīrusiem un apdraudējumiem caur savu IT drošības portālu *Esi Drošs*. Portālā katra apmeklētāja IP adrese tiek pārbaudīta, salīdzinot ar inficēto IP adrešu datubāzi, un apmeklētāji saņem informāciju par jebkuru ievainojamību vai infekciju saskaņā ar CERT.LV datiem. CERT.LV ir iesaistīts arī specifisku profesionālo grupu izglītošanā, ieskaitot par IT drošību atbildīgās amatpersonas, darbiniekus, pārvaldniekus, studentus un skolēnus. 2012. gadā CERT.LV sāka iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs (ISP)", piešķirot kvalitātes marķējumu ISP, kuri sadarbojas ar komandu. Šāda sadarbība iekļauj incidentu informācijas nodrošināšanu gala lietotājiem, sadarbību ar Latvijas Interneta asociācijas Drošāka interneta centru, lai izņemtu no interneta nelikumīgu materiālu, un interneta satura filtra nodrošināšanu, ko pēc pieprasījuma var uzstādīt bez maksas. Pašlaik Latvijā ir 13 "atbildīgi ISP", kas aptver aptuveni 77 % no Latvijas interneta piekļuves tirgus.

Turklāt CERT.LV organizē izglītības pasākumus, piemēram, "Kiberšahs", un citas zināšanu apmaiņas aktivitātes. Šie pasākumi piesaista privātā sektora pārstāvjus digitālās drošības vingrinājumiem (piemēram un Locked Shields), kur viņiem ir jāveic dažādi uzdevumi kopā ar kolēģiem no publiskā sektora.

Zemessardzes Kiberaizsardzības vienība (ZS KbrAV) apvieno ekspertus, kuri ir ieinteresēti regulāras sadarbības attīstībā digitālās drošības jautājumos, uzlabojot kompetenci un zināšanas valsts un starptautiskā līmenī, kā arī piedaloties un organizējot apmācību digitālās drošības uzbrukumu novēršanai un sniedzot atbalstu sabiedriskajām organizācijām (ja tas ir atbilstoši). ZS KbrAV galvenais mērķis ir sniegt atbalstu informācijas tehnoloģiju drošības incidentu reaģēšanas vienībām, lai novērstu digitālās drošības incidentus un reaģētu uz tiem, kā arī mazinātu to sekas.

AM sadarbojas ar LIKTA (Latvijas Informācijas un komunikācijas tehnoloģijas asociācija), kurā ir 160 biedru, lai organizētu, piemēram, gada balvas pasniegšanu par "Labāko kiberdrošības iniciatīvu".

Latvijas Drošības un aizsardzības industriju federācija (DAIF Latvija) pārstāv Latvijas drošības un aizsardzības nozari. Valsts līmenī organizācija aktīvi sadarbojas ar Aizsardzības ministriju, Iekšlietu ministriju, Ārlietu ministriju, Ekonomikas ministriju un Saeimu. DAIF Latvija ir izveidojusi Latvijas Drošības un aizsardzības klasteri, ko veido mazi un vidēji uzņēmumi un pētniecības iestādes, ES projekta ietvaros.

Starptautiskā sadarbība

Latvija ir izveidojusi ciešu trīspusēju sadarbību ar kaimiņvalstīm Igauniju un Lietuvu. Trīs valstu politiķi regulāri (vismaz divreiz gadā) tiekas, lai paplašinātu esošo koordināciju, veiktu informācijas apmaiņu par jaunākajām digitālās drošības tendencēm un — dažos gadījumos — koordinētu kopējo pozīciju par digitālās drošības jautājumiem starptautiskās diskusijās. Praktiskā līmenī CERT.LV sadarbojas ar Lietuvas un Igaunijas CERT komandām, veicot informācijas apmaiņu par jaunākajiem drošības apdraudējumiem, vīrusiem un citiem riskiem un regulāri tiekoties dažādos forumos. 2015. gadā Igaunijas, Latvijas un Lietuvas Aizsardzības ministrijas oficiāli parakstīja Saprašanās memorandu par sadarbību kiberdrošības jautājumos. Tomēr šķiet, ka Baltijas valstu Ekonomikas lietu ministrijām, pietrūkst sadarbības digitālās drošības jautājumos, kaut arī Igaunijas Ekonomikas lietu ministrija ir digitālās drošības politikas vispārējais koordinators Igaunijā (5.6).

CERT.LV vadītāja bija Eiropas CSIRT foruma (TF-CSIRT) priekšsēdētāja no 2014. līdz 2019. gadam. Šajā amatā viņa atbalstīja Eiropas CSIRT kopienas izaugsmi un attīstību, sekmēja sadarbību digitālās drošības jomā starp akadēmiskajām institūcijām, valdību un sabiedrisko, kā arī sekmīgi pārstāvēja Eiropas CSIRT kopienu dažādos starptautiskos forumos.

Latvija piedalās vairākos starptautiskos apmācības pasākumos un praktiskos vingrinājumos. Kā piemēru var minēt trīs mācības "Cyber Europe", kuras organizē Eiropas Savienības Kiberdrošības aģentūras (ENISA).

Latvija iesaistās arī NATO, ES, EDSO un ANO darbā. Tā ir ratificējusi Eiropas Padomes Konvenciju par kibernoziegumiem un tās Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. Turklāt Latvija aktīvi atbalsta dziļāku sadarbību starp Ziemeļvalstīm-Baltijas valstīm, Poliju un Amerikas Savienotajām Valstīm.

Secinājumi un politikas ieteikumi

Latvijai jāturpina balstīties uz 2015. gada ESAO rekomendāciju par digitālās drošības risku pārvaldību ekonomiskai un sociālai labklājībai

ESAO 2015. gada rekomendācija par OECD digitālās drošības risku iekļauj astoņus principus, kas rezumē "digitālās drošības riska pārvaldības" pieeju (5.1. ielikums), pamatojoties uz izpratni, ka digitālā drošība ir ekonomiska un sociāla prioritāte, kā arī tehnisks vai nacionālās drošības jautājums. Tas nozīmē, ka:

- Digitālās drošības visaptverošs mērķis ir palielināt ekonomisko un sociālo aktivitāšu panākumu iespējamību: digitālajai drošībai ir jābūt labklājības nodrošinātājai, nevis jāaprobežojas ar sevi.
- Organizācijas nevar pilnībā novērst digitālās drošības risku, bet var novērtēt un samazināt riskus līdz pieņemamam līmenim aktuālo ekonomikas un sociālo mērķu kontekstā.
- Digitālās drošības pasākumi sabiedriskās un privātās organizācijās var negatīvi ietekmēt ekonomiskās un sociālās aktivitātes, kuru aizsardzībai tie ir paredzēti. Lai izvairītos no šīs situācijas, sabiedrisko un privāto organizāciju vadītājiem un lēmumu pieņēmējiem ir jāintegrē digitālās drošības risku pārvaldība savos uzņēmējdarbības lēmumu pieņemšanas procesos, nevis jāuztic tehniskajiem speciālistiem.

Organizāciju vadītājiem un lēmumu pieņēmējiem ir tandēmā jāpārvalda ekonomiskās iespējas un drošības riski, kas izriet no digitālo tehnoloģiju izmantošanas.

5.1. ielikums. ESAO rekomendācijas par digitālās drošības risku pārvaldību ekonomiskai un sociālai labklājībai principi

Vispārīgie principi

1. ***Informētība, prasmes un iespēju paplašināšana.*** Visām ieinteresētajām pusēm ir jāizprot digitālās drošības risks un tā pārvaldības veids.
2. ***Atbildība:*** Visām ieinteresētajām pusēm ir jāuzņemas atbildība par digitālās drošības riska pārvaldību.
3. ***Cilvēktiesības un pamatvērtības.*** Visām ieinteresētajām pusēm ir jāpārvalda digitālās drošības risks caurskatāmi, kā arī konsekventi ievērojot cilvēktiesības un pamatvērtības.
4. ***Sadarbība.*** Visām ieinteresētajām pusēm ir jāsadarbojas, tostarp pāri robežām.

Darbības principi

1. ***Risku novērtējums un apstrādes cikls.*** Vadītājiem un lēmumu pieņēmējiem ir jānodrošina digitālās drošības riska izskatīšana uz pastāvīgas risku izvērtēšanas pamata.
2. ***Drošības pasākumi.*** Vadītājiem un lēmumu pieņēmējiem ir jānodrošina, lai drošības pasākumi būtu piemēroti un atbilstoši riskam.
3. ***Inovācijas.*** Vadītājiem un lēmumu pieņēmējiem ir jānodrošina inovāciju izskatīšana.
4. ***Gatavība un nepārtrauktība.*** Vadītājiem un lēmumu pieņēmējiem ir jānodrošina gatavības un nepārtrauktības plāna pieņemšana.

Avots: ESAO (2015. g.), *Digital Security Risk Management for Economic and Social Prosperity*, *www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*.

Latvija ir spērusi nozīmīgus soļus šīs Rekomendācijas īstenošanas virzienā, atzīstot digitālo drošību kā sabiedrības politikas jautājumu, kuram ir nepieciešama vadības kopēja pieeja, *Latvijas kiberdrošības stratēģijā (2014-2018)* un *Informācijas sabiedrības attīstības pamatnostādnēs*. Turklāt Latvijas kiberdrošības stratēģija (2019.-2022. gadam) atzīst risku pārvaldības pieejas svarīgumu un to, ka ir nepieciešami kompromisi, lai ieviestu efektīvu digitālās drošības stratēģiju, ņemot vērā to, ka, lai gan digitālās drošības pasākumu mērķis ir sekmēt uzticamību, tie var arī mazināt uzticību. Faktiski šādi pasākumi var būt pretrunā vai tikt uzskatīti pretrunā ar cilvēktiesībām un pamatvērtībām, it īpaši privātumu un vārda brīvību. Digitālā drošība un cilvēktiesības var pastiprināt vai graut viena otru atkarībā no to pārvaldības. Turklāt, kaut arī digitālās drošības pasākumu mērķis ir aizsargāt ekonomiskās un sociālās aktivitātes, tie var tās arī kavēt, palielinot izmaksas, samazinot veiktspēju un — vissvarīgāk — samazinot digitālās vides atvērtību un dinamismu, kas ir svarīgi, lai realizētu visus digitālās transformācijas ieguvumus.

Latvijas digitālās drošības vadības struktūras un iniciatīvu analīze (sadaļas 0 un 0) akcentēja ESAO rekomendācijas principu lielākās daļas ievērošanu. Tomēr sadarbības, atbildības un inovācijas principu īstenošana joprojām ir nepilnīga. Ja digitālā drošība tiek galvenokārt uztverta kā tehnisks vai valsts drošības jautājums, tad visticamāk tiks ierobežota riska piederība un mijiedarbība starp uzņēmumu vadītājiem un lēmumu pieņēmējiem gan privātajā sektorā, gan pilsoniskajā sabiedrībā, un atbildīgo digitālās drošības institūciju. Turklāt mazāk ticams, ka par nacionālo drošību atbildīgās institūcijas veicinās caurskatāmību un horizontālo sadarbību, kā arī pārvaldīs ar digitālās drošības inovācijām, MVE un jaunajiem uzņēmumiem saistītās programmas.

Vēl svarīgāk ir tas, ka Latvijas pieeja akcentē tehnoloģiju, tiesībaizsardzību un nacionālo drošību, bet mazāk uzmanības pievērš ekonomikas un sociālajām dimensijām (5.3. attēls). Kaut arī *Latvijas kiberdrošības stratēģija (2019.-2022. gadam)* šķietami labāk integrē cilvēktiesības un pamatvērtības, kā arī risku novērtēšanu un darbu ar tiem, ekonomikas un sociālā perspektīva šķiet nepietiekami attīstīta. Tas var ierobežot valdības un organizāciju spēju pienācīgu novērtēt riskus, uzlabot informētību un sniegt iespēju visām ieinteresētajām pusēm uzņemties pienācīgo atbildības daļu. It īpaši varētu attīstīt šādas jomas: programmas labākai ekonomisko faktoru stimulēšanai, lai veiktu pienācīgus drošības

pasākumus (piemēram, sertifikāciju, vairāku ieinteresēto pušu partnerības); nozaru un starpnozaru iniciatīvas digitālās drošības veicināšanai, piemēram, caur informācijas apmaiņas iniciatīvām (ISAC), kā arī programmas, kas ir saistītas ar digitālās drošības inovācijām un sasaista attiecīgās ieinteresētās puses (piemēram, uzņēmējus, pētniekus, uzņēmumus un valdības).

Informācijas sabiedrības attīstības pamatnostādnēs (VARAM, 2014. gads) identificētie šķēršļi digitālās drošības uzlabošanai Latvijā ir aptuveni tādi paši kā tie, kas tika konstatēti 2016. gada termiņa vidusposma pārskatā par pirmās *Kiberdrošības stratēģijas* īstenošanu (AM, 2016. gads). Tie iekļauj cilvēku un finanšu resursu trūkumu institūcijām, kuras ir atbildīgas par digitālo drošību, digitālās drošības prasmju trūkumu Latvijā un ieinteresēto pušu digitālās drošības risku piederības trūkumu, it īpaši augstākajai vadībai, piemēram, lēmumu pieņēmējiem un uzņēmumu vadītājiem. Kamēr digitālā drošība tiek aplūkota un uztverta galvenokārt kā tehnisks un nacionālās drošības jautājums, nevis kā ekonomiskās un sociālās labklājības attīstības faktors, Latvijas varas iestādēm būs grūti palielināt informētību un paplašināt lietotāju un kopienu iespējas. Piemēram, Igaunijā tās kiberstratēģijas pamatprincipi atzīst digitālo drošību kā ekonomiskās izaugsmes veicinātāju un kā pamatvērtības norāda caurskatāmību un atvērtu komunikāciju (Igaunija, 2019. gads).

Latvijai nepieciešams izmantot savas stiprās puses, lai attīstītu digitālās drošības politikas ietvaru

CERT.LV un AM ir kļuvuši par digitālās drošības politikas ietvara galvenajiem dalībniekiem. Tomēr citas institūcijas Latvijā vēl nav ieviesušas līdzīgu saistību līmeni attiecībā uz digitālajai drošībai atvēlētajiem cilvēkresursiem un finanšu resursiem. Tas varētu liegt šīm institūcijām pilnībā iesaistīties Latvijas digitālās drošības stratēģijas izstrādē un īstenošanā.

Lai likvidētu šo plaisu, citām Latvijas institūcijām ir jāattīsta savas iespējas un pieejas digitālajai drošībai. CERT.LV un AM var palīdzēt šādas kapacitātes izveidē, piemēram, ar kopīgiem darbsemināriem, kvalifikācijas celšanas semināriem un pagaidu darbinieku apmaiņu.

