SOCIETY. INTEGRATION. EDUCATION
Proceedings of the International Scientific Conference. Volume V, May 28th-29th, 2021. 318-329

INFORMĀCIJAS TEHNOLOĢIJU IZMANTOŠANA ATTĀLINĀTĀS SUPERVĪZIJAS PRAKSĒ: DATU DROŠĪBA

Use of Information Technologies in Supervision Remote Practice: Data Security

Kirils Dubiņins
Rīgas Stradiņa Universitāte, Latvija

Kristīne Mārtinsone
Rīgas Stradiņa Universitāte, Latvija

Abstract*. Provision of remote services became relevant all over the world, during the 2020 COVID-19 pandemic. Latvian supervisors were also forced to transfer their practice to the digital space as well. COVID-19 pandemic challenges opened a wider range of opportunities for improvement remote practice. Pandemic also highlighted the risks associated with lack of relevant competences. At the global level over the last decade, risks associated with remote counselling summarized in guidelines, providing professionals with examples of best practice. In Latvia, on other hand, such guidelines have not adopted yet.*

This study developed with the aim to find out the awareness of Latvian supervisors about the risks (cyber security) of using information technology and the protection of personal data in the conditions created by the COVID-19 pandemic.

To find out how Latvian supervisors are aware about the risks of using information technology (cyber security) and personal data protection, a survey conducted among Latvian supervisors and organizing an expert panel discussion, scientific strength of the study ensured by data triangulation.

The obtained results allowed to conclude that the COVID-19 pandemic highlighted the need for supervision remote practice, at the same time the research data show that the awareness of Latvian supervisors about the risks of information technology use (cyber security) and personal data protection is medium to low.

The results of the research show that in the education of Latvian supervisors it is necessary to allocate place for the acquisition of information technology (cyber security) risk and personal data protection regulation.

This research emphasizes the importance of several supervisors' competences such as digital knowledge and personal data protection, however further research is needed to find the most effective methods how to improve these competences.

Keywords: *COVID-19 pandemic, Cybersecurity, Personal Data protection, Remote practice, supervision, supervision competences.*

© Rēzeknes Tehnoloģiju akadēmija, 2021
https://doi.org/10.17770/sie2021vol5.6389

Ievads
Introduction

2020.gadā COVID-19 pandēmijas rezultātā izveidojās apstākļi (ierobežojumi) (Ministru kabinets, 2020, 216A), kad tiešie (klātienes) kontakti ar citām personām tika būtiski ierobežoti vai pat neiespējami, kas, savukārt, radīja unikālu situāciju, kad attālinātā prakse kļuva par vienīgo iespēju nodrošināt supervīziju, proti, sniegt konsultatīvu atbalstu jautājumos, kas saistīti ar darbu un profesionālo darbību (Profesionālās izglītības un nodarbinātības trīspusējās sadarbības apakšpadome (PINTSA), 2019). Attālinātā prakse jeb attālinātā supervīzija tiek īstenota, izmantojot informācijas tehnoloģijas, proti, metožu un instrumentu kopumu – attēlu, teksta, skaņas un informācijas apstrādei, iegūšanai, uzglabāšanai un izplatīšanai ar datoru un telesakaru kombināciju (Nipers, Zīds, & Kuklis, 2012). Attālinātai praksei, izmantojot informācijas tehnoloģijas, būtu jāatbilst tiem pašiem profesionālajiem standartiem, kas ir noteikti klātienes praksei (Joint Task Force for the Development of Telepsychology Guidelines for Psychologists (APA), 2013).

Attālinātā prakse aktualizē vairākus profesionālo zināšanu, prasmju un attieksmju jautājumus – līdzās jau minētajai informācijas tehnoloģiju izmantošanai, supervizoram jāspēj ievērot arī personas datu aizsardzības normas attālinātās prakses procesā, nodrošināt dokumentu apriti normatīvajos aktos paredzētajā kārtībā (PINTSA, 2019). Lūkojoties plašākā kontekstā, jānorāda, ka šīs prasības sasaucas ar Nacionālās attīstības plānu, kurš nosaka, ka nākotnē turpināsies digitalizācijas attīstība, kura kļūšot par vienojošu elementu, īpaši tādās jomās kā inovācijas un zinātne, izglītība un veselības aprūpe (LR Saeima, 2020, 127). Digitālo transformāciju pamatnostādnes arī izvirza digitālo kompetenci kā vienu no mūžizglītības pamatkompetenču daļu un sevī ietver informācijas tehnoloģiju pārliecinātu, kritisku un atbildīgu izmantošanu un darbošanos ar šīm tehnoloģijām mācību un darba vajadzībām (Vides aizsardzības un reģionālās attīstības ministrija (VARAM), 2020). Attiecībā uz supervizora darbu tas nozīmē, ka supervizoram būs jāspēj apgūt un izmantot jaunākās informācijas tehnoloģijas profesionālās darbības veikšanai, kas jau šobrīd ir noteikts supervizora profesijas standartā (PINTSA, 2019).