Jāuzlabo CERT.LV un NITDP lomas

Pēdējo gadu laikā CERT.LV ir kļuvis par uzticamu institūciju, kas spēj atbalstīt privāto sektoru, tostarp Latvijas MVU, drošības incidentu gadījumos. Kaut arī NITDP ir raksturota *Kiberdrošības stratēģijā* kā "centrālā nacionālā institūcija valsts un privātā sektora informācijas apmaiņai un sadarbībai", šķiet, ka CERT.LV faktiski atrodas vairāku ieinteresēto pušu sadarbības centrā Latvijā. Papildus saiknei ar privāto sektoru CERT.LV ir izveidojis spēcīgas saites ar pilsonisko sabiedrību un tehnisko kopienu, ko parāda tā mijiedarbība ar IT drošības ekspertu grupu un ikgadējā konference "Kiberšahs". CERT.LV ir darbojies arī kā instruments nesenās politikas attīstībā Eiropas Savienības līmenī, kā arī plašākā CERT kopienā, piemēram, attiecībā uz ievainojamības atbildīgu atklāšanu. Tomēr CERT.LV galvenā auditorija joprojām ir IT komandas sabiedriskajās un privātajās organizācijās. Viens no Latvijas paredzamajiem izaicinājumiem ir digitālās drošības risku piederības pāriešana no šīm IT komandām uz administrāciju.

Latvija varētu līdzsvarot CERT.LV panākumus, lai labāk izglītotu un iesaistītu citas ministrijas digitālās drošības stratēģijas ieviešanā, piemēram, ar personāla kopīgu pasākumu un darbsemināru kopīgu organizēšanu.

Kā norādīts iepriekš, NITDP izveidošana bija svarīgs solis kopīgas valdības pieejas veidošanā attiecībā uz digitālo drošību; tomēr ir konstatēti daži trūkumi. Joprojām nav skaidrības par NITDP lomu: tā ir alternatīvi definēta kā valdības iekšējā koordinācijas organizācija, AM konsultatīvā grupa, iestāde, kas atbild par *Kiberdrošības stratēģijas* izstrādi, ieviešanu, uzraudzību un novērtēšanu, un vārteja starp valdību un citām ieinteresētajām pusēm. Lai gan NITDP pašreizējais formāts ir sniedzis Latvijai iespēju paaugstināt digitālo drošību līdz svarīgam sabiedrības politikas jautājumam, tas var arī ierobežot tās biedru spēju pilnībā risināt jautājumu par jēgpilnu apmaiņu un koordināciju. Pastāv risks, ka NITDP var kļūt par monolītu struktūru, kurā amatpersonas apspriež iniciatīvas, īsti nepievēršoties galvenajiem politikas jautājumiem.

Lai pilnībā līdzsvarotu NITDP potenciālu, var izpētīt dažādus ceļus:

- palielināt sanāksmju biežumu, piemēram, ar darba līmeņa sanāksmi kā augsta līmeņa sanāksmes papildinājumu, koncentrējoties uz pievēršanos galvenajiem politikas jautājumiem un ātrāk nodrošinot rezultātus;

- labāk veidot sasaisti ar citām ieinteresēto pušu grupām, izmantojot CERT.LV atbalstu; izmantot "foruma" formātu, lai uzņēmumu vadītāji varētu regulāri, nevis tikai uz "ad-hoc" pamata apspriest problēmas, ar kurām viņi saskaras digitālās drošības jomā;
- tikties vienreiz vai divreiz gadā premjerministra biroja vadībā. Tas skaidri norādītu, ka digitālā drošība nav tikai valsts drošības jautājums, bet drīzāk tāds, kas attiecas uz ekonomiskajām un sociālajām aktivitātēm.

Latvijai ir jāveic labāka ekonomiskās un sociālās politikas dimensijas integrēšana valdības struktūrā, kas attiecas uz digitālo drošību

Digitālās drošības politikas ietvaru Latvijā veido spēcīgas tehniskās dimensijas (CERT.LV) kombinācija ar stratēģisko dimensiju (NITDP), tomēr tai trūkst politiskās dimensijas, kas aptver ekonomikas un sociālas perspektīvas. Lai pievērstos šim trūkumam, jāizpēta šīs iespējas:

- palielināt visas valdības iesaistīšanos un koordināciju ar skaidrām pilnvarām un plāniem "horizontālajām" ministrijām (piemēram, EM, VARAM), lai izstrādātu un ieviestu politiku, pamatojoties uz digitālās drošības ekonomiskajām un sociālajām dimensijām (nozaru partnerības, inovācijas, sertifikācija u.c.);
- labāk integrēt *Kiberdrošības stratēģiju* ar *Informācijas sabiedrības attīstības pamatnostādnēm*;
- pastiprināt *Kiberdrošības stratēģijas* rīcības plānu ar nosakāmiem mērķiem, kas ir orientēti uz ekonomisko un sociālo labklājību;
- attīstīt trīspusēju sadarbību ar Latvijas kaimiņvalstīm Igauniju un Lietuvu. Pašlaik šāda sadarbība digitālās drošības politikas jomā pastāv tikai starp CERT.LV un AM. Varētu izveidot jaunu darbības virzienu, kas sasaista par ekonomikas jautājumiem atbildīgās Baltijas valstu ministrijas, lai pārrunātu digitālo drošību no ekonomiskās un sociālās perspektīvas. (Faktiski Ekonomikas lietu ministrija ir atbildīga par digitālās drošības politikas koordinēšanu Igaunijā). Trīs valstu politiķi varētu regulāri (vismaz divreiz gadā) tikties, lai paplašinātu koordināciju un veiktu informācijas apmaiņu par saiknēm starp digitālo drošību un ekonomisko un sociālo labklājību.

5.2. ielikums. Politikas ieteikumi

Lai pievērstos digitālās drošības izaicinājumiem un iespējām, Latvija var balstīties uz esošajiem stabilajiem pamatiem. Latvijas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) ir starptautiski atzīta par savu tehnisko kompetenci un rādījusi piemēru attiecībā uz koordinētas ievainojamības atklāšanas politikas pieņemšanu. Latvijas Aizsardzības ministrija (AM) ir arī stingri apņēmusies atbalstīt digitālo drošību kā stratēģijas jautājumu, kā tiek norādīts *Latvijas kiberdrošības stratēģijā (2019.-2022. gadam)*. Vissvarīgākais ir tas, ka *Kiberdrošības stratēģijā* digitālā drošība tiek pienācīgi atzīta kā ekonomikas un sociālo risku pārvaldības izaicinājums, nevis vienkārši tehnisks jautājums. Nacionālās IT drošības padomes (NITDP) izveidošana 2011. gadā bija labs pirmais solis, veidojot valdības kopējo pieeju digitālajai drošībai.

Tomēr sabiedrības politikas un pārvaldības ietvars, kas attiecas uz digitālo drošību Latvijā, vēl nepietiekami atspoguļo šo ekonomikas un sociālo risku pārvaldības pieeju. Turklāt digitālās drošības politikas izstrāde un ieviešana Latvijā joprojām koncentrējas uz nacionālās drošības ietvaru. Tā rezultātā institūcijās un valsts politikā netiek pietiekami pievērsta uzmanība digitālās drošības ekonomiskajai un sociālajai dimensijai (piemēram, prasmes, inovācijas, MVU). Turklāt ieinteresētās puses nav pietiekami konsultētas par digitālās drošības politikas veidošanu. Lai risinātu šīs problēmas, Latvijai jāapsver:

- savas digitālās stratēģijas atbalstīšana augstākajā valdības līmenī;
- pastiprinot visas valdības pieeju digitālajai drošībai, palielinot "horizontālo" (proti, par ekonomikas un reģionālo attīstību atbildīgo) ministriju iesaistīšanās līmeni digitālās drošības politikas veidošanā un iniciatīvās;
- labāka digitālās drošības stratēģijas integrēšana ar valsts digitālo stratēģiju (*Informācijas sabiedrības attīstības pamatnostādnes*);

5.2. ielikums. Politikas ieteikumi *(cont.)*

- prasmju pilnveidošanas un darbaspēka apmaiņas programmu izveidošana starp valsts iestādēm, lai citas ministrijas varētu gūt labumu no CERT.LV un AM pieredzes, kā arī karjeras iespēju veicināšana digitālās drošības jomā;
- atbalsts vairāku ieinteresēto pušu kopienas izveidošanai un vairāku ieinteresēto pušu sadarbības palielināšanai ar ilgtspējīgām partnerībām uz uzticamības pamata (piemēram, NITDP lomas paplašināšana, organizējot "foruma" formāta pasākumus, lai efektīvi iesaistītu kopienu);
- starptautiskās sadarbības palielināšana, it īpaši ar citām Baltijas valstīm, digitālās drošības jomā, lai veicinātu ekonomikas un sociālo labklājību, papildus nacionālās drošības vai IT drošības jomās esošajām programmām.

Uzticamības veidošana ar lielāku privātumu

(VDAR) Vispārīgā datu aizsardzības regula nodrošina galveno tiesību aktu struktūru personas datu aizsardzībai Latvijā un citās ES valstīs. *(FPDAL) Fizisko personu datu apstrādes likums* tika pieņemts tādu noteiktu jautājumu regulēšanai, kas attiecas uz VDAR tiešu pielietojumu Latvijā, piemēram, nosakot uzraudzības iestādes statusu unvalsts prasības specifiskās personas datu apstrādes situācijās.

FPDAL pieņemšanā tika ņemta vērā VDAR un līdz ar to aptvertas *ESAO Pamatnostādnes par privātās dzīves aizsardzību un personas datu pārrobežu plūsmu*. Visiem publiskajiem un privātajiem pārziņiem ir jāievēro FPDAL prasības.

Šajā sadaļā ir pārskatītas FPDAL galvenās funkcijas un to ieviešana. Likumā tiek ņemti vērā iespējamie izaicinājumi, kas ir atklāti VDAR kontekstā un uzraudzības iestādes galvenās aktivitātes saskaņā ar FPDAL un VDAR.

Datu aizsardzības tiesiskais regulējums

FPDAL kopā ar VDAR un likumu Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā veido pašreizējo tiesisko regulējumu, kas nosaka personas datu apstrādi publiskajam un privātajam sektoram Latvijā. FPDAL ir sadalīts 8. nodaļās un satur 37. sadaļas un 5 pārejas nosacījumus. FPDAL pilnībā stājās spēkā 2018. gada 5. jūlijā, un neilgi pēc tam tika pieņemti *Ministru kabineta noteikumi Nr. 478* ar nosaukumu "Datu valsts inspekcijas direktora amata pretendentu atlases un atbrīvošanas no amata noteikumi", kas stājās spēkā 2019. gada 18. oktobrī.

Vairāki likumi nosaka personas informācijas privātumu un apstrādi dažādās jomās Latvijā. Tie iekļauj šos:

- Šengenas informācijas sistēmas darbības likums nosaka, kurām institūcijām ir piekļuve šai sistēmai, un pilnvaro DVI personas datu apstrādes uzraudzībai šajā sistēmā.
- *Elektronisko dokumentu likums* nosaka elektroniskās komercijas un elektronisko parakstu juridisko statusu, kā arī nosacījumus elektronisko dokumentu glabāšanai un noteikumus par sertifikācijas pakalpojumu sniedzēju un uzticamo sertifikācijas pakalpojumu sniedzēju akreditāciju un uzraudzību.
- *Elektronisko sakaru likums* pilnvaro Datu valsts inspekciju (DVI) uzraudzīt personas datu aizsardzību elektronisko sakaru sektorā saskaņā ar FPDAL norādītajām tiesībām.
- *Cilvēka genoma izpētes likums* nosaka DVI uzraudzības funkcijas attiecībā uz ģenētikas datiem, iekļaujot sūdzību izskatīšanu, kas attiecas uz tādu ģenētisko datu apstrādi, kurus datu subjekti var iesniegt DVI.
- *Informācijas tehnoloģiju drošības likums* nosaka darbības, kas jāveic informācijas drošības incidenta gadījumā.
- *Pacientu tiesību likums* nosaka pacientu tiesības un aizsardzību, iekļaujot personas datu aizsardzību.
- *Latvijas Administratīvo pārkāpumu kodekss*, kura termiņš beidzas 2020. gada 1. jūlijā, nosaka sankcijas (un to apjomu), kuras var piemērot personas datu aizsardzības pārkāpumu gadījumos, kā arī šādu sankciju piemērošanas procedūras.
- *Administratīvā procesa likums* attiecas uz administratīvajām procedūrām institūcijās, ja citi likumi neparedz konkrētus noteikumus.

- *Krimināllikums* nosaka krimināltbildību par personas datu pārkāpumiem. Ja DVI secina, ka lieta var nozīmēt krimināltbildību, tā var pārsūtīt lietu Valsts policijai.
- *Bērnu tiesību aizsardzības likums* nosaka aizliegumu izplatīt informāciju par bērniem, piemēram, tas attiecas uz informāciju, kas ir personīgi iegūta no bērniem kā upuriem vai lieciniekiem, vai bērniem, kuri ir izdarījuši likumpārkāpumu.

Atsevišķos noteikumos ir aprakstīti arī personas datu aizsardzības tehniskie un organizatoriskie pasākumi.

MK noteikumos 117/2004 *par elektronisko dokumentu izvērtēšanas veidu, uzglabāšanas kārtību un nodošanu valsts arhīvam glabāšanā*ir norādīts elektronisko dokumentu izvērtēšanas veids, uzglabāšanas kārtība un laika periodi, kad šādi dokumenti tiek nodoti glabāšanā valsts arhīvos. Noteikumi attiecas uz valsts un pašvaldības iestādēm un juridiskajām personām, kurām elektroniskie dokumenti ir jānodod valsts glabāšanai saskaņā ar normatīvajiem aktiem.

MK noteikumos 473/2005 ir norādītas papildu procedūras, kas attiecas uz elektronisko dokumentu izstrādi, sagatavošanu, uzglabāšanu un apriti valsts un pašvaldību institūcijās, procedūras, kas nosaka elektronisko dokumentu apriti starp valsts un pašvaldību iestādēm vai šīm iestādēm un fiziskām personām, un juridiskām personām.

Institucionālā uzraudzība

Datu valsts inspekcija (DVI) tika izveidota 2001. gada 2. janvārī un darbojās saskaņā ar iepriekšējo Personas datu aizsardzības likumu (nav spēkā kopš 2018. gada 5. jūlija). Tagad DVI darbojas saskaņā ar FPDAL, VDAR, *likumu Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā* un 2019. gada 18. oktobra *Ministru kabineta noteikumiem Nr. 478*.

DVI strādā 25 cilvēki, un tās paziņotais budžets 2019. gadā bija 640 998 EUR. Ņemot vērā tās plašos pienākumus kopš FPDAL un VDAR stāšanās spēkā, ir jāpalielina personāls un resursi. It īpaši DVI nepietiek resursu, lai noalgotu speciālu IT un tehnisko personālu privātuma pārkāpumu izmeklēšanai digitālajā telpā

Turklāt DVI uzrauga Šengenas informācijas sistēmas nacionālo komponentu, pārbaudot, vai personas datu apstrādē netiek pārkāptas datu subjektu tiesības, un pārstāv Latvijas Republiku Šengenas informācijas sistēmas kopīgās uzraudzības iestādē, Eiropola kopīgās uzraudzības iestādē, Eiropola apelācijas komitejā un Muitas informācijas sistēmas kopīgās uzraudzības iestādē, Eiropas Datu aizsardzības padomē un Eiropas Padomes konsultatīvajā komitejā saistībā ar Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (*108. konvencija*), kā arī pārbauda citas Eiropas Savienības un starptautisko datu aizsardzības iestāžu darbības.

Nākamajās sadaļās tiek aplūkots līmenis, kādā DVI efektīvi darbojas, ieviešot FPDAL un VDAR, un analizēta pieejamā statistika saistībā ar DVI darbību uzraudzību un novērtēšanu.

Valsts datu inspekcijas (DVI) mērķi un tvērums

Saskaņā ar FPDAL DVI mērķis ir aizsargāt fundamentālās cilvēku tiesības un brīvības datu aizsardzības jomā. DVI veic savas darbības un darbojas uz neatkarīga pamata, ņemot vērā principus par vienlīdzību likuma priekšā, nevainīguma prezumpciju, ticamību un likumību.

DVI specifiskās darbības un uzdevumi (papildus VDAR 57. pantā norādītajiem) ir ietverti FPDAL 4. sadaļā (5.3. ielikums).

Citi DVI galvenie saistības uzdevumi ar FPDAL un VDAR iekļauj ikgadējā ziņojuma izstrādi par tās darbību un funkcijām; ziņojums tiek iesniegts Saeimai, Ministru kabinetam, Augstākajai Tiesai, Eiropas Komisijai un Eiropas Datu aizsardzības kolēģijai (līdz 1. martam), kā arī tiek nodrošināta tā pieejamība tās tīmekļa vietnē (13. sadaļa).

Tāpat arī FPDAL 5 sadaļā (papildus VDAR 58. pantā ietvertajām tiesībām) tiek norādīts DVI saraksts ar FPDAL ieviešanas tiesībām un pilnvarām (5.4. ielikums).

5.3. ielikums. Latvijas DVI galvenās regulatīvās pilnvaras un darbības saskaņā ar FPDAL

1. Uzraudzīt personas datu apstrādes atbilstību likumu un noteikumu prasībām.
2. Veicināt datu aizsardzības efektivitāti.
3. Nodrošināt datu aizsardzības sertifikācijas procedūras.
4. Nodrošināt datu aizsardzības darbinieku kvalifikācijas pārbaudi un uzturēt to datu aizsardzības darbinieku sarakstu, kuri ir nokārtojuši kvalifikācijas eksāmenu.
5. Sniegt ieteikumus Saeimai, Ministru kabinetam, pašvaldībām un citām institūcijām atbilstoši savai kompetencei attiecībā uz likumu un noteikumu grozījumiem, kā arī piedalīties citu institūciju sagatavoto likumprojektu un noteikumu izstrādē un atzinumos.
6. Sniegt atzinumus par valsts pārvaldes iestādēs izveidojamo datu apstrādes sistēmu atbilstību normatīvo aktu prasībām.
7. Sniegt atzinumus valsts akreditācijas iestādei par sertifikācijas iestādes atbilstību Datu aizsardzības regulai.
8. Sadarboties ar ārvalstu uzraudzības iestādēm, kas ir iesaistītas datu aizsardzībā, informācijas atklātībā un piekļuvē, kā arī nevēlamā komerciālā komunikācijā.
9. Nodrošināt, lai informācijas pieprasījumi no datu objekta tiktu pārsūtīti uz Eiropas Tiesiskās sadarbības vienību (Eurojust) un Eiropas Policijas biroju (Eiropolu).
10. Pārstāvēt Latvijas Republiku starptautiskās organizācijās un pasākumos datu aizsardzības jomā.
11. Veikt pētījumus, analīzi, sniegt ieteikumus un viedokļus, kā arī informēt sabiedrību par savas kompetences jomu aktuālajiem jautājumiem.
12. Veikt citos likumos un noteikumos norādītos uzdevumus.
13. Publicēt informāciju savā tīmekļa vietnē par Datu aizsardzības regulas pārkāpumiem, ko izdarījušasjuridiskas personas, valsts un privātas iestādes un amatpersonas, kā arī citas valsts iestādes, un to novēršanu.

5.4. ielikums. DVI tiesības saskaņā ar FPDAL

1. Veikt datu apstrādes pārbaudi, ievērojot likumos un noteikumos iekļautās prasības.
2. Sastādīt ziņojumus par administratīvajiem pārkāpumiem, izmeklēt administratīvo pārkāpumu lietas un piemērot administratīvās sankcijas par pārkāpumiem.
3. Pieprasīt un saņemt dokumentus, kopijas un citus materiālus, kas ir nepieciešami pārbaudei, tostarp ierobežotas pieejamības informāciju, bez maksas no privātpersonām, valsts pārvaldes institūcijām un amatpersonām.
4. Apmeklēt valsts pārvaldes institūcijas un ražotnes, noliktavas, komerciālas un citas nedzīvojamas telpas, kas pieder, ir īpašumā vai ko izmanto juridiskas un fiziskas personas Latvijas teritorijā, lai pārbaudītu pārziņa darbības atbilstību likumos un noteikumos iekļautajām prasībām, rīkojoties savas kompetences ietvaros.
5. Atbilstoši savai kompetencei brīvi iepazīties ar visu veidu informāciju, kas ir pieejama reģistros, informācijas sistēmās, datubāzēs un tai piekļūt (neatkarīgi no informācijas īpašnieka), lai iegūtu pārbaudei nepieciešamo informāciju.
6. Pieprasīt un saņemt atbilstoši savai kompetencei informāciju, dokumentus un citus tādus materiālus par personām sniegtajiem pakalpojumiem, kas ir nepieciešami pārbaudei.
7. Pieprasīt un saņemt neatkarīga un objektīva eksperta viedokli pārbaudes ietvaros.
8. Sniegt atbildes angliski, izmeklējot nerezidentu sūdzības sadarbībā ar citām uzraudzības iestādēm.
9. Ierosināt lietas izskatīšanu tiesā par šī Likuma vai Datu regulas pārkāpumiem.

Saskaņā ar FPDAL 6. sadaļas 2. apakšpunktu DVI direktoram ir pienākums izveidot konsultatīvās padomes, kā arī darba grupas jautājumu izvērtēšanai DVI kompetences jomās. Pēc Tieslietu ministrijas (TM) iniciatīvas 2018. gadā tika izveidota Fizisko personu datu aizsardzības konsultatīvā atbalsta padome (DAKP). DAKP mērķis ir veicināt vispārējās izpratnes un labas pārvaldības principu pielietojumu VDAR ieviešanā, kliedēt mītus un novērst nepareizas interpretācijas ne tikai publiskajā administrācijā, bet arī sabiedrībā kopumā.

Turklāt DAKP ir kā platforma diskusijām jautājumos, kas attiecas uz VDAR un tās piemērošanu, labākās pieredzes un kompetences apmaiņu, datu aizsardzības sekmēšanu un savstarpēji interesējošu jautājumu pārrunāšanu. Padomi pārvalda TM valsts sekretārs, un tā ietver DVI un lielāko nozaru (piemēram, plašsaziņas līdzekļu, veselības aprūpes, labklājības un izglītības) pārstāvjus.

Latvijas Pašvaldību savienība (LPS) regulāri organizē diskusijas un publicē informāciju par datu aizsardzību. LPS ir sabiedriska organizācija, kas apvieno Latvijas Republikas pašvaldības uz brīvprātības pamata. Saskaņā ar *Likuma par pašvaldībām* 96. pantu LPS ir pilnvarota pārstāvēt pašvaldības sarunās ar Ministru kabinetu, jo LPS pārstāv vairāk nekā pusi no visu veidu pašvaldībām. Visas Latvijas pašvaldības (no 9 pilsētām un 110 municipalitātēm) ir LPS dalībnieces. Citas institūcijas var sazināties arī ar TM un DVI. 2019. gada sākumā datu aizsardzības speciālisti no ministrijām un to pakļautībā esošajām iestādēm sapulcējās, lai pārrunātu aktuālākos jautājumus saistībā ar VDAR ieviešanu, iekļaujot datu aizsardzību, un veiktu labākās pieredzes un kompetences apmaiņu.

FPDAL satur piecus pārejas nosacījumus. 5. sadaļā ir norādīts, ka Ministru kabinetam ir jānovērtē regulējuma efektivitāte attiecībā uz datu aizsardzības darbinieku kvalifikācijas eksāmenu, ko satur FPDAL, un jāiesniedz vērtējums par šī eksāmena atcelšanas iespēju Saeimai līdz 2021. gada 30. jūnijam.

Piemērošana

DVI ir atbildīga par FPDAL, VDAR un citu nacionālo normatīvo kas nosaka privātumu un datu aizsardzību, ieviešanu.

2019. gada 26. augustā DVI piemēroja naudas sodu 7000 EUR apmērā tiešsaistes mazumtirgotājam par VDAR neievērošanu, it īpaši par to, ka netika ievērotas un aizsargātas datu subjektu tiesības uz izdzēšanu un sadarbību ar uzraudzības iestādi. Sankcijas tika piemērotas tādēļ, ka mazumtirgotājs neveica savu pārziņa pienākumu par datu subjekta pieprasījuma izpildi, kā arī nenodrošināja DVI pieprasīto informāciju norādītajā laika periodā. Turklāt mazumtirgotājs neievēroja rīkojumu, kuru DVI bija sniegusi saskaņā ar VDAR pantu 58(2)(c) un (g) FPDAL 23. pantu.[5]

Attiecībā uz lēmumiem par soda naudām DVI saņēma 1236 sūdzības saistībā ar iespējamiem personas datu apstrādes pārkāpumiem. Atbildot uz to, tika veiktas 246 pārbaudes, un 9 gadījumos tika uzlikti naudas sodi.. Administratīvo pārkāpumu lietās piemērotie naudas sodi bija no 300 līdz 150 000 EUR. Septiņos gadījumos tika izteikts brīdinājums.

Attiecīgi 2018. un 2017. gadā pieņemto lēmumu skaits administratīvo pārkāpumu lietās ir parādīts 5.1.

5.1. tabula. Administratīvo pārkāpumu lietās pieņemtie lēmumi

	Pieņemtie lēmumi (skaits)	Lēmumi par lietas izbeigšanu (skaits)	Piemērots sods (skaits)	Iekļaujot		Soda naudu kopsummas (eiro)
				Piemērotās soda naudas (skaits)	Brīdinājumu izteikšana (skaits)	
2017	151	86	65	35	30	46 593
2018	97	71	26	12	14	10 230
2019	45	29	16	9	7	163 523

Avots: DVI (2020), *Activity Report 2019*, Data State Inspectorate Republic of Latvia, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

Līdzīgā veidā DVI ziņo, ka no 20 inspekcijas amatpersonu apstrīdētajiem lēmumiem attiecībā uz administratīvo pārkāpumu 12 tika pārsūdzēti tiesā. Kopumā 2018. gadā tika sāktas 24 tiesvedības. DVI ziņo, ka tiesā pārsūdzēto lietu skaits 2018. gadā samazinājās, jo apstrīdēto inspekcijas lēmumu, kas tika pārsūdzēti, skaits 2017. gadā samazinājās par 3.

Tehniskie pasākumi datu aizsardzībai

FPDAL nesatur nekādus specifiskus nosacījumus vai sadaļas, kas attiektos uz personas informācijas tehniskiem un organizatoriskiem drošības pasākumiem. VDAR 32. pantā ir noteikti pārziņu un apstrādātāju pienākumi, kas attiecas uz pienācīgu tehnisko un organizatorisko pasākumu ieviešanu, lai nodrošinātu riskam atbilstošu drošības līmeni.

Latvijas *Elektronisko sakaru likuma* 68.panta pirmajā daļā ir ietverts nosacījums par personas datu apstrādes drošību elektronisko sakaru komersantiem kur norādīts, ka minētie pakalpojumu sniedzēji: 1) nodrošina to, ka personas datiem var piekļūt tikai pilnvarots personāls un tie tiek izmantoti tikai iepriekš norādītajos nolūkos; 2) nodrošina personas datu aizsardzību pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu zudumu, kā arī neatļautu vai nelikumīgu glabāšanu, apstrādi, piekļuvi vai izpaušanu; 3) dokumentē iekšējās procedūras, kas tiek veiktas personas datu aizsardzības pārkāpuma izmeklēšanas un novēršanas nolūkos.

Paziņojums par personas datu pārkāpumu

VDAR 33. pantā ir noteikts, ka pārzinim ir jāziņo uzraudzības iestādei par drošības incidentiem vai personas informācijas datu pārkāpumiem bez liekas kavēšanās un ne vēlāk kā 72 stundas pēc uzzināšanas par situāciju, ja datu pārkāpums rada risku indivīdu tiesībām un brīvībām. VDAR 34. pantā ir noteiktas datu pārziņu pienākums paziņot datu subjektam par personas informācijas datu pārkāpumiem bez nepamatotas kavēšanās, ja datu pārkāpums varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām.

Darbības, kas jāveic datu pārkāpuma gadījumā, ir noteiktas saskaņā ar VDAR un *likumu Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā*. VDAR un *Pamatnostādnes, kas attiecas uz personas datu pārkāpuma paziņojumu saskaņā ar Regulu 2016/679*, nosaka pienākumus, kas attiecas uz ziņošanu par datu pārkāpumiem, datu pārziņiem un datu apstrādātājiem.[6]

Informācijas tehnoloģiju drošības likums nosaka darbības, kas jāveic informācijas drošības incidentu gadījumos.

Informācijas tehnoloģiju drošības likuma galvenais mērķis ir uzlabot informācijas tehnoloģiju drošību valsts, pašvaldību iestāžu un privātu institūciju starpā. Likums nosaka pienākumus, kas attiecas uz ziņošanu par drošības incidentiem un darbībām drošības ievainojamības novēršanai. Sadaļā 6(2) ir atrunāts, ka valsts vai pašvaldības institūcijām vai informācijas tehnoloģiju kritiskās infrastruktūras īpašniekam ir 90 dienu laikā jāveic visas nepieciešamās darbības, lai novērstu drošības neaizsargātību, un jāinformē kompetentās incidentu reaģēšanas vienības. Turklāt saskaņā ar sadaļu 7(4) Drošības incidentu reaģēšanas vienībai var tikt atļauts veikt personas datu apstrādi, kas nav saistīta ar šādu incidentu novēršanu, tikai tad, ja tā sagatavo un nosūta DVI aprakstu par personas datu plānoto apstrādi un aizsardzību. Drošības incidentu reaģēšanas vienībai ir jāsagatavo un jāiesniedz DVI ziņojums par iepriekšējā gadā veikto personas datu apstrādi līdz nākamā gada janvāra beigām.