Svarīgi, lai supervizējamais (supervīzijas klients, pasūtītājs) tiek atbilstoši informēts un izglītots par informācijas tehnoloģiju izmantošanas riskiem attālinātā supervīzijā. It īpaši uzsverot, ka daļai Latvijas supervizoru izglītība tiek iegūta pedagoģijā (Angena & Mārtinsone, 2020), tādējādi supervizoriem, sniedzot konsultatīvu un izglītojošu atbalstu, ne tikai ir jāstrādā atbilstoši profesijas standartā noteiktām kompetencēm (PINTSA, 2019), nodrošinot drošu supervīzijas vidi izmantojot informācijas tehnoloģijas, bet arī jāspēj sniegt atbilstošu informāciju saviem klientiem. Līdz ar to jāspēj "pilnvērtīgi izmantot

digitālās telpas, rīkus un ar to saistīto procesu iespējas, sekmējot sabiedrības spēju efektīvi rīkoties, lai atbildētu mūsdienu izaicinājumiem" (VARAM, 2020).

Izmantojot informācijas tehnoloģijas supervīzijas praksē, speciālistiem ir svarīgi apzināties specifiskos un unikālos riskus, ko rada šo tehnoloģiju izmantošana, jeb kiberdrošības riskus, kuri ir neatņemama informācijas tehnoloģiju izmantošanas sastāvdaļa. Citu (sistēmu, tehnoloģiju, ierīču) kiberdrošības risku starpā īpaši jāizdala cilvēciskais faktors, kas izriet no kompetenču/zināšanu trūkuma (APA, 2013). Līdz šim supervizoru kompetences personas datu aizsardzības un informācijas tehnoloģiju (kiberdrošības) jomā nav pētītas. Tomēr tas ir īpaši aktuāli, ņemot vērā Nacionāla attīstības plāna prioritātes, kuru starpā ir izvirzītas digitālās un karjeras vadības prasmes, mediju un informācijas pratība (Ministru kabinets, 2020, 127).

American Psychological Association vadlīnijas iesaka speciālistiem pirms attālinātās prakses uzsākšanas pārliecināties par attālinātās prakses organizēšanas tiesisko pamatu, kā arī saņemt atbilstošas konsultācijas no datu aizsardzības un/vai tehnoloģiju drošības speciālistiem par attālinātās prakses organizēšanu, kā arī pārskatīt ar attālinātas prakses organizēšanu saistītos lietvedības/grāmatvedības aspektus (piemēram, rēķinu izrakstīšanas kārtību) (APA, 2013).

Vispārīgā datu aizsardzības regula nosaka, ka, "ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu un spētu uzskatāmi parādīt, ka apstrāde notiek saskaņā ar regulu." (Eiropas Parlaments un Padome, 2016, 119). Līdzās normatīvo aktu prasībām personas datu aizsardzības jomā, supervizora profesijas standarts paredz, ka supervizoram jānodrošina savas prakses atbilstību personas datu aizsardzības prasībām, noformējot atbilstošus dokumentus un korekti veicot ar personu datu aizsardzību saistīto dokumentu apriti (PINTSA, 2019). Minētais aktualizē nepieciešamību pēc attālinātās prakses tiesisko pamatu noskaidrošanas uz izzināšanas, it īpaši jautājumos, kas saistīti ar personas datu apstrādes procesu.

Atšķirībā no citām valstīm (piemēram, ASV), šobrīd Latvijā nav specifiska regulējuma (vadlīniju), kas iekļautu visu normatīvo aktu prasības vienotā normatīvā dokumentā un ļautu supervizoriem organizēt savu praksi atbilstoši profesionāliem standartiem un normatīvo aktu prasībām, ka arī līdz šīm netika veikti specifiski pētījumi, kas ļautu apzināties supervizoru izpratni par datu drošību un kopējo attālinātas supervīzijas prakses organizāciju, kas ir svarīgi lai izveidot gan profesionālas darbības vadlīnijas, gan profesionālas apmācības programmas, nodrošinot supervizoru profesionālo izaugsmi un kompetenču attīstību.

Pētījuma **mērķis** bija izzināt Latvijas supervizoru informētību par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem un personas datu aizsardzību COVID-19 pandēmijas radītājos apstākļos.

Atbilstoši pētījuma mērķim tika izvirzīti pētījuma **jautājumi**:

1. Kāda ir Latvijas supervizoru informētība par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem?
2. Kāda ir Latvijas supervizoru informētība par personas datu aizsardzību?

Metodoloģija
Metodology

Lai sasniegt pētījuma mērķi, tika izvēlēts secīgais izskaidrojošs jaukta tipa dizains. Šī darba īstenošana notika divos posmos – pētījuma sagatavošanas un pētījuma posmā.

Pētījuma sagatavošanas posmā, lai formulētu aptaujas jautājumus, vispirms, izmantojot juridiskās interpretācijas metodes, tika analizētas normatīvo aktu prasības datu aizsardzības jomā (Eiropas Parlaments un Padome, 2016, 119), normatīvo aktu prasības, kuros minēta supervīzija (Prasības sociālo pakalpojumu sniedzējiem (Ministru kabinets, 2017, 126), kā arī supervizora profesijas standarts (PINTSA, 2019). Ar mērķi iegūt plašāku izpratni par attālināto darbu, tika ņemtas vērā arī ar konsultatīvo atbalstu saistīto nozaru vadlīnijas, kas tiek pielietotas ārvalstu praksē, piemēram., ASV Psihologu asociācijas vadlīnijas attālinātai psiholoģiskai konsultēšanai (APA, 2013), piemēram – par rēķinu izrakstīšanas kārtību (minētās vadlīnijas iesaka šifrēt rēķinu saturu), par attālinātas prakses tiesiskā pamata noskaidrošanu pirms uzsākt šāda veida praksi utt., apzinoties, ka minētās vadlīnijas nav saistošas Eiropas savienībā.

Lai definētu aktuālus kiberdrošības riskus, izmantojot tematisko analīzi, tika izpētīti kiberdrošības ekspertu atzinumi un statistika (Verizon, 2019; PwC, 2018; Google/Harris Poll, 2019; Statista, 2017), kā arī informācijas tehnoloģiju un pasaulē atzīti kiberdrošības standarti (International Organization for Standardization, 2018, International Telecommunication Union, 2008). Balstoties uz starptautiski izmantoto incidentu taksonomiju jeb formalizētu veidu, kā apkopo, sadala kategorijās un reprezentē par apdraudējumiem iegūto tehnisko informāciju, tika veidoti aptaujas jautājumi (piemēram, par attālinātā praksē izmantotām ierīcēm un programmnodrošinājumu un to konfigurācijas īpatnībām – izmantotā operētājsistēma, izmantotās paroles, citu lietotāju piekļuves iespējas utt.).

Anketas jautājumi par attālinātas prakses organizēšanu (jautājumi par rēķinu izrakstīšanu, klientu informēšanu un attālinātās prakses dokumentācijas

noformēšanu) tika balstīti uz supervizora profesijas standartā noteiktajām kompetencēm (personas datu aizsardzības un informācijas tehnoloģiju izmantošanas jomā), kā arī no normatīvo aktu izrietošām prasībām, piemēram, Vispārīgas datu aizsardzības regulas ES 2016/679 7.panta pirmās daļas normām, kas nosaka, ka "personas datu apstrāde pamatojas uz piekrišanu un ir jāspēj uzskatāmi parādīt, ka datu subjekts ir piekritis savu personas datu apstrādei", kā arī uz minētā normatīvā akta 32.panta normu prasībām, kas nosaka, ka, "ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, jāīsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam". Pamatojoties uz minēto, tika formulēti aptaujas jautājumi (Eiropas Parlaments un Padome, 2016, 119).

Pētījuma posmu veido divas daļas – kvalitatīvā un kvantitatīvā. Vispirms tiks raksturota kvantitatīvā pētījuma daļa.

Instrumentārijs. Anketa, ko viedo četras daļas – pirmajā daļā ietverti jautājumi par sociāli demogrāfiskajiem rādītājiem – dzimums, vecums, supervīzijas prakses stāžs, bāzes izglītība (4 jautājumi), un jautājumi par supervīzijas praksi, tostarp, kādu supervīzijas veidu praktizē, kas veido supervīzijas klientu loku, cik daudz stundas mēnesī praktizē, kāda ir rēķinu izrakstīšanas kārtība (4 jautājumi); otrajā daļā – jautājumi par supervīzijas attālināto praksi pirms COVID-19 pandēmijas – cik lielu daļu no prakses sastādīja attālinātā prakse, kādu attālinātās prakses veidu izmantoja, kur praktizēja (4 jautājumi); trešajā daļā – jautājumi par supervīzijas attālināto praksi COVID-19 pandēmijas laikā – cik lielu daļu no prakses sastādīja attālinātā prakse, kādu attālinātas prakses veidu izmantoja, kur praktizēja, kas veido klientu loku (grupas, komandas, organizācijas, individuāli klienti) un kādu profesiju pārstāvji veido klientu loku (6 jautājumi); ceturtajā daļā – jautājumi par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem (11 jautājumi), un personas datu aizsardzību (10 jautājumi).