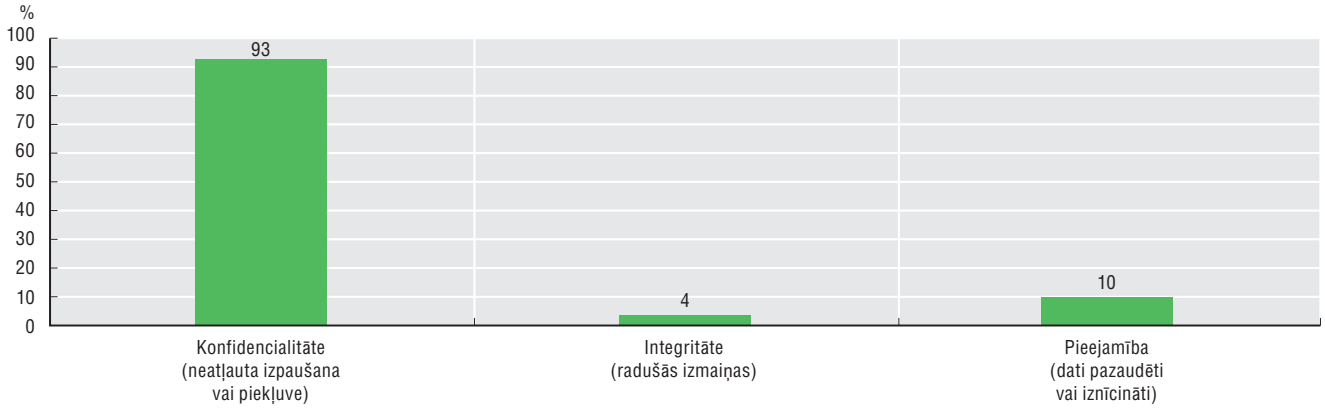
DVI 2019. gada ikgadējā ziņojumā ir norādīts, ka DVI ir saņēmusi 1236 sūdzības un pieteikumus saistībā ar personas datu apstrādes iespējamiem pārkāpumiem. Pieteikumus un sūdzības saskaņā ar VDAR 57. pantu iesniedza gan datu subjekti, gan citas valsts iestādes (visbiežāk tiesībaizsardzības iestādes), kā arī organizācijas un asociācijas. DVI saņēma 107 ziņojumus par personas datu pārkāpumiem, un daži no tiem satur vairāku veidu pārkāpumus (5.7. attēls).

Privātuma pārvaldības programmas

Pārskatāmības princips ir viens no 1980. gada Privātuma pamatnostādņu astoņiem sākotnējiem pamatprincipiem. Privātuma pamatnostādņu 2013. gada pārskatījumā tika iekļauta jauna sadaļa "Pārskatāmības ieviešana", kurā tiek akcentēti elementi, kas ir nepieciešami datu pārziņiem, lai ieviestu pārskatāmības principu, it īpaši ieviešot jēdzienu "privātuma pārvaldības programmas" (PPP). Saskaņā ar pārskatītajām Pamatnostādnēm PPP ir primārais darba instruments, kas, kā paredzams, palīdzēs praksē īstenot Pamatnostādņu 2. daļā ietvertos pamatprincipus. It īpaši pievienotajā sadaļā ir norādīts, ka datu pārzinim ir jānodrošina atbilstība Pamatnostādnēm attiecībā uz visiem viņa pārziņā esošajiem personas datiem, ieviešot savu darbību struktūrai, mērogam, apjomam un sensitivitātei

pielāgotu PPP, un tas nodrošina pienācīgu aizsardzību, pamatojoties uz privātuma riska novērtējumu un iekļaujot plānus reaģēšanai uz jautājumiem un incidentiem. Turklāt datu pārzinim vajadzētu būt gatavam pierādīt sava PPP darbību un, ja nepieciešams, informēt iestādes un datu subjektus, ja ir bijis ievērojams drošības pārkāpums, kas ietekmē personas datus. Eiropā PPP joprojām ir agrīnā attīstības fāzē, un tikai dažas valstis ir pieņēmušas vispusīgas pamatnostādnes un labāko pieredzi publiskā sektora institūcijām.[7]

5.7. attēls. Ziņotie personas datu pārkāpumi Latvijā



Avots: DVI (2020), *Activity Report 2019*, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

2018. gada 18. decembrī DVI izstrādāja *Sarakstu ar tām apstrādes darbībām, uz kurām attiecas novērtējuma par ietekmi uz datu aizsardzību prasība*, saskaņā ar VDAR pantu 35(4). Dokumentā ir saraksts ar piemēriem, kas datu pārziņiem jāņem vērā, ja datu apstrāde var izraisīt augstu risku fizisku personu tiesībām un brīvībai. Dokumentā ir norādītas 13 dažādas iespējas, kad datu pārziņiem, kuru iestādes galvenā vieta ir Latvijas teritorija, jāveic datu ietekmes novērtējums.

DVI ir publicējusi arī vairākas rekomendācijas (piemēram, par komerciālo komunikāciju un personas datu apstrādi sociālajos tīklos). DVI cieši sadarbojas ar asociācijām, lai izstrādātu specifiskas vadlīnijas personas datu apstrādei dažādās jomās.[8]

Politikas veidošana

NVO var piedalīties politikas veidošanā, komentējot likumprojektus, kas ir paziņoti sabiedrībai, lai saņemtu komentārus to veidošanas periodā. Konsultēšanās ar NVO notiek pirms katras jaunas iniciatīvas un likumdošanas projekta priekšlikuma, galvenokārt balstoties uz uzaicinājumu no TM, kas vada tiesību aktu projekta izstrādi privātuma jomā. Svarīgās NVO iekļauj Datu aizsardzības speciālistu asociāciju, Latvijas Informācijas un komunikācijas tehnoloģijas asociāciju un Latvijas Finanšu nozares asociāciju. Piemēram, MK noteikumi par kredītinformācijas biroju sertifikāciju un uzraudzību tika izstrādāti, konsultējoties ar Latvijas Finanšu nozares asociāciju un Sertificēto personas datu speciālistu asociāciju. Vēl viens piemērs ir DVI ikgadējo rekomendāciju izstrāde koordinācijā ar NVO, iekļaujot privātos dalībniekus, piemēram, rekomendācija "Personas datu apstrāde tiešsaistes sociālajos tīklos", kas tika izstrādāta pēc dažādu sociālo tīklu pakalpojumu sniedzēju viedokļu analīzes.

DVI 2018. gada ikgadējā ziņojumā ir norādīts, ka DVI ir atbalstījusi personas datu aizsardzības vadlīniju izstrādi, kas ir attiecināmas uz dažādu nozaru asociācijām. Piemēram, tiek minēts, ka DVI ir iesaistījusies datu aizsardzības vadlīniju izstrādē kopā ar Latvijas Finanšu nozares asociāciju un Latvijas Personāla vadīšanas asociāciju, kā arī sniegusi atbalstu Latvijas Zvērinātu advokātu padomei, sagatavojot vēl vienu vadlīniju komplektu datu aizsardzībai.

Pārrobežu sadarbības īstenošana

2013. gada ESAO pārskatītajās privātuma vadlīniju IV sadaļā tiek akcentēta pārrobežu sadarbības nozīme, īstenojot privātuma likumus un sekmējot savstarpējo juridisko palīdzību privātuma tiesībaizsardzības iestādēm.

VDAR 61. un 62. pantā ir akcentēts uzraudzības iestāžu pienākums nodrošināt savstarpēju un efektīvu sadarbību, kas attiecas uz konsultācijām, pārbaudēm un izmeklēšanām saistībā ar datu aizsardzību, un noteikti kritēriji, kas ir nepieciešami, lai veiktu kopīgas izmeklēšanas un kopīgus ieviešanas pasākumus pret pārziņiem un datu apstrādātājiem, kuri attiecīgi atrodas vairāk nekā vienā ES dalībvalstī.

Līdz 2016. gadam DVI sadarbojās ar ārvalstu datu aizsardzības iestādēm (DAI) katrā atsevišķā gadījumā un regulāri ar citām Baltijas valstīm. Pēc VDAR pieņemšanas DVI regulāri sadarbojas ar ES dalībvalstu datu aizsardzības iestādēm atbilstoši VDAR.

DVI 2018. gada ikgadējā ziņojumā ir norādīts, ka 2017. gada 15. jūnijā DVI parakstīja sadarbības memorandu par principa "Vispirms konsultācija" ieviešanu, kas atbalsta koncentrēšanos uz klientu valsts regulatīvajās darbībās. Pielietojot principu "Vispirms konsultācija" DVI ir pamudinājusi pārzini VDAR izklāstīto pienākumu veikšanai 179 gadījumos. Ziņojumā ir norādīts, ka pārziņi ir rīkojušies atbilstoši DVI pamudinājumam 25 lietās (78 %).

Latvija vēl nepiedalās Globālajā privātuma tiesībaizsardzības tīklā (GPEN) un līdzīgos starptautiskos tīklos, kuri īsteno privātuma un datu aizsardzības likumus.

Latvija ir ratificējusi Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personu datu automātisko apstrādi (*108. konvencija*) 2001. gada 30. maijā un tās *Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām* 2017. gada 21. novembrī. Latvija ir parakstījusi grozījumu protokolu *(Konvencija 108+Konvencija 108*) 2018. gada 10. oktobrī, bet nav turpinājusi ar ratifikāciju.

DVI 2018. gada ikgadējā ziņojumā ir norādīts, ka DVI turpina iesaistīties Eiropas Padomes 108. konvencijas konsultatīvās komitejas darbā, piedaloties sanāksmēs, nodrošinot nepieciešamo statistisko informāciju un komentējot sagatavotos darba dokumentus.

Uzraudzība

DVI izveido ikgadējo ziņojumu un iesniedz ziņojuma kopsavilkumu TM. Šajā ziņojumā ir detalizēti atspoguļotas DVI galvenās darbības, sniegta informācija par finanšu resursiem un personālu, kā arī informācija par galvenajām problēmām, kas radušās gada laikā. Tajā tiek iezīmētas arī DVI nākamā gada prioritātes. Saskaņā ar attiecīgajiem MK noteikumiem ikgadējie ziņojumi un to kopsavilkumi ir pieejami (latviski) DVI tīmekļa vietnē.

DVI saņemtās sūdzības tiek analizētas katru ceturksni un izskatītas atbilstoši DVI attiecīgā gada plānotajām prioritātēm. Dažos gadījumos sūdzības vairāk tiek analizētas pēc ad - hoc principa, piemēram, ja DVI saņem vairākas sūdzības par vienu jautājumu īsā laika periodā.

Izglītība un informētība

DVI 2018. gada ikgadējā ziņojumā ir norādīts, ka DVI sadarbībā ar TM ir izstrādājusi informācijas materiālus iedzīvotājiem par VDAR pielietojuma apjomu. Tie ir zināmi kā "Mīti un patiesība", kas valsts pilsoņiem izskaidro viņu tiesības, kā arī pārziņu un datu apstrādātāju pienākumus saskaņā ar VDAR. DVI ir organizējusi 52 lekcijas un semināru par personas datu aizsardzību un VDAR pielietojumu valsts un privātā sektora pārstāvjiem un apmeklējusi 76 semināru, konferences, diskusiju sanāksmes un darba grupas, ko organizēja citas institūcijas un uzņēmēji.

Datu pārvaldības struktūras

Piekļuve datiem un to kopīgošana ir izšķiroši svarīga digitālās ekonomikas inovācijās. Piemēram, piekļuve datiem var uzlabot publisko pakalpojumu nodrošināšanu un sekmēt jauno valdības un sociālo izaicinājumu identificēšanu.

Atvērto datu politikas pārvaldību koordinē Latvijas valdība.

Latvijas Atvērto datu portālu izveidoja Eiropas Reģionālās attīstības fonds ar Publiskās pārvaldes informācijas un komunikācijas tehnoloģiju arhitektūras pārvaldības sistēmas (PIKTAPS) atbalstu.[9]

Latvija piedalās Atvērtās pārvaldības partnerībā (OGP), un kā minēts Latvijas Atvērto datu portālā, *Latvijas Trešais nacionālais atvērtās pārvaldības rīcības plāns* ietver darbību, kas veicinātu atvērtību, atbildību, sabiedrības iesaistīšanos un IKT izmantošanu. Šajā plānā ir iekļautas darbības dažādu tiešsaistes pakalpojumu uzlabošanai un ieviešanai. Vienas no 12 saistībām ir publiskos resursos pieejamu publisko datu portāla izstrāde. Tomēr, lai sasniegtu OGP 2017.-2019. gada plāna mērķus, Latvija ir apņēmusies iesaistīt sabiedrību datu kopu atlasīšanā. Līdz ar to tīmekļa vietnē ir funkcija, kas lietotājiem ļauj balsot par datiem, kurus viņi vēlas atvērt.

Secinājumi un politikas ieteikumi

Latvija ir ievērojami progresējusi privātuma un datu aizsardzības tiesību īstenošanā kopš VDAR un FPDAL stāšanās spēkā. DVI ir sākusi proaktīvi īstenot tiesisko regulējumu un uzlikt organizācijām administratīvus sodus par likumos noteikto vispārējo saistību neievērošanu. Tomēr DVI ir jābūt nodrošinātiem cilvēku un finanšu resursiem, kas ir nepieciešami, lai efektīvi veiktu tās uzdevumus, kuri iekļauj privātuma un datu aizsardzības digitālajā telpā konsultācijas un izmeklēšanas.

ESAO Privātuma pamatnostādņu 2013. gada pārskatījumā tika ieviesta PPP koncepcija, kas kalpo kā centrālie darbības mehānismi, ar kuru palīdzību organizācijas īsteno privātuma aizsardzību. It īpaši 15(a)(i) sadaļā ir norādīts, ka datu pārziņa PPP ir jāievieš ESAO Privātuma pamatnostādnēs "visiem personas datiem, kas ir tā kontrolē". Tiek gaidīta Eiropas Padomes 108. konvencijas konsultatīvās komitejas ceļveža izstrāde DVI, lai vairāk proaktīvi ieviestu VDAR nosacījumus par privātumu pēc ieceres un par privātumu pēc noklusējuma, kā arī PPP, un tajā ir jāņem vērā EDAK izstrādātās pamatnostādnes, kā arī esošā labākā pieredze ESAO dalībvalstīs.

Attiecībā uz pārskatāmības saistībām DVI ir izstrādājusi sarakstu ar apstrādes darbībām, kurām ir nepieciešami privātuma ietekmes novērtējumi. Tomēr DVI joprojām ir jāizstrādā pamatnostādnes pārskatāmības saistībām, kas ir izklāstītas saskaņā ar VDAR, piemēram, rīcības kodeksu ievērošana un esošo sertifikācijas shēmu izmantošana, ievērojot attīstību šajā jomā visā ESAO dalībā. Rakstīšanas laikā DVI ir jānosaka arī eksāmeni datu aizsardzības speciālistiem.

Attiecībā uz starptautisko sadarbību DVI ir bijusi diezgan aktīva Eiropas kontekstā, it īpaši attiecībā uz tās dalību Datu aizsardzības kolēģijā (EDAK) un Eiropas Padomes 108. konvencijas konsultatīvajā komitejā. Tomēr DVI vēl nav pievienojusies Globālajam privātuma aizsardzības tīklam (GPEN), kas varētu sekmēt un uzlabot tās sadarbību ar citām valstīm un reģioniem.