Anketā lielākoties tika izmantoti slēgta tipa jautājumi par informācijas tehnoloģiju izmantošanu un personas datu aizsardzību, un jautājumi ar Likerta skalu, kur respondentiem vajadzēja izvērtēt informācijas tehnoloģiju un personas datu aizsardzības jomā izmantotos jēdzienus un informētību par normatīvo aktu saturu (no 1 – nav informēts, līdz 5 – informēts).

Procedūra. Laikā no 2020.gada 4.oktobra līdz 4.decembrim respondentiem – Latvijas Supervizoru apvienības biedriem (ar biedrības valdes locekles piekrišanu) un supervīzijas studentiem no Rīgas Stradiņa universitātes un Biznesa mākslas un tehnoloģiju augstskola "RISEBA" tika nosūtīti e-pasti ar aicinājumu piedalīties pētījumā un lūgumu aizpildīt anketu. Anketēšana notika, izmantojot *Google Forms*. Tās aizpildīšanai nebija laika ierobežojuma, un kopējais anketas aizpildīšanas laiks sastādīja ~15 min. Anketas ievaddaļā tika

sniegta informācija par datu izmantošanas nosacījumiem un konfidencialitāti. Respondentiem tika nodrošināta iespēja vajadzības gadījumā sazināties ar pētījuma autoru (e-pastā).

Dalībnieki. 39 supervizori un supervīzijas studenti, no kuriem 5,1% (n=2) vīrieši un 94,9% (n=37) sievietes, respondentu vecums 45 gadi (kumulatīvi 51,3%). Respondentu supervīzijas prakses stāžs 4 līdz 6 gadi (kumulatīvi 71,8%). Respondentu bāzes izglītība – pedagoģijā 20,5% (n=8); uzņēmējdarbība un finanses 17,9% (n=7), sociālais darbs 17,9% (n=7) u.c. Visbiežāk respondenti 30,8% (n=12) praktizē individuālo un grupu supervīziju lielākā daļa 79,5% (n=31) respondentu praktizē individuālo supervīziju ar privātpersonām, 38,5 % (n=15) praktizē supervīziju mazāk par 8 stundām mēnesī, 35,9% (n=14) praktizē supervīziju no 9 līdz 18 stundām mēnesī. Tikai 7,7% (n=3) praktizē supervīziju 40 un vairāk stundas mēnesī.

Datu apstrāde. Kvantitatīvo datu apstrādei tika pielietota datorprogramma *IBM SPSS Statistics 21.0*. Tika apskatīta aprakstoša statistika (piemēram, procenti). Tā kā dati atbilst nominālai skalai, datu analīzei tika izmantota neparametriska statistika.

Kvalitatīvo pētījuma daļu veidoja supervīzijas nozares ekspertu paneļdiskusija par informētības līmeni par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem un personas datu aizsardzību. Paneļdiskusija tika veikta ar mērķi nodrošināt datu triangulāciju. Tajā piedalījās divi eksperti – supervizori ar profesionālās darbības stāžu vairāk nekā 5 gadi. Paneļdiskusijas analīzei tika izmantota tematiskā analīze pēc Braunas un Klārkas (Braun & Clarke, 2006) modeļa. Rezultātu pārskatā ir ietvertas vinjetes no šīs diskusijas.

Rezultātu analīze
Results analysis

Noslēdzoties anketēšanai tika iegūtas 39 pilnīgi aizpildītas anketas, to dati tika analizēti kopā ar ekspertu paneļdiskusijas laikā iegūtiem atzinumiem un tiek pasniegti sintezētā veidā.

Atbildot uz pētījuma jautājumu, kāda ir Latvijas supervizoru informētība par personas datu aizsardzību, konstatēts, ka attālinātās prakses datu apstrādes atbilstības novērtējumu neveica 68,4% (n=26) no respondentiem, 21,1% (n=8) no respondentiem sniedza atbildi, ka nezina, kas ir personas datu pārstrādes atbilstības novērtējums, un 10,5% (n=4) veica atbilstības novērtējumu. Jāmin, ka 7,9% (n=3) konsultējās ar personas datu aizsardzības un/vai tehnoloģiju drošības speciālistiem par attālinātās prakses organizēšanu, 65,8% (n=25) neveica konsultācijas, bet aplūkoja informāciju no publiskiem avotiem un 26,3% (n=10) neveica konsultācijas, jo nesaskatīja tajās vajadzību.

Rēķinu izrakstīšanas kārtību nepārskatīja 84,2% (n=32) no respondentiem, tomēr 15,8% (n=6) norādīja, ka sāka izrakstīt rēķinus elektroniskā formā, pirms COVID-19 pandēmijas to darīja 56,4% (n=22) no respondentiem. Neviens no respondentiem nav izmantojis šifrēšanu, nosūtot rēķinus elektroniski.

Atbildot uz jautājumu par vienošanas noslēgšanu, kur tiktu atrunāti datu apstrādes jautājumi un klientu piekrišanas datu apstrādei pirms uzsākt attālināto praksi, 65,8% (n=25) no respondentiem sniedza atbildi, ka nebija noslēguši rakstveida vienošanos (piemēram, līgumu), kur būtu atrunāti minētie jautājumi.

Respondenti dod priekšroku sinhronai multimediju jeb tiešsaistes attālinātās prakses formai, lielākā daļa no respondentiem (97,4% (n=37)) attālinātā praksē izmantoja *Zoom* platformu, tomēr, pirms izmantot programmnodrošinājumu attālinātā praksē, 63,2% (n=24) no respondentiem nebija noskaidrojuši tā atbilstību normatīvo aktu prasībām personas datu apstrādes jomā, kā arī 44,7% (n=17) nebija iepazinušies ar minētā programmnodrošinājuma privātuma politiku.

Pēc respondentu sniegtajām atbildēm, kas atklāja viņu informētības līmeni par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem, var secināt, ka drošības standartos (International Organization for Standardization, 2018) minētās prasības attiecībā uz ierīču izmantošanu netiek ievērotas, un 92,1% (n=35) no respondentiem atbildēja, ka attālinātā praksē izmantoja datoru (tai skaitā portatīvo), ko izmanto arī privātām vajadzībām. Minētais standarts paredz, ka ierīce var būt izmantota gan darbam, gan privātām vajadzībām, ja tiek nodrošināta atbilstoša informācijas aizsargāšana un šifrēšana, tomēr, ņemot vērā, ka 31,6% (n=12) no respondentiem uz jautājumu, kādi autentifikācijas drošības rīki tika izmantoti attālinātā praksē lietotajās ierīcēs, atbildēja, ka neizmantoja nekādus drošības rīkus, un 65,8% (n=25) pēdējā pusgada laikā nemainīja attālinātā praksē izmantoto ierīču paroles, secināms, ka izlasē pastāv būtisks kiberdrošības risks attālinātā praksē izmantoto ierīču aizsardzības jomā. Svarīgi atzīmēt, ka 15,8% (n=6) pieļāva, ka darbam izmantotās ierīces izmanto arī ģimenes locekļi (piemēram, dzīvesbiedrs, laulātais, bērni), kas rada papildu riskus drošībai.

Operētājsistēmas izvēle ietekmē arī drošības standartu piemērošanu, jo katrs programmnodrošinājuma ražotājs veido savu drošības politiku. Pasaulē populārāko operētājsistēmu – *Windows*, izmanto 57,9% (n=22) no respondentiem. *Windows* ražotājs iesaka mainīt paroli kaut vienreiz laika posmā no 30 līdz 90 dienām (*Hicock*, 2016), tas nozīmē, ka pusgada laikā lietotājam būtu jāmaina parole no 2 līdz 6 reizēm, atkarībā no izvēlētajiem drošības iestatījumiem. Tikai 2,6% (n=1) no respondentiem pēdējā pusgada laikā mainījuši paroli 2 līdz 4 reizes, un jau minētie 65,8% attālinātā praksē izmantoto ierīču paroles nemainīja vispār. Ņemot vērā, ka pēc drošības ekspertu atzinuma 81% no visiem kiberdrošības incidentiem ir saistīts ar vājo un/vai kompromitēto

paroļu izmantošanu (*Verizon,* 2019), minētais norāda, ka supervizoriem pastāv iespēja tikt pakļautiem kiberdrošības riskiem tieši novecojušo paroļu dēļ. Minēto risku pastiprina fakts, ka 28,9% (n=11) no respondentiem norādīja, ka attālinātā praksē izmantoto servisu/ierīču paroles sakrīt ar kādu no privātām vajadzībām izmantotām parolēm, kas neatbilst ISO/IEC 27001:2018 drošības standarta prasībām (International Organization for Standardization, 2018).