Speciālo datu kategoriju izmantošanas un apstrādes skaidra nošķiršana no privātuma tiesību aizsardzības paliek īpašs uzdevums, kuram ir jāveltī sevišķa uzmanība MI un IoT attīstības kontekstā. DVI ir tādējādi jānodrošina pastāvīga datu subjektu tiesību īstenošana saskaņā ar VDAR un nacionālās datu aizsardzības juridisko struktūru. Jātupina izstrādāt turpmākie aizsardzības pasākumi, kas palīdz uzlabot datu subjekta tiesību aizsardzību MI kontekstā, kā arī pārējie IoT uzdevumi. To var sasniegt ar turpmāku iesaistīšanos un sadarbībā ar starptautiskiem forumiem datu aizsardzības un privātuma jomā, iekļaujot ESAO darbu šajās jomās.

5.5. ielikums. Politikas ieteikumi

Latvijai veicamās turpmākās darbības, lai uzlabotu privātumu:

- Datu valsts inspekcijas (DVI) nodrošināšana ar cilvēku un finanšu resursiem, kas ir nepieciešami, lai efektīvi veiktu tās uzdevumus, kas iekļauj privātuma un datu aizsardzības konsultācijas un izmeklēšanas digitālajā telpā;
- veicināt DVI pamatnostādņu izstrādi, kā pamatu izmantojot esošo labo pieredzi, lai sekmētu pārskatāmību un "privātuma pārvaldības programmas" (PPP);
- mudināt uz DVI un citu valstu, tostarp ārpus ES, savstarpējo sadarbību, piemēram, pievienojoties Globālajam privātuma aizsardzības tīklam (GPEN);
- izveidot pienācīgu MI un IoT pārvaldību, tostarp turpinot iesaistīšanos un sadarbību ar starptautiskiem forumiem, piemēram, ESAO.

Patērētāju aizsardzība

Politikas struktūra

Latvijas *Patērētāju tiesību aizsardzības likums*[10] un *Negodīgas komercprakses aizlieguma likums*[11] satur vispārīgus principus, kas aptver: 1) informācijas izpaušanu; 1) produktu drošību; 3) negodīgu, maldinošu un agresīvu komercpraksi, kas attiecas uz tradicionālajiem un e-komercijas darījumiem. Saskaņā ar Eiropas Savienības (ES) *Patērētāju tiesību direktīvu 2011/83/ES* Patērētāju tiesību aizsardzības likums 2014. gadā tika grozīts ar *Attālinātā darba līgumu regulējumu*[12], kurā tiek identificētas galvenās informācijas izpaušanas prasības pirms līguma noslēgšanas (attiecībā uz uzņēmumu, produktu un darījumu). Regulējumā ir aptverti arī distances līgumu apstiprināšanas nosacījumi, kas saskaņā ar 17. pantu ir jānodrošina patērētājiem ar izturīga datu nesēja starpniecību un pamatoti pieņemamā laikā pēc līguma noslēgšanas (ne vēlāk kā preču piegādes laikā vai pirms pakalpojuma izpildes). Ar regulējumu tiek ieviestas arī jaunas atteikšanās tiesības patērētājiem, kuri noslēdz distances līgumus (tostarp ar e-komercijas starpniecību).

Papildus iepriekš minētajiem likumiem specifiski e-komercijas nosacījumi ir iekļauti *Informācijas sabiedrības pakalpojumu likumā*,[13] *Elektronisko sakaru likumā*[14] un iepriekš minētajā *Negodīgas komercprakses aizlieguma likumā*.

- *Informācijas sabiedrības pakalpojumu likumā* ir norādīta galvenā informācija, kas pakalpojumu sniedzējiem ir jānodrošina patērētājiem, iekļaujot pirmslīguma informāciju par uzņēmumu, produktu un darījumu. Tas aptver arī rīcības kodeksus, nosacījumus par informācijas glabāšanu terminālļa aprīkojumā, prasības par komercsakariem, atbildību, kā arī uzraudzības iestāžu, piemēram, Latvijas Patērētāju aizsardzības centra un DVI, lomu un pienākumiem.[15] Likuma 4. pantā ir norādīta vispārīga informācija, kas jānodrošina pakalpojumu sniedzējiem. 5. pantā ir izklāstīta informācija, kas pakalpojumu sniedzējam jānodrošina pirms pasūtījuma veikšanas. 7. pantā ir norādīta informācija par līguma noteikumiem un rīcības kodeksu, kas jānodrošina pakalpojumu sniedzējam.
- *Elektronisko sakaru likums* aptver lietotāju, elektronisko sakaru nodrošinātāju, privātu elektronisko sakaru tīklu un valsts administratīvo institūciju, kas ir saistītas ar elektronisko sakaru sektoru, tiesības un saistības. Tas satur arī nosacījumus par elektronisko sakaru pakalpojumiem un ierobežoto resursu lietošanu un administrāciju, iekļaujot spektra iedalīšanu un radio frekvenču piešķiršanu. Turklāt likumā ir noteiktas attiecīgo regulatīvo aģentūru tiesības un saistības dažādos sektoros saskaņā ar regulējumu. Tajā ir izklāstītas specifiskās saistības, kas attiecas uz juridiskajām personām un uzņēmumiem ar ievērojamu ietekmi tirgū, saistības attiecībā uz universāliem pakalpojumiem, datu aizsardzības saistības elektronisko sakaru sektorā un saistības, kas attiecas uz datu saglabāšanu balss telefonijas un publiskās telefonijas nodrošināšanā, kā arī publiskās interneta piekļuves pakalpojumu nodrošināšanā.
- *Negodīgas komercprakses aizlieguma likums* aptver arī bērniem paredzētas tiešsaistes reklāmas, maldinošu un negodīgu komercpraksi, kā arī produktu drošību.

Papildu prasības, kas nosaka darījumus tiešsaistē un it īpaši reklāmas bērniem, ir norādītas *Reklāmas likumā*[16] (5. sadaļā), kurā ir izklāstītas soda sankcijas par likuma un sekundārā regulējuma neievērošanu.

Maksājumu pakalpojumus, elektronisko naudu un maksājumu kartes nosaka *Maksājumu pakalpojumu un elektroniskās naudas likums*,[17] kurā ir noteiktas maksājumu pakalpojumu sniedzēju un lietotāju, e-naudas izdevēju un turētāju tiesības un pienākumi, kā arī prasības, kas attiecas uz maksājumu pakalpojumu nodrošināšanu e-naudas izsniegšanai, sadalei un atgūšanai, un atbildība par maksājumu iestādēm un e-naudas iestādēm.

Turklāt Latvijā pašlaik notiek process, kura gaitā tiek ieviestas turpmākās politikas par patērētāju aizsardzību, kas saskan ar nesen pieņemtajiem ES regulējumiem, kuri ietver centienus veicināt un uzlabot Eiropas vienoto digitālo tirgu, tostarp ES regulējumu par ģeobloķēšanu.[18] Pēc tam, kad stājās spēkā ES *regula*[19] par sadarbību starp valsts varas iestādēm, kuras ir atbildīgas par patērētāju aizsardzības likumu īstenošanu, 2018. gadā tika pieņemts Latvijas *Elektronisko sakaru likums*, kas valsts Patērētāju tiesību aizsardzības centram (PTAC) nodrošina papildu pilnvaras informācijas pieprasīšanai elektronisko sakaru nodrošinātājiem, un tas attiecas uz informāciju par abonentu vai lietotāju (piemēram, tīmekļa pārzini).

ESAO principu ieviešana digitālo patērētāju aizsardzībā

Šīs sadaļas mērķis ir novērtēt pakāpi, kādā Latvijas patērētāju politikas struktūra iemieso digitālo patērētāju aizsardzības vispārīgos principus, saskaņā ar ESAO *Rekomendāciju par patērētāju aizsardzību e-komercijas jomā*, kas ir zināma arī kā "E-komercijas rekomendācija" (ESAO, 2016. gads). Rekomendācijas galvenie nosacījumi ir ietverti 5.6. ielikums. Turklāt sadaļā tiek pētīta pakāpe, kādā Latvijas struktūra aptver pašreizējo e-komercijas formu dažādību, iekļaujot darījumus starp patērētājiem, darījumus ar mobilo ierīču starpniecību un darījumus, kas neietver naudas maksājumu.

5.6. ielikums. Digitālo patērētāju aizsardzības vispārīgie principi

- Godīga uzņēmējdarbības un reklāmu prakse
- Atbilstīga izpaušana
- Efektīvi procesi darījumu apstiprināšanai un maksājumiem
- Produkta drošība e-komercijas piegādes ķēdēs
- Jēgpilna piekļuve efektīviem mehānismiem, lai atrisinātu strīdus
- Patērētāju izglītība un informētība
- Varas iestāžu pilnvaras izpētīt un rīkoties iekšzemes līmenī
- Varas iestāžu spēja iesaistīties starptautiskajā politikā un īstenošanas sadarbībā.

Avots: OECD (2016).

E-komercijas rekomendācija tika pārskatīta 2016. gadā, lai aptvertu daudzas jaunas problēmas un attīstības, piemēram, ātru izaugsmi un nemateriālu digitālā satura produktu pieņemšanu no patērētāju puses, mainīgu un aktīvāku patērētāju rīcību tiešsaistē, tostarp ar mobilo ierīču starpniecību, plaša tiešsaistes un mobilo maksājumu klāsta parādīšanos, kā arī pieaugošās raizes par tiešsaistes produktu drošību. Rekomendācijā ir izcelta arī nepieciešamība nodrošināt kompensāciju patērētājiem, kuri ir iesaistīti nemonetāros darījumos, un ietverts aicinājums uzņēmumiem, lai klientiem tiktu nodrošināta skaidra un skaidri redzama informācija par digitālā satura produktu ierobežojumiem, funkcionalitāti un mijiedarbību un notiktu pievēršanās e-komercijas pakalpojumu privātuma un drošības riskiem, iekļaujot maksājumu metodes.

Institucionālā uzraudzība

E-komercijas rekomendācija satur atjauninātus nosacījumus par patērētāju aizsardzības iestādēm (PAI) un nepieciešamību uzlabot savu patērētāju aizsardzības spēju e-komercijā. Rekomendācijas 2. daļā tiek akcentēti regulatīvās struktūras ieviešanas principi un valdības tiek aicinātas sadarbībai ar ieinteresētajām pusēm, lai sasniegtu Rekomendācijas mērķi:

- pārskatot un, ja nepieciešams, pieņemot un pielāgojot likumus, kas aizsargā patērētājus e-komercijā, paturot prātā tehnoloģijas neitralitātes principu (53 ii);
- izveidojot un uzturot PAI, kurām ir pilnvaras un iespējas veikt izmeklēšanu un rīkoties, lai patērētājus aizsargātu pret krāpniecisku, maldinošu vai negodīgu komerciālo praksi, kā arī resursi un tehniskā kompetence savu pilnvaru efektīvai izmantošanai (53 iii);
- iedrošinot efektīvu kopīgas regulācijas un pašregulācijas mehānismus pastāvīgu attīstību, kas palīdz uzlabot uzticību e-komercijai, tostarp atbalstot efektīvus strīdu izšķiršanas mehānismus (53 v).

Latvijā par patērētāju politikas veidošanu, realizēšanu un ieviešanu saistībā ar e-komerciju ir atbildīgas tās pašas varas iestādes, kuras pārzina tradicionālo iepirkšanos. Patērētāju politikas veidošanu vada EM,[20] it īpaši konkurences, tirdzniecības un patērētāju tiesību daļa. Nozaru politiku, kas attiecas uz patērētāju jautājumiem (piemēram, veselības aprūpes pakalpojumi, transports vai telekomunikācijas), koordinē citas ministrijas kopā ar EM. Tā kā patērētāju aizsardzība, tostarp strīdu izšķiršana, ir cieši saistīta ar civiltiesiskajiem un administratīvajiem likumiem, TM ir iesaistīta arī patērētāju politikas attīstībā.

Galvenā īstenošanas un ieviešanas iestāde ir PTAC,[21] kas ir pakļauta EM. Kaut arī EM ir atbildīga par PTAC pieņemto lēmumu juridiskās atbilstības pārskatīšanu, tā nevar iejaukties PTAC lēmumu pieņemšanas procesā vai pārskatīt viedokli, uz kura pamata pieņemts lēmums. EM ir tiesības iejaukties un likt PTAC pieņemt lēmumu tikai gadījumos, kad PTAC nerīkojas saskaņā ar likumu (nelikumīga bezdarbība). Ministru kabinets pēc EM ieteikuma ieceļ PTAC direktoru uz piecu gadu termiņu. Saskaņā ar Patērētāju tiesību aizsardzības likumu PTAC lēmumus var apelēt tiesā saskaņā ar Administratīvo procedūru likumā norādītajām procedūrām.

PTAC galvenais uzdevums ir īstenot patērētāju tiesības un intereses. Tās pienākumi iekļauj atsevišķu patērētāju sūdzību izskatīšanu, tirgus novērošanu lielākajai daļai nepārtikas produktu un patērētāju likumu un noteikumu īstenošanu. Papildu tiesībaizsardzības iestādes papildina PTAC konkrētās jomās, tostarp DVI, kas ir atbildīga par personas datu aizsardzību, un dažas nozaru specifiskās ministrijas, kurām ir īpašs budžets un personāls patērētāju aizsardzībai.

PTAC ir plašas regulatīvās pilnvaras (skatiet 5.7. ielikums), tostarp iespēja pieprasīt uzņēmumiem publicēt attiecīgo informāciju, ja ir pārkāptas patērētāju tiesības, piemēram, nepareizas vai maldinošas produktu informācijas, negodīgas komercprakses vai bīstamu produktu gadījumā.

5.7. ielikums. PTAC galvenās izpildes pilnvaras

- Pieprasīt no uzņēmumiem, valsts, pašvaldības institūcijām un fiziskām vai juridiskām personām visu informāciju, kas PTAC ir nepieciešama, lai izpildītu savas funkcijas.
- Lūgt uzņēmumiem veikt brīvprātīgas darbības paredzētajā laika periodā, lai nodrošinātu komercprakses atbilstību likuma un regulatīvajām prasībām, piemēram, izbeigtu nelikumīgu komercpraksi.
- Pieprasīt uzņēmumiem publicēt attiecīgu informāciju, ja ir pārkāptas patērētāju tiesības, piemēram, nepareizas vai maldinošas produktu informācijas, negodīgas komercprakses vai bīstamu produktu gadījumā.
- Apmeklēt jebkuru ēku, telpu vai vietu, kur tiek ražotas, glabātas vai tirgotas preces, kas neatbilst patērētāju tiesību aizsardzības politikai un likumam, vai tiek sniegti neatbilstīgi pakalpojumi; apmeklēt jebkuru vietu, kur tiek izmantoti, ražoti, remontēti vai pārdoti mērinstrumenti.
- Pieprasīt un saņemt tādu preču paraugus, par kurām ir aizdomas, ka tās pārkāpj patērētāju tiesības saskaņā ar normatīvajos aktos noteiktajām procedūrām, lai veiktu laboratorijas vai citu speciālistu izmeklējumus.
- Pieprasīt preču izņemšanu no apgrozības vai pārtraukt pakalpojumu sniegšanu neatbilstības ar patērētāju aizsardzības politiku, regulu vai tehnisko standartu gadījumos.
- Pārtraukt izmeklēšanas laikā preču pārdošanu vai pakalpojumu sniegšanu, līdz tiek pieņemts lēmums, pamatojoties uz laboratorijas testēšanas rezultātu vai eksperta viedokli.
- Piemērot administratīvās sankcijas un soda naudas.

PTAC pašlaik ir 107 štata darbinieki, no kuriem vairākums ir iesaistīti patērētāju tiesību īstenošanā un produktu drošības jautājumos, iekļaujot preču un pakalpojumu uzraudzību, patērētāju tiesību aizsardzību, patērētāju konsultācijas un sūdzības, kā arī pārrobežu jautājumus. Daļu patērētāju likuma īstenošanas realizē DVI, it īpaši e-komercijas kontekstā. E-komercijas uzraudzību veic PTAC speciālās uzraudzības daļas ar atbalsta vienību palīdzību. 5.2. tabula ir norādīta budžeta un personāla resursu informācija par 2017.-19. gada periodu. [22]

Papildus PTAC informācijas pieprasīšanu un saņemšanu, kā arī administratīvo sankciju (soda naudu, aizliegumu) piemērošanu var veikt Valsts Veselības inspekcija (par veterināro un farmaceitisko pakalpojumu reklamēšanu) un Nacionālā elektronisko plašsaziņas līdzekļu padome (reklāmas). Gadījumos, kas ietver krimināpārkāpumus (piemēram, saistībā ar surogātpastu), var tikt iesaistīta Valsts policija.

5.2. tabula. PTAC budžets un personāls, 2017.-19. gads

	Budžets (EUR)	Personāls (bez ECC-Net)
2017	2 383 111	96
2018	2 895 983	107
2019	2 849 981	107

Avots: ESAO, pamatojoties uz PTAC datiem.

Pēdējo gadu laikā ir ievērojami pieaudzis PTAC saņemto patērētāju sūdzību skaits par distances līgumiem. Piemēram, 2017. gadā tika iesniegtas aptuveni 486 sūdzības, to apjomam pieaugot par vairāk nekā 200 % salīdzinājumā ar 2017. gadu, kad tika iesniegtas 222 sūdzības. PTAC ir izmeklējusi vairākas lietas un pieņēmusi lēmumus par patērētāju interešu aizsardzību, kā arī publicējusi norādes patērētājiem un brīdinājumus plašsaziņas līdzekļos, lai patērētājus informētu par problēmām, kas ir saistītas ar konkrētiem tiešsaistes mazumtirgotājiem un platformām.

5.3. tabula ir norādīti dati par PTAC iesniegtajām patērētāju sūdzībām laikā no 2017. gada līdz 2019. gada jūnijam.

5.3. tabula. PTAC saņemtās un atrisinātās patērētāju sūdzības laikā, 2017. g. – 2019. g. jūnijs

	Saņemtās sūdzības	Atrisinātās sūdzības
2017	3 616	958
2018	3 604	1 002
2019. g. (līdz 30. jūnijam)	1 940	405

Avots: ESAO, pamatojoties uz PTAC datiem.

Piemērošana

PTAC regulāri apņemas veikt īstenošanas darbības e-komercijas kontekstā. Papildus regulatīvajām pilnvarām, kas aprakstītas 5.7. ielikums, PTAC var likt tīmekļa vietnēs bloķēt nelikumīgu saturu, kas ir kaitīgs bērniem, tostarp no pakalpojumu sniedzējiem, kas ir reģistrēti ārpus Eiropas Savienības. Daudzos gadījumos PTAC īstenošanas darbības ir saistītas ar negodīgu komerciālo praksi e-komercijā.

Ar kriminālu krāpšanu saistītās sūdzības parasti tiek nosūtītas Valsts policijai, lai tā veiktu attiecīgu izmeklēšanu un pārbaudes ar kriminālprocesuālu darbību palīdzību. Dažas no sūdzībām attiecās uz tiešsaistes mazumtirgotājiem, kuri nepiegādāja produktus vai neizmaksāja kompensāciju patērētājiem. 5.4. tabula ir norādīti dati par sūdzībām, kas saņemtas no 2017. gada līdz 2019. gada jūnijam.

5.4. tabula. Ar e-komerciju saistītās sūdzības, 2017. g. – 2019. g. jūnijs

	Iesaistītie uzņēmumi	Saņemtās patērētāju sūdzības	Lēmums
2017	6 tiešsaistes mazumtirgotāji	196	Nodots Valsts policijai
2018	3 tiešsaistes mazumtirgotāji	252	Nodots Valsts policijai
2019. g. (līdz 30. jūnijam)	1 izklaides pasākums	105	Nodots Valsts policijai

Avots: ESAO, pamatojoties uz PTAC datiem.

Negodīga komercprakse tiek uzskatīta par kolektīvo patērētāju interešu pārkāpumu un to īsteno ar kolektīvām patērētāju darbībām (izmantojot administratīvo tiesvedību). Atsevišķas patērētāju sūdzības nevar atrisināt ar šādu kolektīvu rīcību, tomēr PTAC ir kompetents iejaukties un pārtraukt šīs komercdarbības, pārkāpjot patērētāju tiesību aktus. To var izdarīt pēc brīvprātības principa ar brīvprātīgu pārkāpumu pārtraukšanu vai apņemšanos, vai pieņemot administratīvus lēmumus. Uzņēmumu apņemšanās un PTAC administratīvos lēmumus var izmantot kā pierādījumus patērētāji, kuri meklē kompensāciju tiesā vai iesaistās alternatīvā strīdu atrisināšanā. Tomēr ne visas patērētāju sūdzības izraisa kolektīvas darbības (piemēram, viena kolektīvā lieta var saturēt vairākas patērētāju sūdzības, patērētāja sūdzība par pārkāpumu var netikt uzturēta vai kolektīvā lieta var būt ierosināta pirms patērētāja sūdzības).[23]

Kaut arī nav pieejama specifiska statistika par negodīgu praksi e-komercijā, 5.5. tabula ir norādītas sūdzību darbības saistībā ar dažādu veidu komercpraksi, no kurām dažas ir saistītas ar e-komerciju.

5.5. tabula. Oficiālās patērētāju sūdzības par negodīgu komercpraksi laikā 2017. g. – 2019. g. jūnijs

	Sūdzības
2017	204
2018	279
2019. g. (līdz 30. jūnijam)	197

Avots: ESAO, pamatojoties uz PTAC datiem.

Pagaidām nav pieejama arī specifiska oficiālā statistika par nelikumīgu praksi e-komercijā. 5.6. tabula ir redzama iekšējā lietu izskatīšanas informācija ("Uzraugs"), kas tiek glabāta PTAC iekšējā datubāzes sistēmā.

5.6. tabula. Nelikumīgas e-komercijas prakses, 2017. g. – 2019. g. jūnijs

	Sāktās administratīvās lietas (saistībā ar tiešsaisti)	PTAC aicinājumi uz brīvprātīgu pārtraukšanu (saistībā ar tiešsaisti)	Saņemtās rakstveida apņemšanās (saistībā ar tiešsaisti)	Pieņemtie administratīvie lēmumi (saistībā ar tiešsaisti)	Piemērotie sodi, EUR (saistībā ar tiešsaisti)
2017	99	50	8	12	85 000
2018	177	149	1	18	194 900
2019. g. (līdz jūnijam)	71	39	2	6	52 570

Piezīme: PTAC = Patērētāju tiesību aizsardzības centrs.

Avots: ESAO, pamatojoties uz PTAC datiem.

Uzraudzība un novērtēšana

Patērētāju aizsardzības īstenošana e-komercijas kontekstā ir novērtēta ziņojumā, ko PTAC katru gadu iesniedz EM.[24] PTAC 2018. gada ikgadējā ziņojumā[25] tika iekļauti vairāki interesanti ieskati, statistika un informācija par e-komercijas jomā veiktajām īstenošanas darbībām. Piemēram, attiecībā uz godīgu cenu noteikšanas praksi un distances līguma noteikumiem no tiešsaistes mazumtirgotājiem ziņojumā ir norādīts, ka "tika pārbaudīti 25 no populārākajiem interneta veikaliem un ierosinātas 25 administratīvās lietas", kam sekoja pārkāpuma brīvprātīga pārtraukšana.

Vēl viens noderīgs uzraudzības instruments ir interneta pārbaude,[26] ko organizē Eiropas Komisija un Starptautiskais patērētāju tiesību aizsardzības un īstenošanas tīkls (*ICPEN*) kā līdzekli ES patērētāju aizsardzības likuma realizēšanai. Pārbaudes ir veiktas dažādās jomās, iekļaujot digitālos produktus, tiešsaistes lidsabiedrību biļešu pārdošanu un bērniem paredzētas tiešsaistes spēles. Rezultāti sniedz noderīgu informāciju par patērētāju aizsardzības tiesību aktu iespējamiem pārkāpumiem un palīdz Latvijai novērtēt jautājuma nopietnību, kā arī patērētāju politikas ieviešanas efektivitāti valstī.

Izglītība un informētība

PTAC regulāri informē patērētājus par veidiem, kā droši iepirkties tiešsaistē, gan reaģējot uz žurnālistu jautājumiem, gan arī caur sociālo tīklu kanāliem. PTAC uztur tīmekļa vietni,[27] lai patērētājus informētu par iespējamiem riskiem, kas ir saistīti ar maldinošu un krāpniecisku komercpraksi, ko īsteno specifiski tiešsaistes veikali un platformas.

Turklāt PTAC ir izstrādājis kontrolsarakstu[28] ar ieteikumiem un noderīgu informāciju patērētājiem, kad viņi pieņem lēmumu par to, vai iepirkties tiešsaistes veikalā.

Turklāt PTAC ir izplatījis informāciju (video, gif, infografiku), ko nodrošina Eiropas Patērētāju centru tīkls (*ECC-Net*) par abonēšanas lamatām un iepirkšanos tiešsaistē. 2018. gadā PTAC sadarbojās ar Patentu biroju kampaņā par viltotām precēm.

2019. gadā PTAC piedalījās valdības institūciju atvērto durvju dienā.[29] Augstskolas studenti apmeklēja PTAC un piedalījās dažādās aktivitātēs, ieguva informāciju par drošu iepirkšanos tiešsaistē un nedrošu preču atpazīšanu, kā arī uzzināja par patērētāju tiesībām ne tikai Latvijā, bet arī ES.

PTAC ir ļoti aktīvi atbalstījis patērētāju tiesības sociālajos tīklos. 2019. gada Valentīna dienā tas uzsāka kampaņu par to, kā izvēlēties interneta iepazīšanās tīmekļa vietni.[30] Turklāt PTAC regulāri internetā (savā tīmekļa vietnē) publicē informāciju par patērētāju tiesību aizsardzību.

Papildus patērētāju izglītošanai PTAC ir iesaistījies patērētāju tiesību veicināšanā attiecībā uz e-komercijas darbībās iesaistītajiem uzņēmumiem. It īpaši PTAC ir izlaidis nesaistošas vadlīnijas, lai uzņēmumiem palīdzētu interpretēt likumdošanas aktus, it īpaši koncentrējoties uz elektronisko sakaru pakalpojumu tirgiem, līgumu noteikumiem un nosacījumiem e-komercijā, grupu pirkumiem, kā arī paziņojumu un rīcības procedūrām, lai panāktu brīvprātīgu pārkāpumu pārtraukšanu tīmekļa vietnēs.

2015. gada septembrī PTAC publicēja paketi *Vadlīnijas godīgas komercprakses īstenošanai bērniem paredzēto tiešsaistes spēļu jomā*.[31] Iestāde sadarbojās ar Eiropas Komisiju un Dāniju attiecībā uz pirkumiem lietotnēs, koncentrējoties uz bērnu spēļu mobilajām lietotnēm, un rezultāti tika iekļauti Vadlīnijās.

Arī nacionālās NVO aktīvi iesaistās patērētāju aizsardzības veicināšanā e-komercijas kontekstā. Piemēram, Latvijas Interneta asociācija[32] organizē iniciatīvas, lai uzlabotu informētību par interneta drošību, tostarp e-komercijas kontekstā. LIKTA[33] sadarbībā ar EM ir organizējusi vairākas aktivitātes, tostarp seminārus par e-komerciju un e-pakalpojumiem, organizējusi e-komercijas informācijas dienu un izveidojusi e-komercijas balvu labākajam e-komercijas pārdevējam. Turklāt NVO ir svarīga loma ar negodīgu komercpraksi saistīto tiesību aktu īstenošanā e-komercijas kontekstā, regulāri informējot PTAC par iespējamiem pārkāpumiem.

Turklāt LIKTA veicina e-prasmes, kā arī informētību tiešsaistes drošības jautājumos. Vairāk nekā 180 000 cilvēku visā Latvijā ir piedalījušies tās apmācības iniciatīvā *Latvija@Pasaule* kopš 2005. gada, kas piedāvā apmācību un sertifikāciju, un ir izstrādājuši dažādus apmācību projektus e-prasmēm un iekļaujošai apmācībai.

Domstarpību izšķiršana un tiesību atjaunošana

Latvijas politikas mērķis strīdu izšķiršanā un tiesiskajā aizsardzībā (*DRR*) ir sniegt patērētājiem iespēju izmantot savas tiesības, noslēdzot līgumus ar ražotājiem, tirgotājiem vai pakalpojumu sniedzējiem un nodrošināt patērētājiem piekļuvi godīgai un efektīvai *DRR*, rīkojoties individuāli vai kolektīvi gan Latvijā, gan arī saistītās pārrobežu domstarpībās.

Domstarpības, ko nevar atrisināt uzņēmuma un patērētāja starpā, tiek izskatītas civiltiesās vai strīdu alternatīvās izšķiršanas (SAI) struktūrās. SAI galvenās institūcijas ir PTAC un Sabiedrisko pakalpojumu regulēšanas komisijas (SPRK), kā arī privātas SAI organizācijas.

PTAC iekļauj nacionālu SAI kontaktpunktu un uztur SAI institūciju sarakstu, kā arī Patērētāju sūdzību komiteju (PSK).

PSK tika izveidota līdz ar jaunākajiem Patērētāju tiesību aizsardzības likuma grozījumiem saskaņā ar ES direktīvu 2013/11/ES par alternatīvu strīdu izšķiršanu patērētāju strīdos. PSK rīkosies pēc PTAC pilnvarām un atrisinās patērētāju un tirgotāju (uzņēmumu) savstarpējos strīdus. PSK veidos trīs vai vairāk komitejas biedri, pēc vienlīdzības principiem pārstāvot ekspertus no patērētāju un tirgotāju NVO ar vienu neatkarīgu pārstāvi.

Latvijas *Patērētāju ārpustiesas strīdu risināšanas likums*[34] ir bijis spēkā kopš 2015. gada jūlija. Likumā ir izklāstīti noteikumi ārpustiesas strīdu risināšanas organizācijām, kas nodrošina, ka patērētāji var publicēt un aizsargāt savas likumīgās tiesības, iesniedzot sūdzības pret uzņēmumiem un vienlaikus piedāvājot neatkarīgas, objektīvas, caurskatāmas, efektīvas, ātras un godīgas ārpustiesas strīdu izšķiršanas procedūras. Likums attiecas uz SAI juridiskajām personām un procedūrām iekšzemes un pārrobežu strīdu izšķiršanā attiecībā uz līgumsaistībām. Turklāt likumā ir norādīti konkrēti noteikumi un atbildība (pienākumi) SAI juridiskajām personām un piemērotas procedūras, iekļaujot struktūru SAI juridisko personu savstarpējai sadarbībai, kā arī sadarbībai starp SAI un citām institūcijām. Likums

neattiecas uz procedūrām pie strīdu izšķiršanas organizācijām, kad par strīdu izšķiršanu atbildīgās fiziskās personas nodarbina vai atalgo tikai atsevišķs tirgotājs; uz procedūrām patērētāju sūdzību izskatīšanas sistēmās, ko izmanto tirgotājs; uz tiešām pārrunām patērētāja un tirgotāja starpā; uz procedūrām, kuras tirgotājs ir sācis pret patērētāju; uz tirgotāju savstarpējiem strīdiem; uz strīdiem saistībā ar veselības aprūpes pakalpojumiem, kurus veselības aprūpes speciālisti sniedz pacientiem, lai novērtētu, uzturētu vai atjaunotu viņu veselības stāvokli, iekļaujot medicīnas produktu un medicīnas ierīču izrakstīšanu, izsniegšanu un nodrošināšanu; uz strīdiem par tālākizglītības vai augstākās izglītības publiskiem pakalpojumu sniedzējiem; uz strīdiem saistībā ar rīcību vai nolaidību no zvērināto notāru vai tiesas izpildītāju puses.

Ministru kabineta noteikumi 631/2008[35] regulē procedūras patērētāju prasījumu iesniegšanai par līguma noteikumiem neatbilstošu preci vai pakalpojumu.

Eiropas Parlamenta un Padomes Regulā (EK) 861/2007[36] ir noteikta Eiropas mazo prasījumu procedūra, kas ir paredzēta izmaksu samazināšanai, kā arī tiesvedības vienkāršošanai un paātrināšanai saistībā ar mazajiem prasījumiem pārrobežu lietās. Latvijā prasījumus par nelielām summām var iesniegt saskaņā ar Latvijas Civilprocesa kodeksu,[37] kas paredz vienkāršotu procesu attiecībā uz prasībām, kuru summa ir mazāka par 2100 EUR.

Īstenošana un piemērošana

EM[38] ir svarīga loma Latvijas DRR politikas īstenošanā, cieši sadarbojoties ar citām ministrijām un iestādēm, piemēram, Valsts Veselības inspekciju, Valsts Pārtikas un veterināro dienestu un SPRK, kā arī NVO.

Saskaņā ar noteikumiem par strīdu izšķiršanas procedūrām, kas ir ietverti Patērētāju tiesību aizsardzības likumā (26. sadaļā), patērētājiem ir vispirms jāiesniedz prasība uzņēmumam, lai meklētu tiešu izlīgumu. PTAC un citas institūcijas sniedz konsultācijas patērētājiem par viņu tiesībām īpašās situācijās un attiecīgām darbībām, lai pieprasītu atlīdzību. Konsultācijas var organizēt pa tālruni, e-pastu un klātienē PTAC telpās. Aptuveni 40-45 % no sākotnējām prasībām var atrisināt ar šādu samierināšanās procedūru palīdzību. Ja tiešās sarunās nevar panākt risinājumu, patērētājiem ir vairākas citas iespējas.

Ja patērētājs iesniedz prasību PTAC un uzņēmumā nevar panākt risinājumu, var sākt strīdu izšķiršanas procedūru saskaņā ar Ministru kabineta 613. regulējumu, kuru ievērojot, PTAC sasaistās tieši ar uzņēmumu, lai panāktu risinājumu. Tas var iekļaut administratīvu procedūru un saistošu lēmumu. Šādas administratīvas procedūras, ko veic valsts institūcijas, neparedz nekādas izmaksas patērētājiem, un atbildīgās institūcijas pienākums tiesā (ja lēmums tiek pārsūdzēts tiesā) ir ievākt nepieciešamo informāciju un pierādījumus strīdu atrisināšanai.

Vairākas nozares Latvijā nodrošina savus strīdu izšķiršanas mehānismus. PSK, kas darbojas PTAC pārvaldībā un iekļauj privātā sektora pārstāvību, ir izveidojis alternatīvu strīdu izšķiršanas organizāciju.

Sistemātiski tiek ievāktas patērētāju sūdzības, un tās tiek izskatītas pēc produkta kategorijas un patērētāju aizsardzības jautājuma. Turklāt PTAC, citas valdības aģentūras un NVO veic uzraudzības darbības, lai regulāri analizētu tirgus tendences. PTAC organizē dažādas informētības kampaņas, tostarp sadarbībā ar valsts uzņēmumiem un NVO, lai palīdzētu patērētājiem ar DRR.

Patērētāju tiesību aizsardzības likumā (22. un 23. sadaļā) ir norādītas nevalstisko patērētāju organizāciju tiesības aizstāvēt patērētāju intereses un piedalīties lēmumu pieņemšanā. Turklāt saskaņā ar Ministru kabineta noteikumiem Nr. 300 *Ministru kabineta kārtības rullis*[39] nevalstiskajām ieinteresētajām pusēm ir jābūt iesaistītām likumprojektu un politikas plānošanas dokumentu sastādīšanā. Patērētāju NVO ir arī tiesības izmeklēt patērētāju sūdzības, palīdzēt patērētājiem tiesvedībāun pārstāvēt patērētāju intereses valsts tiesās. NVO darbs tiek uztverts kā svarīgs avots informācijai par attīstību patērētāju tirgos, iekļaujot patērētāju tiesību potenciālus vai faktiskus pārkāpumus. 5.7. tabula ir parādīta statistika par patērētāju iekšzemes un pārrobežu strīdiem.

Iepriekš minētā informācija norāda, ka Latvijas datu ievākšanas un analīzes sistēma pēdējo gadu laikā ir uzlabojusies, un PTAC tagad var nodalīt iekšzemes krāpšanas un pārrobežu lietas.

5.7. tabula. Iekšzemes un pārrobežu patērētāju strīdi

	Iekšzemes lietas			Pārrobežu lietas ECC-Net		
	Strīdi	Tiesību atjaunošana[1]	Atrisinātās[2]	Strīdi	Tiesību atjaunošana[1]	Atrisinātās[2]
2017	1929	-	595	634	-	285
2018	1976	-	707	489	-	203
2019. gads (līdz 30. jūnijam)	1132	-	203	235	-	172

1. "Atrisināta" nozīmē to, ka ir panākta pušu savstarpējā vienošanās (tomēr ne obligāti tiesību atjaunošana).
2. PTAC nav pieejama informācija par tiesību atjaunošanu.

Avots: PTAC.

Likumu piemērošana attiecībā uz surogātpastu

Latvijas politikas mērķis attiecībā uz surogātpastu ir veicināt godīgu komercpraksi un nodrošināt personas datu apstrādes noteikumu ievērošanu komerciālās komunikācijas kontekstā. Komerciālā komunikācija iekļauj automātiskus zvanus, e-pastu un faksu, kas tiek nosūtīts fiziskām personām bez viņu tiešas piekrišanas. Personas datu apstrādes noteikumi aptver kontaktinformāciju, kuru var ievākt pakalpojumus sniedzējs, it īpaši iekļaujot gadījumus, kad šāda apstrāde tiek veikta nolūkos, kas nav komercdarījums, kura nolūkā dati tika ievākti.

Tiesiskais regulējums

Vispārīgās prasības par informāciju, kas ražotājiem vai pakalpojumu sniedzējiem (uzņēmumiem) ir jāsniedz patērētājiem, ir noteiktas *Patērētāju tiesību aizsardzības likumā*. *Negodīgas komercprakses aizlieguma likums* regulē komercprakses, kas ir maldinošas, agresīvas vai nekompetentas profesionālās uzcītības ziņā. *Personas datu apstrādes likums* nodrošina personas datu aizsardzības principus un regulējumu, it īpaši attiecībā uz nevēlamu komerciālu ziņojumu vai surogātpasta sūtīšanu, ko var uzskatīt par pārkāpumu. *Informācijas tehnoloģiju drošības likuma*[40] galvenais mērķis ir uzlabot informācijas tehnoloģiju drošību. Likumā ir norādītas svarīgākās prasības, lai garantētu ar šādu tehnoloģiju starpniecību nodrošināto svarīgo pakalpojumu saņemšanu. Ar to tiek izveidota arī Latvijas Informācijas tehnoloģiju drošības incidentu reaģēšanas vienība (CERT.LV)[41] — institūcija, kuras pilnvaras iekļauj valsts un pašvaldību varas iestāžu informācijas tehnoloģiju drošības uzraudzību un pārvaldību, kas var iekļaut surogātpasta apkarošanu.

Vairāk detalizēti noteikumi par personas datu aizsardzību un nevēlamas komerciālās komunikācijas aizliegumiem ir ietverti *Informācijas sabiedrības pakalpojumu likumā*. Ar šo likumu tiek aizliegta automatizēta komerciālā komunikācija, ja tās adresāts nav sniedzis iepriekšēju, brīvu un skaidri formulētu piekrišanu, turklāt šādā komunikācijā ir jāiekļauj iespēja, ka adresāts var to noraidīt. Šīs juridiskās saistības attiecas arī uz automātiskām zvanu sistēmām, kas darbojas bez cilvēka iejaukšanās, iekļaujot e-pastu un faksu. Turklāt likumā ir norādīti nosacījumi, ar kuriem pakalpojumu sniedzējs, kurš ir ieguvis elektroniskā pasta adreses no patērētājiem komerciālo darījumu kontekstā, var šādas adreses izmantot citai komerciālai komunikācijai. Tie iekļauj šos apstākļus: 1) komerciālā komunikācija attiecas uz līdzīgiem pakalpojumu sniedzēja produktiem vai pakalpojumiem; 2) klients nav iebildis pret turpmāko e-pasta ziņojumu saņemšanu; 3) klientam ir sniegta skaidra, noteikta bezmaksas iespēja noraidīt turpmākos e-pasta ziņojumus.

Izpildes pilnvaras

Divas galvenās institūcijas, kuru pienākumi un pilnvaras ir saistītas ar surogātpastu, ir DVI un PTAC. Abas iestādes var pieprasīt un saņemt informāciju, īstenot likumīgos pienākumus un piemērot administratīvās sankcijas (soda naudas un aizliegumus). Turklāt Latvijas Valsts policija[42] (Iekšlietu ministrija) var iesaistīties, ja surogātpasta lietas ir saistītas ar kriminālpārkāpumiem, un CERT.LV var iejaukties, ja lietas ietekmē informācijas sistēmu un tīklu drošību. Ar patērētāju aizsardzību saistītie uzņēmumi un NVO sekmē uz surogātpastu attiecināmo tiesību aktu īstenošanu, tostarp informējot atbildīgo uzraudzības iestādi par iespējamiem pārkāpumiem.

Ja kāda uzraudzības iestāde konstatē likumpārkāpumu, tai ir tiesības: 1) pieprasīt visu informāciju, kas ir nepieciešama lietas apstākļu noskaidrošanai; 2) likt pakalpojumu sniedzējam pārtraukt likuma pārkāpšanu un norādīt laika periodu, kurā uzņēmumam ir jānodrošina atbilstība likumam.

Lai izvairītos no interešu konflikta, PTAC darbības strīdu novēršanā tiek nodalītas no izpildes darbībām. Strīdu izšķiršanu veic patērētāju konsultāciju un sūdzību daļa, un tiesībaizsardzību realizē patērētāju tiesību aizsardzības daļa.

Pārrobežu sadarbība

Latvijas tiesībaizsardzības iestādes surogātpasta jautājumos sadarbojas ar ārvalstu (galvenokārt Eiropas) tiesībaizsardzības iestādēm surogātpasta jautājumos. It īpaši saskaņā ar *Informācijas sabiedrības pakalpojumu likumu* PTAC sadarbojas ar iestādēm no Eiropas Ekonomikas zonas (EEZ) valstīm. Turklāt DVI piedalās ES dalībvalstu valsts iestāžu sadarbības tīklā saskaņā ar EK regulu 2006/2004[43] par sadarbību starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā. Šī sadarbība it īpaši ir saistīta ar surogātpasta lietām, kas ietver Personas datu aizsardzības likuma pārkāpumus.

Nav pietiekamas informācijas vai pierādījumu par pakāpi, kādā PTAC un DVI vērtē Latvijas surogātpasta politiku un ir veikušas atbilstīgus pasākumus un uzlabojumus, piemēram, uzlabotu sadarbību ar ārvalstu tiesībaizsardzības iestādēm ārpus EEZ.

PTAC nav konkrētas informācijas vai statistikas par surogātpastu vai saistītiem jautājumiem un tiesībaizsardzības darbībām. Datus par surogātpastu ievāc CERT.LV. Sadarbība starp aģentūrām, lai veiktu saistītās informācijas apmaiņu un analizētu šādus datus, varētu palīdzēt risināt patērētāju problēmas šajā jomā.

Divpusēja palīdzība un pārrobežu sadarbība

Pārrobežu krāpšanas gadījumi galvenokārt tiek izskatīti, PTAC piedaloties vairākos Eiropas un starptautiskajos tīklos, kas uzlabo informācijas apmaiņu un sadarbību tiesībaizsardzības jomā. PTAC ir daļa no Eiropas Tiesībaizsardzības aģentūru sadarbības tīkla, kas tika izveidots saskaņā ar *Patērētāju tiesību aizsardzības likuma regulu un tiek izmantots, lai risinātu kolektīvāa patērētāju lietas*. Latvija ir dalībniece arī EEK tīklā (ECC-Net),[44] kas aptver visu Eiropu un palīdz atrisināt atsevišķus pārrobežu strīdus ES. Četras PTAC ieceltas personas pašlaik strādā EKK tīklā. Labāko praksi un izpildes mehānismus izplata arī Eiropas Komisija un ES Padomes darba grupas..

Turklāt PTAC ir *ICPEN* dalībniece un piedalās ES un *ICPEN* pārbaudēs, lai novērstu pārrobežu pārkāpumus dažādās jomās, piemēram, saistībā ar tūrismu un pirkumiem lietotnēs. PTAC iesaistās arī Krāpšanas novēršanas mēnesī, ko koordinē *ICPEN*.

Latvijas ir parakstījusi vairākus divpusējus līgumus par pārrobežu krāpšanas apkarošanu. It īpaši PTAC ir parakstījis sadarbības līgumus ar Lietuvas un Igaunijas patērētāju aizsardzības un tirgus uzraudzības iestādēm. Kopīgas sanāksmes tiek noturētas vismaz vienreiz gadā, lai pārrunātu darba rezultātus un kopējās lietas, kā arī veiktu labākās pieredzes apmaiņu. 2011. gada septembrī PTAC parakstīja arī Kopīgā nodoma deklarāciju ar Izraēlas Rūpniecības, tirdzniecības un darba ministriju (*MoITAL*), lai sadarbotos saistībā ar tirgus uzraudzību un tiesībaizsardzību nepārtikas patērētāju produktu drošības jomā.

Latvijas patērētāji, kas ir saskārušies ar krāpšanu, kas saistīta ar citā valstī bāzētu uzņēmumu, var iesniegt sūdzību PTAC. Ja Latvijā tiek konstatēta ES pārrobežu pārkāpuma lieta, tad PTAC rīkojas saskaņā ar Regulu par sadarbību patērētāju tiesību aizsardzības jomā, nosūtot informācijas un/vai tiesībaizsardzības pieprasījumus citām ES tiesībaizsardzības aģentūrām. Ja pārkāpumu ir izdarījis uzņēmums, kas darbojas ārpus ES, tad PTAC var izmantot *ICPEN* sadarbības mehānismu. Patērētāji var arī iesniegt sūdzības e-patērētāju tīmekļa vietnē,[45] kas ir globāla sistēma sadarbībai pārrobežu lietās, kurās PTAC piedalās.

Noslēgums un politikas ieteikumi

Lodziņā 5.6 ir Latvijai piedāvāti ieteikumi, lai uzlabotu tās pierādījumu bāzi patērētāju politikas lēmumu pieņemšanai un patērētāju aizsardzību ES un ārpus tās.

5.8. Ielikums. ESAO ieteikumi Latvijai par patērētāju aizsardzības uzlabošanu

Latvijai ir jāapsver:

- e-komercijai specifisku patērētāju sūdzību datu izstrāde, lai labāku saprastu ar e-komercijas darījumiem saistīto patērētāju problēmu raksturu un mērogu (saskaņā ar ESAO E-komercijas rekomendācijas 53. sadaļu);
- patērētāju informētības uzlabošana ar e-komerciju saistītos jautājumos un viņu digitālās kompetences uzlabošana ar informētības programmām, paturot prātā dažādu grupu īpašās pamatvajadzības, piemēram, vecumu, ienākumus un lasītprasmi (saskaņā ar ESAO e-komercijas rekomendācijas 50.-51. sadaļu);
- valsts strīdu izšķiršanas un kompensācijas sistēmas efektivitātes novērtēšana, piemēram, izpētot patērētāju lietojumu un apmierinātību, kā arī neatrisinātu strīdu gadījumus;
- pārrobežu strīdu ārpus ES pierādījumu bāzes uzlabošana, kā arī pārrobežu sadarbība tiesībaizsardzības jomā ES un ārpus tās.

Atsauces

AM (2020), *Publiskais pārskats par CERT.LV uzdevumu izpildi: 2020. gada 1. ceturksnis* [CERT.LV Quarterly Public Review], Aizsardzības ministrija, Rīga, *https://cert.lv/uploads/parskati/CERT-LV_Q1_2020_pub.pdf*.

AM (2019), *Kiberdrošī bas stratēģija 2019.-2022. gadam* [Cyber Security Strategy 2019-2022], Aizsardzības ministrija, Rīga, *https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf*.

AM (2016), *Pārskats par kiberdrošī bas stratēģijas 2014-2018 īstenošanu viduspos mā* [Mid-term Review of the Implementation of the 2014-2018 Cyber Strategy], Aizsardzības ministrija, Rīga.

AM (2014), *Latvijas kiberdrošī bas stratēģija (2014-2018)* [Cyber Security Strategy of Latvia (2014-2018)], Aizsardzības ministrija, Rīga, *www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20%281%29.pdf*.

CERT.LV (2020), *CERT.LV reģistrētie incidenti no 01.01.2020. līdz 31.03.2020* (Incidents registered with CERT.LV from 01.01.2020. until 31.03.2020), *https://cert.lv/lv/2020/04/pieejama-statistika-par-2020-gada-1-ceturksni*.

CERT.LV (2018), *CERT.LV Public Performance Report*, Aizsardzības ministrija, Rīga, *https://cert.lv/uploads/cert-gada-parskats-2019.pdf*.

DVI (2020), *2019. gada darbī bas ziņojums* [Activity Report 2019], Latvijas Republikas Datu valsts inspekcija, Rīga, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

ELKM (Igaunija) (2019), *Cyber Security Strategy*, Ekonomikas lietu un komunikāciju ministrija, Tallina, *www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

ESAO (2016), *Consumer Protection in E-commerce: OECD Recommendation*, OECD Publishing, Parīze, *www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*.

ESAO (2015), *Digital Security Risk Management for Economic and Social Prosperity*, OECD Publishing, Parīze, *www.oecd.org/sti/ieconomy/digital-securityrisk-management.pdf*.

ESAO (2012), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, ESAO, Parīze, *www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf*.

ESAO (2002), *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, ESAO, Parīze, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0312*.

ESAO (1998), *Cryptography Policy: The Guidelines and the Issues: The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy*, OECD Publishing, Parīze, *https://dx.doi.org/10.1787/9789264162426-en*.

VARAM (2014), *Informācijas sabiedrī bas attīstī bas pamatnostādnes 2014-2020* [Information Society Development Guidelines 2014-2020], Vides aizsardzība un reģionālās attīstības ministrija, Rīga *www.varam.gov.lv/eng/darbibas_veidi/e_gov/?doc=13317*.

Piezīmes

Izraēla

Statistikas datus par Izraēlu sniedza, un par tiem atbild Izraēlas attiecīgās iestādes. Šo datu izmantošana ESAO neskar Golānas augstieņu, Austrumjeruzalemes un Izraēlas apmetņu statusu Rietumkrastā saskaņā ar starptautisko tiesību noteikumiem.

1. WannaCry ir ļaunprātīga programmatūra, kas ir izraisījusi ievērojamu kaitējumu organizācijām. Mirai inficē datorus ar robottīklu, kas pēc tam veic izkliedētā pakalpojumu atteikuma (DDoS) uzbrukumus.
2. Pirmā Datordrošības incidentu reaģēšanas vienība (*CSIRT*) Latvijā tika izveidota 2006. gadā un 2011. gadā kļuva par CERT.LV;
3. Digitālās drošības politika Latvijā aptver daudzas jomas, iekļaujot kiberkaru (AM), kibernoziegumus (IeM), telekomunikācijas (SM), finanšu sistēmu digitālo drošību (FM) un privātuma aspektus (TM).

4. Izņemot Latvijas Banku, kurai NITDP ir pastāvīgs pārstāvis.
5. Skatiet Eiropas Datu aizsardzības padomes jaunumu sadaļu, kas ir pieejama šeit: *https://edpb.europa.eu/news/national-news/2019/data-state-inspectorate-latvia-imposes-financial-penalty-7000-euros-against_en*. DSI preses izlaidums ir pieejams šeit: *www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-piemero-7000-eiro-lielu-naudas-sodu-internetveikalam-par-personas-datu-apstrades-parkapumiem*.
6. Papildinformācija, kas attiecas uz ziņošanu par datu pārkāpumiem un paziņojumu formātu, ir pieejama DVI tīmekļa vietnē: *www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana*.
7. Daži saistītie piemēri ir *Labākās pieredzes ceļvedis par privātuma programmu (PPP) pārvaldību (Practice Guide on Privacy Management Programs (PMP)*), kuru ir izstrādājis Honkongas Privātuma biroja Personas datu komisārs, akcentējot privātajam un publiskajam sektoram piemērojamo privātuma pārvaldības programmu prasības, kas ir pieejamas šeit: *www.pcpd.org.hk/pmp/pmp.html*. Līdzīgā veidā Singapūras Personas datu aizsardzības komisārs ir publicējis Ceļvedi datu aizsardzības pārvaldības programmas izstrādei, kas tika pārskatīts 2019. gada jūlijā un kura mērķis ir palīdzība *2012. gada personas datu aizsardzības akta* atbilstības nodrošināšanā; pieejams šeit: *http://bit.do/fp4*. Arī *Vadlīnijas privātuma pārvaldības programmas ieviešanai, lai nodrošinātu privātuma pārskatāmību Manitobas publiskajā sektorā (Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector)* tika sastādītas saskaņā ar dokumentu *Pārskatāmības tiesību iegūšana ar privātuma pārvaldības programmu (Getting Accountability Right with a Privacy Management Program)*, kuru kopīgi publicēja Kanādas Privātuma biroja komisārs un Albertas un Britu Kolumbijas Informācijas un privātuma biroju komisāri; pieejams šeit: *www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf*. Meksikas Datu aizsardzības aģentūra (INAI) 2018. gada augustā izstrādāja komplektu *Vadlīnijas datu aizsardzības pārvaldības programmām (Guidelines for Data Protection Management Programs)*, kas bija paredzēts publiskā sektora juridiskajām personām un satur norādes, pasākumus un rekomendācijas, lai ievērotu saistības, kas izklāstītas *Vispārīgajā likumā par personas datu aizsardzību publiskā sektora juridiskajām personām (General Law on Protection of Personal Data for Public Sector Entities)* un *Vispārīgajās vadlīnijās par personas datu aizsardzību publiskā sektora juridiskajām personām (General Guidelines on Personal Data Protection for the Public Sector)*. Dokuments spāņu valodā ir pieejams šeit: *http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4*
8. DVI rekomendācijas un vadlīnijas ir pieejamas šeit: *www.dvi.gov.lv/en/legal-acts/recommendations-and-guidelines*.
9. **data.gov.lv mērķis ir apkopot un laist apgrozībā valdības iestāžu un organizāciju ievāktos datus vienuviet publiskai izmantošanai, pamatojoties uz to, ka šie dati ir vērtīgi inovāciju attīstībai. Pieejams šeit: *https://data.gov.lv*.**
10. 1999. gada 18. marta *Patērētāju tiesību aizsardzības likumu* skatiet šeit: *https://likumi.lv/ta/en/id/23309-consumer-rights-protection-law*.
11. 2007. gada 22. novembra *Negodīgas komercprakses aizlieguma likumu* skatiet šeit: *https://likumi.lv/ta/en/en/id/167759-unfair-commercial-practices-prohibition-law*.
12. 2014. gada 20. maija regulējumu Nr. 255 *Noteikumi par distances līgumu* skatiet šeit: *https://likumi.lv/ta/en/en/id/266462-regulations-regarding-distance-contracts*.
13. 2004. gada 4. novembra *Informācijas sabiedrības pakalpojumu likumu* skatiet šeit: *https://likumi.lv/ta/en/en/id/96619-law-on-information-society-services*.
14. 2004. gada 28. oktobra *Elektronisko sakaru likumu* skatiet šeit: *https://likumi.lv/ta/en/id/96611-electronic-communications-law*.
15. Pieejams šeit: *www.dvi.gov.lv/en*.
16. 1999. gada 20. decembra *Reklāmas likumu* skatiet šeit: *https://likumi.lv/ta/en/en/id/163-advertising-law*.
17. *Maksājumu pakalpojumu un elektroniskās naudas likumu* skatiet šeit: *www.fktk.lv/texts_files/0_Law_Payment_Services_Electronic_Money.pdf*.
18. *Eiropas Parlamenta un Padomes regulu (ES) 2018/302, ar ko novērš nepamatotu ģeogrāfisko bloķēšanu un citus diskriminācijas veidus iekšējā tirgū klientu valstspiederības, dzīvesvietas vai uzņēmējdarbības veikšanas vietas dēļ*, skatiet šeit: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0302*.
19. *Eiropas Parlamenta un Padomes Regula (ES) 2017/2394 (2017. gada 12. decembris) par sadarbību starp valstu iestādēm, kas atbild par tiesību aktu izpildi patērētāju tiesību aizsardzības jomā,un ar ko atceļ Regulu (EK) Nr. 2006/2004*, skatiet šeit: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017R2394*.
20. Papildinformācija ir pieejama šeit: *www.em.gov.lv/en*.
21. Papildinformācija par PTAC ir pieejama šeit: *www.ptac.gov.lv/en/content/about-crpc*.
22. Pieejams šeit: *http://ptac.gov.lv/sites/default/files/01_tame_ptac_2018_01.pdf*.

23. Saņemtās rakstveida apņemšanās ir publicētas PTAC tīmekļa vietnē šeit: *http://ptac.gov.lv/lv/table/rakstveida-apnemsanas*. *PTAC pieņemtie administratīvie lēmumi ir publicēti PTAC tīmekļa vietnē šeit: http://ptac.gov.lv/lv/table/ptac-l-mumi*.
24. Pieejams šeit: *www.em.gov.lv/en*.
25. Pieejams šeit: *http://ptac.gov.lv/sites/default/files/gada-parskats-2018.pdf*.
26. Pieejams šeit: *https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/sweeps_en*.
27. Pieejams šeit: *www.ptac.gov.lv/lv/content/aizdomigo-interneta-vietnu-saraksts*.
28. Pieejams šeit: *www.ptac.gov.lv/lv/content/k-izv-l-ties-dro-u-i-veikalu*.
29. Papildinformācija ir pieejama šeit: *www.facebook.com/ptacgovlv/posts/1164183977095012*.
30. Papildinformācija ir pieejama šeit: *www.facebook.com/ptacgovlv/photos/a.274069902773095/1111458369034240/?type=3&theater*.
31. Pieejams šeit: *http://ptac.gov.lv/sites/default/files/docs/nr_19_vadlinijas_tiessaistes_speles_0.pdf*.
32. Papildinformāciju skatiet šeit: *www.lia.lv*.
33. Papildinformācija ir pieejama šeit: *https://likta.lv/en/home-en*.
34. 2015. gada 18. jūnija *Patērētāju ārpustiesas strīdu risinātāju likumu* skatiet šeit: *https://likumi.lv/ta/en/id/275063-law-on-out-of-court-consumer-dispute-resolution-bodies*.
35. Pieejams šeit: *www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._631_-_Consumer_Claims.doc*.
36. Pieejams šeit: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0861&qid=1408967394914&from=LV*.
37. Pieejams šeit: *https://likumi.lv/ta/en/id/50500-civil-procedure-law*.
38. Pieejams šeit: *www.em.gov.lv/en*.
39. Pieejams šeit: *https://likumi.lv/ta/en/id/190612-rules-of-procedures-of-the-cabinet-of-ministers*.
40. 2010. gada 10. novembra *Informācijas tehnoloģiju drošības likumu* skatiet šeit: *www.dvi.gov.lv/en/legal-acts/law-on-the-security-of-information-technologies*.
41. Pieejams šeit: *https://cert.lv/en*.
42. Pieejams šeit: *www.vp.gov.lv*.
43. Pieejams šeit: *https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32004R2006*.
44. Papildinformācija ir pieejama šeit: *www.ecclatvia.lv*.
45. Pieejams šeit: *www.econsumer.gov*.