Tika konstatēts, ka starp supervizoriem ir zems izpratnes līmenis par kiberuzbrukumu riskiem, piemēram, sociālā inženieringa jēdzienu (kas ir viens no svarīgākajiem informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem) (*Granger,* 2001), tikai 7,6% (n=3) minēto jēdzienu izprot pilnīgi, bet 61,5% (n=24) no respondentiem sniedza atbildi, ka pilnībā neizprot jēdziena "sociālais inženierings" būtību. Līdzīga situācija novērojama arī ar jēdzienu "pikšķerēšana" (*phishing*) – 50% (n=19) no respondentiem atbildēja, ka pilnībā neizprot minēto jēdzienu, un 17,9% (n=7) sniedza atbildi, ka pilnībā to izprot. Paneļdiskusijas eksperti nespēja sniegt minēto jēdzienu definīcijas, kā arī, mēģinot izskaidrot jēdzienu saturisko tvērumu saviem vārdiem, nesniedza precīzas, pārliecinošas atbildes, piemēram, par jēdzienu "sociālais inženierings": "[..]tas droši vien saistīts ar sociālo tīklu veidošanu[..]", par pikšķerēšanu: "[..]zinu, ka tas ar drošību saistīts, kad kāds mēģina… nu lai mani dati nenokļūst nekur, paliek konfidenciāli[..]".

Personas datu apstrādes jomā konstatējams, ka supervizoru informētības līmenis ir zems/vidējs – 36,8% (n=14) atbildēja, ka pilnībā izprot tādus jēdzienus kā "datu subjekta tiesības", 50% (n=19) sniedza atbildi, ka pilnībā izprot jēdzienu "datu subjekta piekrišana", un 71% (n=24) no respondentiem atbildēja, ka pilnībā izprot jēdzienu "informēta piekrišana". Atzīmējams, ka Vispārīga datu aizsardzības regula un tās saturs ir labi pazīstams, un vairāk pazīstams, nekā nepazīstams attiecīgi 34,2% (n=13) un 36,8% (n=14) no respondentiem. Paneļdiskusijā intervētie eksperti atzīmēja, ka normatīvos aktus pārzina vāji, bet atzīst, ka tādas zināšanas būtu nepieciešamas: "Seminārā par datu aizsardzību stāstīja par datu aizsardzību, bet tas nebija ar supervīziju saistīts [..]", "[..]jā, vadlīniju tiešām nav, bet būtu labi, ka tādas būtu, par citu nozaru vadlīnijām es neko nezinu[..]".

Gandrīz puse no respondentiem 47,4% (n=18) neapsprieda ar saviem klientiem attālinātā praksē izmantoto informācijas tehnoloģiju (kiberdrošības) riskus. Vienlaikus atzīmējams, ka 81,6% (n=31), uzsākot attālināto praksi, nebija pierādāmi vienojošies ar saviem klientiem par attālinātās supervīzijas sesijas fiksācijas nosacījumiem, tikai 23,7% (n=9) atspējoja ieraksta funkciju izmantotā programmnodrošinājumā, lai nepieļautu nesankcionēto attālinātās supervīzijas sesijā notiekošā ierakstīšanu/fiksāciju/saglabāšanu, bet 31,6% (n=12) nebija aizdomājušies par tādu nepieciešamību.

Attālinātas supervīzijas sesiju fiksācijas nolūku ar klientiem pierādāmi (sarakstē) apsprieda 7,9% (n=3) no respondentiem. Piebilstams, ka 94,7% (n=36) no respondentiem apgalvoja, ka sesiju ieraksti netika veikti, tomēr tikai 23,7% (n=9) atspējoja ieraksta funkciju izmantotajā programmā. Paneļdiskusijas ekspertu intervijās arī tika atzīmēti dokumentācijas trūkumi: "[..]izmantoju to līgumu, ko piedāvā pasūtītājs, jo bieži vien strādāju ar organizācijām[..]"; "[..]man ir līgums, tur ir atrunāti konfidencialitātes principi… tas, ka neizpaudīšu informāciju[..]".

Anketas nobeigumā respondenti sniedza atbildi uz jautājumu, kādam supervīzijas veidam sniegs priekšroku turpmāk, kur 26,3% (n=10) sniedza atbildi, ka viņiem nav īpašas nozīmes, un tikai 10,5% (n=4) dos priekšroku attālinātai supervīzijas praksei, pārējie (63,2% (n=24)) respondenti izvēlēsies klātienes supervīziju. Minēto apstiprināja arī eksperti, raksturojot savu attālināto praksi: "[..]attālināti strādāt šobrīd ir vajadzība, man patīk kaut to pirmo sesiju klātienē organizēt – ļoti svarīgi redzēt cilvēkus, kamerā tikai galvas redzu[..]"; "[..]attālināto darbu uzveru viegli, citas iespējas šobrīd nav, bet darbu ir jādara[..]".

Vērtējot pētījuma rezultātus, jāņem vērā pētījuma ierobežojumi, proti anketēšanā iesaistījās neliels respondentu skaits, kas savukārt neļauj vispārināt datus, tomēr iegūtie dati raksturo noteiktas tendences. Svarīgi norādīt, ka pētījumā iegūtie dati atbilst Latvijas iedzīvotāju informētības līmenim par informācijas tehnoloģiju izmantošanas riskiem, ņemot vērā pirms pieciem gadiem Eiropas komisijas ekspertu novērojums par stabilu ikgadējo pozitīvo tendenci informētības līmeņa pieaugumā (European Commission, 2015).

Raugoties uz pētījuma rezultātiem no supervīzijas klienta puses, konstatējams, ka klients tiek nepietiekami informēts par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem supervīzijas attālinātā praksē. Līdz ar to supervīzijas klientiem var rasties grūtības realizēt Vispārīgā datu aizsardzības regulā viņiem noteiktās tiesības. Pētījuma rezultāti norāda uz nepieciešamību nodrošināt supervizorus ar minimālām normatīvo aktu prasībām un atbilstošu dokumentu kopumu (piemēram, privātuma politikas paraugs), kā arī ~~ir~~ supervizoru profesionālām apvienībām ir ieteicams aktualizēt diskusiju par profesionālo vadlīniju izveidošanu un ieviešanu praksē.

Ņemot vērā minēto, būtu nepieciešams pilnveidot supervizoru izglītības programmas, piemēram, papildinot programmas ar mācību saturu, kur fokuss būtu vērsts uz topošo supervizoru izglītošanu kiberdrošības un personas datu aizsardzības jomās, tādējādi nodrošinot supervizoru izglītību atbilstoši profesijas standartā noteiktajām kompetencēm. Ieteicams veicināt esošo supervizoru informētību par informācijas tehnoloģiju izmantošanas riskiem un personas datu apstrādi, nodrošinot tiem pieejamu un skaidru informāciju par minētiem attālinātās prakses aspektiem un to uzlabošanas iespējām, piemēram, informējot

supervizorus par nepieciešamību nošķirt darba un privātām vajadzībām izmantotās ierīces, sniegt informāciju par konfidenciālās informācijas šifrēšanas iespējām, būtu svarīgi informēt supervizorus par paroļu un drošības iestatījumu regulāra pārskata svarīgumu un nepieciešamību (piemēram, sniedzot informāciju par to, kā pārbaudīt izmantoto paroļu drošumu).

Ņemot vērā, ka aptaujas rezultāti parāda, ka supervizori mēdz iegūt informāciju pašizglītības ceļā, kā arī mēdz dalīties ar informāciju ar saviem klientiem, tai pašā laikā nemēdz vērsties pie attiecīgo nozaru speciālistiem pēc konsultācijas, profesionālām organizācijām ieteicams fokusēties uz īsu, kodolīgu informācijas avotu veidošanu (piemēram, infografika).

Secinājumi
Conclusions

Kopumā secināms, ka izvirzītais pētījuma mērķis noskaidrot Latvijas supervizoru informētību par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem un personas datu aizsardzību, COVID-19 pandēmijas radītājos apstākļos ir sasniegts, iegūtos rezultātus attiecinot uz konkrēto izlases kopumu.

COVID-19 pandēmija aktualizēja nepieciešamību pēc attālinātās prakses. Tomēr secināms, ka pašas attālinātās prakses organizēšanas tiesiskais pamats un dokumentācijas noformēšana ir joma, kurā nākotnē nepieciešams veikt atbilstošus uzlabojumus profesionālo standartu un vadlīniju līmenī, kā arī supervizoru un supervīzijas studentu izglītības un profesionālo kompetenču pilnveides līmenī.

Aptaujātie supervizori un studenti, kopumā uz aptaujas laiku bija vāji informēti par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem un savā attālinātajā praksē izmantoja tikai pēc noklusējuma pieņemtos drošības pasākumus. Saskatāms, ka supervizoriem pietrūka izpratnes par specifiskiem informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem, līdz ar to supervizoru vidū pastāv risks kļūt par specifisku, tieši uz attālināto praksi vērsto kiberuzbrukumu upuriem, kā arī ciest no kiberuzbrukumiem, kas balstās uz nedrošu/novecojušu/kompromitēto paroļu izmantošanu.

Ņemams vērā, ka informācijas tehnoloģiju joma strauji attīstās un pilnveidojas, līdz ar to ir nepieciešami tālāki pētījumi šajā jomā, lai objektīvi noteiktu izmaiņas Latvijas supervizoru informētībā par informācijas tehnoloģiju izmantošanas (kiberdrošības) riskiem un personas datu aizsardzību.

Summary

In general, it can be concluded that the aim of the study, to find out the awareness of Latvian supervisors about the risks of information technology use (cyber security) and personal data protection in the conditions of COVID-19 pandemic, has been achieved by applying the obtained results to the sample. Provision of remote services became relevant all over the world, during the 2020 COVID-19 pandemic. Latvian supervisors were also forced to transfer their practice to the digital space as well. COVID-19 pandemic challenges opened a wider range of opportunities for improvement remote practice.

The COVID-19 pandemic highlighted the need for remote practice. However, it can be concluded that the legal basis for the organization of the remote practice itself and the preparation of documentation is an area where, in the future, appropriate improvements need to be made, at the level of professional standards and guidelines.

The surveyed supervisors and students, in general, were poorly informed about the risks of using information technology (cyber security) at the time of the survey and used only general security measures in their remote practice. It can be seen that supervisors lacked a sufficient understanding of the specific risks of the use of information technology (cybersecurity), thus there is a risk among supervisors to become victims of specific attacks aimed at remote practices, as well as to suffer from cyber-attacks based on insecure / outdated / compromised passwords. however further research is needed to find the most effective methods how to improve these competences.

The obtained results allowed to conclude that the COVID-19 pandemic highlighted the need for supervision remote practice, at the same time the research data show that the awareness of Latvian supervisors about the risks of information technology use (cyber security) and personal data protection is medium to low.

The results of the research show that in the education of Latvian supervisors it is necessary to allocate place for the acquisition of information technology (cyber security) risk and personal data protection regulation.

Literatūra
References

Angena, A., Mārtinsone, K. (2020). Latvijas supervizoru ētikas kompetences nozīmīguma un īstenojamības pašnovērtējums. *Proceedings of the International Scientific Conference SOCIETY. INTEGRATION. EDUCATION, Volume V*, Vol. 19, 34.

Braun, V., Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3(2),* 77-101.

Eiropas Parlaments un Padome. (2016). Par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). *Eiropas Savienības Oficiālais Vēstnesis*, *119*, 4.5.2016, Pieejams: https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32016R0679&from=LV

European Commission. (2015). *Special Eurobarometer 431: Data protection*. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

Google/Harris Poll, Enterprise. (2019) *Online Security Survey*. Retrieved from https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus*. Retrieved from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Hicock, R. (2016) *Microsoft Password Guidance. Microsoft Identity Protection Team*. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO/IEC 27001:201. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

International Telecommunication Union. (2008). *O. Series X: Data Networks, Open System Communications and Security Telecommunication security*. ITU-T X.1205 Interfaces, 10(20-X), 49. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I

Joint Task Force for the Development of Telepsychology Guidelines for Psychologists (APA). (2013). Guidelines for the practice of telepsychology. *American Psychologist, 68(9),* 791–800. Retrieved from https://doi.org/10.1037/a0035001

LR Saeima. (2020). Par Latvijas Nacionālo attīstības plānu 2021. – 2027. gadam (NAP2027). *Latvijas Vēstnesis*, 127, 06.07.2020. Pieejams: https://likumi.lv/ta/id/315879

Ministru kabinets. (2017). Prasības sociālo pakalpojumu sniedzējiem. *Latvijas Vēstnesis*, 126, 27.06.2017. Pieejams: https://likumi.lv/ta/id/291788

Ministru kabinets. (2020). Par ārkārtējās situācijas izsludināšanu. *Latvijas Vēstnesis*, 216A, 06.11.2020. Pieejams: https://likumi.lv/ta/id/318517

Nipers, J., Zīds, O., Kuklis, J. (2012). *Profesionālajā izglītībā iesaistīto vispārizglītojošo mācību priekšmetu pedagogu kompetences paaugstināšana*. Pieejams: https://profizgl.lu.lv/pluginfile.php/36205/mod_resource/content/0/3_modulis/O_Zida_materials.pdf

Profesionālās izglītības un nodarbinātības trīspusējās sadarbības apakšpadome (PINTSA). (2019). *Supervizora profesijas standarts*. Pieejams: https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/2017/PS-109.pdf

PwC. (2018). *The Global State of Information Security® Survey 2018*. Price Waterhouse Coopers. Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf

Statista. (2017). *Actual status of data security worldwide from 2010 to 2025*. Retrieved from https://www.statista.com/statistics/815167/worldwide-actual-status-of-data-security/

Verizon. (2019). *Verizon 2018 data breach investigations report (DBIR).* Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Vides aizsardzības un reģionālās attīstības ministrija. (2020). *Projekts VSS 48. Digitālās transformācijas pamatnostādnes 2021.-2027.gadam (informatīvā daļa*). Pieejams: https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf