Sisekaitseakadeemia

Finantskolledž

Eliise Schmuul

MAKSUMAKSJATE KESKSE PROFILEERIMISE VAJALIKKUS JA VÕIMALUSED

Lõputöö

Juhendaja:

Airi Jansen-Uueda, MA

Kaasjuhendaja:

Maret Güldenkoh, MBA

Tallinn 2021

SISEKAITSEAKADEEMIA LÕPUTÖÖ ANNOTATSIOON

Finantskolledž	Mai 2021
Töö pealkiri eesti keeles: Maksumaksjate keskse profileerimise vajalikkus ja võimalused	
Töö pealkiri inglise keeles: Necessity and Possibilities of Central Profiling of Taxpayers	
Lühikokkuvõte: Lõputöö on kirjutatud eesti keeles ning koosneb 55 leheküljest. Lõputöös kasutati 60 allikat. Lõputööl on ka ingliskeelne kokkuvõte. Töö uurimisprobleemiks oli küsimus: „Kuidas saavutada mõistlik tasakaal andmekaitse normide ja avaliku huvi vahel isikuandmete töötlemisel?“. Lõputöö eesmärk oli välja selgitada maksumaksjate keskse profileerimise vajalikkus ning leida viisid maksumaksjate keskseks profileerimiseks andmekaitse norme kahjustamata ja avalikku huvi piiramata. Uurimismeetodina kasutati kvalitatiivset uurimismetoodikat. Andmekogumise meetodina kasutati ekspertintervjuusid, mille analüüsimiseks kasutati kvalitatiivset sisuanalüüsi. Maksumaksjate keskne profileerimine on vajalik, kuna suurem andmevahetus ja maksumaksjatega seotud riskide jagamine teiste asutustega tõstaks riigi efektiivsust, vähendaks kulusid ning suurendaks riigi mainet. Maksumaksjate keskne profileerimine võimaldaks läheneda maksumaksjatele juba algfaasis, kui nad enim abi vajavad või proovivad skeemide abil ebaausat konkurentsi tekitades alusetult riigi vahendeid taotleda. Töös leiti, et maksumaksjate keskset profileerimist on võimalik teostada ilma andmekaitse norme kahjustamata ja avalikku huvi piiramata. Tegelikkuses ei ole riigiasutustel seadusandlikke piiranguid andmete kasutamiseks, kui andmed on vajalikud tööülesannete täitmiseks. Selleks, et andmekaitse normide täitmise oht ei suureneks andmevahetuse suurenemisel, tuleks andmekaitsespetsialistidele luua ühine teadmine, mis on andmekaitsenõuete piirides lubatud andmete töötlemisel. Samuti tuleb koostada kindla projekti kohta andmekaitsealane mõjuhinnang, kus hinnatakse võimalikku maksumaksjate õiguste riivet, mille avaldamine on avalikes huvides.	
Võtmesõnad: andmekaitse, avalik huvi, maksud	
Ingliskeelsed võtmesõnad: data protection, public interest, taxes	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Eliise Schmuul	
Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma lõputöö avaldamisega elektroonilises keskkonnas.	
(allkirjastatud digitaalselt)	
Vastab lõputöö nõuetele	
Juhendaja: Airi Jansen-Uueda	(allkirjastatud digitaalselt)
Kaasjuhendaja: Maret Güldenkoh	(allkirjastatud digitaalselt)
Kaitsmisele lubatud	
Kolledži direktor: Kerly Randlane	(allkirjastatud digitaalselt)

SISUKORD

SISSEJUHATUS

Riigikontroll on oma auditi „Andmete kättesaadavus ja kasutamine riigi targaks juhtimiseks“ 29.04.2020 märgukirjas nr 2-1/80031/3 välja toonud, et asutused rakendavad üha enam uuenduslikke andmeanalüüsi meetodeid ning tegelevad andmevahetuse suurendamisega riigiasutuste vahel. Näiteks on Maksu- ja Tolliameti (edaspidi MTA) andmete analüüsivõimekuse kasv võimaldanud luua kõikehõlmava maksuprofiili maksuriskide tuvastamiseks kasutades nii väliste osapoolte kui ka MTA enda andmeid. (Riigikontroll, 2020)

Samuti on märgukirjas esile tõstetud Siseministeeriumi algatus muuta Päästeameti tegevust reguleerivaid õigusakte, et võimaldada Päästeametil saada ka teiste asutuste andmeid tulekahjude ennetamiseks. Auditi märgukirjas leiti probleemina aga andmete kättesaadavus ja kasutamine. Näiteks on üheks andmevahetuse takistuseks lahendamata andmevahetuse õiguslikud probleemid. Samuti vajalikke andmeid ei kaasata andmeanalüüsi, kuna need ei ole tehniliselt kättesaadavad. (Riigikontroll, 2020)

Asutustevaheline andmevahetuse suurendamine on avalikes huvides. Riigikontrolli märgukirjas välja toodud lahendamata andmevahetuse ühe õigusliku probleemina on autori arvates näiteks maksukorralduse seadusest tulenev maksuhalduri kohustus maksusaladuse kaitsele, mis raskendab riigis avalikes huvides andmeid ühtedel alustel töödelda (Maksukorralduse seadus[1], 2002, § 26). Riigiasutuste juurdepääs isikuga seotud andmetele on väga erinev ja andmekogud laiali erinevate asutuste valduses. Selliste piirangute tõttu jääb võimalik maksutulu saamata ning riik väljastab toetusi isikutele, kes ei pruugi olla õigustatud selliseid toetusi saama või toetust tegelikult ei vajagi. Sellest tuleneb ka lõputöö teema valik.

Töö autor defineerib „maksumaksjate keskset profileerimist“ andmevahetuse suurendamisena erinevate asutuste vahel, et tagada ühtsem profiil maksumaksjatest, paremate teenuste pakkumiseks ja pettuste vältimiseks, mis võimaldaks ajakohaseimat kuva maksumaksjatest. Ideaalis näeb autor maksumaksja keskse profileerimisena mitte ainult andmevahetamise suurendamist, vaid ka ühtse riskiprofiili loomist riigis, et tõhustada riikliku järelevalvet. Mait Laaring (2019, lk 252) defineerib riikliku järelevalvet haldusorganite (korrakaitseorganite) tegevusena haldusväliste isikute tegevuse

kontrollimisel. Autori arvates keskne profiil võimaldaks kiirelt reageerida erinevatele isiku profiili muutustele, mis tõhustaks toetuste tagasiküsimisi või hoopis võimaldaks raskustesse sattunud isikut võimalikult efektiivselt ja kiirelt aidata. Maksumaksjate keskseks profileerimiseks on vajalik teada, millisel tasemel on asutuste vaheline koostöö ja andmevahetus, mis võib olla võimaluseks riigiasutuste vahel andmete kättesaadavust ja kasutamist parandada.

Aktuaalsus tuleneb Eesti Vabariigi Valitsuse „Eesti 2035" strateegiast, kus on välja toodud, et riigivalitsemise tõhusus peab suurenema vananeva ja kahaneva rahvastiku tõttu, et pakkuda kvaliteetseid avalikke teenuseid. Seejuures ühe väljundina on toodud andmemajanduse ja digiriigi edendamine, sh planeeritud tegevusena platvormipõhise lähenemise arendamine andmete ja digilahenduste vallas. (Eesti Vabariigi Valitsus, 2021b) Strateegia arenguvajadustena nähakse, et riik peaks tõhustama teabevahetust asutuste ja ettevõtete vahel ning kasutama rohkem reaalajas andmevahetust, sealhulgas ava- ja suurandmeid (Eesti Vabariigi Valitsus, 2021a).

Lõputöö on uudne, kuna autorile teadaolevalt ei ole Eestis varem ühtegi lõputööd maksumaksjate kesksest profileerimisest tehtud. Lõputöös käsitletakse ka andmekaitset, millest on tehtud varasemalt mitmeid bakalaureuse- ja magistritöid, kuid andmekaitset avaliku sektori teabevahetuse suurendamise vaates, millele autor keskendub, ei ole autorile teadaolevalt uuritud. Näiteks Tartu Ülikoolis on Konks (2014) teinud magistritöö teemal „Kriminaalmenetluses kogutud isikuandmete kaitse avaliku sektori teabe taaskasutamisel" ning Parma (2017) lõputöö teemal, mis käsitleb andmevahetuse suurendamist maksuvõlgade sissenõudmisel OECD haldusabi konventsiooni alusel.

Lõputöö uurimisprobleemiks on küsimus: „Kuidas saavutada mõistlik tasakaal andmekaitse normide ja avaliku huvi vahel isikuandmete töötlemisel?". Uurimisprobleemi lahendamiseks on tõstatatud järgmised uurimisküsimused:

1. Millised probleemid on maksumaksjate kesksel profileerimisel?
2. Miks on vajalik riigiasutuste andmevahetuse suurendamine ja praeguste andmekaitse tõkete leevendamine?
3. Kuidas oleks võimalik suurem andmevahetus riigiasutuse vahel ning ühtne riskiprofiili loomine?

Lõputöö eesmärk on välja selgitada maksumaksjate keskse profileerimise vajalikkus ning leida viisid maksumaksjate keskseks profileerimiseks andmekaitse norme kahjustamata ja avalikku huvi piiramata.

Eesmärgi saavutamiseks vajalikud uurimisülesanded on:

1. Analüüsida erialast teaduskirjandust andmekaitsest avalikus sektoris, avalikust huvist ning praegusest haldusorganite vahelisest teabevahetusest ülevaate saamiseks ning siduda need õigusaktide ja kohtulahenditega.

2. Analüüsida ekspertide hinnanguid toetuste määramisega seotud võimalike kitsaskohtade osas tulenevalt olemasolevatest maksumaksja andmetest ja asutuste andmevajaduse osas maksumaksjatele paremate teenuste pakkumisel.

3. Sünteesida teooriat ja ekspertintervjuusid ning teha järeldusi ja ettepanekuid maksumaksjate keskseks profileerimiseks riigis.

Uurimismeetodina kasutatakse lõputöö eesmärgi saavutamiseks kvalitatiivset uurimismetoodikat. Andmeanalüüsi meetodina kasutatakse suunatud kvalitatiivset sisuanalüüsi (Laherand, 2008, lk 45). Andmekogumise meetodina kasutatakse ekspertintervjuusid, kuna lõputöö eesmärgi saavutamiseks on oluline teada erinevate riigiasutuste esindajate arvamust antud teemast, et välja selgitada maksumaksjate keskse profileerimise vajalikkus. Valimiks on mittetõenäosuslik eesmärgistatud valim, milleks on ekspertintervjuud Ettevõtluse Arendamise Sihtasutuse (edaspidi EAS), Haigekassa, Keskkonna Investeeringute Keskuse (edaspidi KIK), MTA, Põllumajanduse Registrite ja Informatsiooni Ameti (edaspidi PRIA), Töötukassa, Tallinna Kesklinnavalitsuse Sotsiaalhoolekandeosakonna ning Sotsiaalkindlustusameti esindajatega.

Lõputöö koosneb kahest peatükist ja alapeatükkidest. Esimeses peatükis analüüsitakse, millised on teoreetilised probleemid maksumaksjate kesksel profileerimisel, antakse ülevaade andmekaitsest avalikus sektoris, avalikust huvist ning praegusest haldusorganite vahelisest teabevahetusest. Selleks analüüsitakse erialast teaduskirjandust, mis seotakse kohtulahendite ja õigusaktidega tegeliku olukorra välja selgitamiseks andmekaitse valdkonnas.

Teises peatükis tuuakse välja praktilised probleemid maksumaksjate kesksel profileerimisel kasutades ekspertintervjuusid riigiasutuste esindajatega. Ekspertintervjuude kaudu analüüsitakse riigiasutuste andmevahetuse suurendamise ja praeguste andmekaitse tõkete eemaldamise vajalikkust. Sünteesides kogu tööd tehakse järeldused ja ettepanekud, kuidas oleks võimalik suurem andmevahetus riigiasutusega ning ühtne riskiprofiili loomine.

1. ANDMEKAITSE AVALIKUS SEKTORIS NING AVALIK HUVI MAKSUMAKSJATE KESKSEL PROFILEERIMISEL

1.1. Andmekaitse avaliku sektori teabevahetuses

Selleks, et mõista intervjueeritavate seisukohti ja probleeme andmevahetuse suurendamisel, on autori arvates oluline anda ülevaade järgnevas alapeatükis andmekaitse olemusest ja üldistest isikuandmete töötlemise piirangutest ning tuua näiteid riikide praktikast erinevate andmevahetussüsteemide arendamisel esinenud probleemidest. Kuna „maksumaksjana“ käsitleb autor töös nii füüsilisi kui ka juriidilisi isikuid, kajastatakse järgnevas peatükis mõlema õigussubjekti andmekaitsenõudeid, mis on erinevad, kuid omavahel seotud.

27. aprill 2016 loodi Euroopa Parlamendi ja Nõukogu määrus 2016/679 (edaspidi GDPR) füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus), mis on peamine regulatsioon Euroopa Liidus, millest tuleb juhinduda andmekaitses. GDPR artikkel 99 järgi on määrus tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides (Euroopa Parlament ja Euroopa Nõukogu, 2016). Andmekaitse eesmärk on teavet kaitsta selle ohtu seadmise, kadumise ja rikkumise eest. GDPR-i ja teiste privaatsust tagavate regulatsioonide kontekstis keskendub andmekaitse eelkõige isikuandmete kaitsele, mis ei piirdu vaid andmete häkkimise või varastamise ennetamisega. Andmekaitse reguleerimisala ulatub klassifitseerimisest ja kategoriseerimisest kuni kogu organisatsiooni andmete säilitamiseni. (Chavalit & Hohler, 2020, p. 36)

Isikuandmed on väärtuslik ressurss nii ärilistes huvides, kui ka avalikes huvides, näiteks isiku asukohaandmetest teavitamine võib aidata liiklusvoolusid tõhustada ning terviseseisundi jagamine võib olla haiguste ohjamisel oluline vahend (Rockenbach, *et al*., 2020, p. 1). Isikuandmeid sisaldavate massandmete töötlusele lisab keerukust vajadus tagada selle õiguspärasus ja seejuures mängivad üha kasvavat rolli tehnoloogilised vahendid (Bogdanov & Siil, 2020, lk 479).

Enne GDPR loomist oli Euroopa Liidus andmekaitse reguleerimiseks andmekaitse direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, mis seadis miinimumstandardid andmekaitse seadusele Euroopa Liidu liikmesriikides. Paljud liikmesriigid kasutasid oluliselt tugevamaid nõudeid, kui andmekaitse direktiivis nõutud, et kaitsta isiklikult tuvastatavat informatsiooni, kuna direktiiv oli selleks ajaks 20 aastat vana ning ei täitnud enam oma eesmärki. Selle tõttu oli organisatsioonidel keeruline orienteeruda erinevate seaduste vahel, eriti kui tehti koostööd mitmete erinevate liikmesriikidega. Sellest tulenevalt otsustas Euroopa Komisjon GDPR loomise kasuks, mis kohalduks kõigile liikmesriikidele füüsiliste isikute õiguste, vabaduste ja privaatsuse kaitseks ning Euroopa Liidu sisese vaba liikumise soodustamiseks organisatsioonidel. (IT Governance Privacy Team, 2017, p. 13)

Andmekaitsekaasuste lahendamisel tuleb vaadata paralleelselt nii vahetult kohaldatavat üldmäärust GDPR-i ning alates 15.01.2019 uut riigisisest isikuandmete kaitse seadust, mis põhineb 95/46/EÜ direktiivil. GDPR täiendab ja täpsustab varasema direktiivi norme ning direktiivis ei ole andmesubjekti õiguste valdkonnas suuri vastuolulisi uuendusi võrreldes varasema direktiiviga. (Salumaa, 2018, lk 92)

Oluline andmekaitsekaasuste lahendamisel on ka teadmine, et inim- ja põhiõiguste praktika Euroopas keskendub üldiselt avaliku võimu organite tegevuse põhjendamisele, lähtudes mõistlikkusest. Õigusakti seaduslikkus sõltub sellest, kas seda on võimalik õigustada selliselt, et seda võiksid mõistlikult aktsepteerida isegi need, kes peavad kandma kõige suuremat koormat. Kõige olulisem on inim- või põhiõiguste teemalistel vaidlustel proportsionaalsuse põhimõte, mis võimaldab struktuurselt hinnata meetme rakendamise üldist mõistlikkust. (Kumm, 2020, lk 103 ja 109) Samuti GDPR preambula lõike 4 kohaselt õigus isikuandmete kaitsele ei ole absoluutne õigus, vaid seda tuleb kaaluda vastavalt selle ülesandele ühiskonnas ning tasakaalustada muude põhiõigustega vastavalt proportsionaalsuse põhimõttele (Euroopa Parlament ja Euroopa Nõukogu, 2016). Kaalutlusõiguse puhul tuleb arvestada puudutatud isikute õiguseid ja avalikke huve ning arvesse võetavad õigused ja huvid peavad olema konkreetse otsuse sisus olulised ja omavahel seotud (Lember, 2019, lk 753).

Andmekaitse määruse täitmiseks peavad organisatsioonid (sh avalik sektor) tuvastama andmete tundlikkuse ja tüübi, mida nad koguvad, töötlevad ja säilitavad. Lisaks peavad nad tagama andmete kättesaadavuse ja säilitama vaid nende organisatsioonile vajalikke

andmeid. Näiteks GDPR artikkel 15 annab andmesubjektidele õiguse taotleda juurdepääsu nende kohta kogutud andmetele ja artikkel 17 alusel lasta need kustutada (Euroopa Parlament ja Euroopa Nõukogu, 2016). Paljud organisatsioonid ei suuda aga neid nõudeid täita, kuna nad ei tea, kus isikuandmeid hoiustatakse või kas neid andmeid saab kustutada. Andmekaitse regulatsioonide järgimist raskendab ka pilvetehnoloogia suurem kasutuselevõtt, kuna organisatsioonide tehnoloogia piirid laienevad ning üha raskem on määratleda andmekaitse vastutusala ning aruandekohustust. (Chavalit & Hohler, 2020, pp. 36–38)

Dakić ja Ribarić (2020, pp. 190–195) leiavad, et GDPR-i tuleks parandada ja täiustada, kuna:

1) kõik terminid ei ole hästi defineeritud ja on määratlemata, mis tekitavad seaduse lünki ja tekitavad erinevaid tõlgendamise võimalusi - seetõttu on isikul, kes peab määruse nõudeid täitma, GDPR-i keeruline lugeda ja mõista;
2) andmekaitsespetsialistidele ei ole seatud standardseid nõudeid, mis tõendaks, et nad on pädevad nõustama töötajaid GDPR-i nõuete täitmisel;
3) kõik ettevõtted ja asutused ei ole võimelised kõiki nõudeid täitma, sest nõuete täitmise tagamine nõuab palju ressurssi;
4) määruses ei ole kirjeldatud minimaalseid turvanõudeid enamkasutatavatele teenustele nagu WIFI ühendus ja eravõrgu kaudu kaugjuurdepääs.

Õigused privaatsusele peavad olema tasakaalus üldise heaolu ja turvalisusega, mis on esmatähtsad (Llanillo & Baustista, 2017, p. 25). Enamasti töötleb avalik sektor isiklikku teavet, kuna neil on selleks seaduslik kohustus või kuna töötlemine on vajalik avalikes huvides. Näiteks arhiivide pidamine on avalikes huvides, kuid isiku õigus olla unustatud mitte. Õigus andmete kustutamisele ja unustamisele on avaliku sektori andmete töötlemisel vähetähtis. Kuid tuleb hoolega jälgida, mis õiguslikel alustel andmeid töödeldakse ning on oluline, et isikutel on andmetele juurdepääsu õigus ning nad saavad neid andmeid parandada. (Klingenberg, 2016, p. 67) Üldjuhul on võimalik andmeid töödelda isiku nõusolekul, kuid andmete töötlemine on võimalik ka avalikes huvides ilma isiku nõusolekuta. Näiteks on võimalik töödelda avalikes huvides eriliiki andmeid.

Eriliiki andmete töötlust avalikes huvides sätestas enne uut määrust 95/46/EC artikkel 8 (4) ja praegu GDPR-i artikkel 9 punkt g. Eriliiki isikuandmed on andmed, millest ilmneb

rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilised andmed, terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. (Euroopa Parlament ja Euroopa Nõukogu, 2016) Liikmesriigid on andmete töötlemise võimalust avalikes huvides kasutanud varasema määruse 95/46/EC artikli 8 lõige 4 alusel erinevatel eesmärkidel, kuid meetme kasutamisel tuleb täpselt kirjeldada, miks ja millistel õiguslikel alustel selline töötlus on vajalik ja kas see on proportsionaalne (Quinn, 2017, p. 356). Sama põhimõte kehtib ka praeguse kehtiva määruse rakendamisel.

GDPR artikkel 6 järgi tuleb isikul anda nõusolek enda andmete töötlemiseks, kuid riigiasutuste puhul, kes peavad isikuandmeid töötlema, on sellise nõusoleku saamine oma ülesannete täitmiseks probleemne. Riigiasutused peavad avalike ülesannete täitmisel põhjendama, miks on andmete töötlemine avalikes huvides vajalik. Kui ametnik peab avalikes huvides andmeid töötlema, kehtib see kõikidele isikutele – isikutele, kes on nõus oma andmete töötlemisega ja isikutele, kes ei ole nõus andmete töötlemisega. Vastasel juhul ei ole asutusel võimalik oma ülesandeid täita. Avaliku võimu asutus ja üksikisik on märkimisväärselt ebavõrdsetel positsioonidel andmete töötlemisel, ning seetõttu ei ole ainult isiku nõusolek andmete töötlemiseks piisav õiguslik alus. (Klingenberg, 2016, p. 69)

Eeltoodust lähtuvalt avalikul sektoril on vajalik andmete töötlemiseks tõendada, et selline töötlus on vajalik avalikes huvides või seadusest tuleneva kohustuse täitmiseks ning õigusliku alusena ei piisa vaid isiku nõusolekust. Kuna andmete töötlemist võimaldavad meetmed on laialdased mõisted, on toodud GDPR-i artiklis 6 täiendav kriteerium töötlemise seaduslikkusele (Euroopa Parlament ja Euroopa Nõukogu, 2016). Määruse järgi liikmesriigi seadused peavad vastama üldist huvi pakkuvatele eesmärkidele või olema vajalikud teiste inimeste õiguste ja vabaduste kaitseks, austama andmekaitse õiguse olemust ja olema proportsionaalsed taotletava õiguspärase eesmärgiga (Klingenberg, 2016, p.70; Dobos & Takács-György, 2019, p. 473).

Sarnaselt Eesti avaliku sektori ideele suurendada asutustevahelist andmevahetust, tekkis Saksamaa avaliku sektori asutustel idee luua ühine toetav süsteem asüüli taotlejatega seonduvate protseduuride läbiviimiseks koostöös kohalike omavalitsusasutuste ja riiklike võimuorganitega. Esiteks tuli neil välismaalaste keskne register muuta jagatud hoidlaks, mis sisaldas umbes 20 miljoni välismaalase isikuandmeid. Keskse süsteemi loomisel

peamiste probleemidena nähti seaduste uuendamise vajadust ning andmekaitse korralduslikke probleeme, kuna kesksel süsteemil puudub üks vastutaja. Selleks, et vastata GDPR-i nõuetele, leiti järgmised lahendused (Rieger, *et al.,* 2019, pp. 268–270):

1) vastutusalade kindlaksmääratlemine;
2) seaduste uuendamisega isikuandmete töötlemise õiguslike aluste loomine;
3) süsteemi kujunduse loomine selliselt, mis võimaldaks parandada või kustutada personaalseid andmeid ning võimaldaks ligi pääseda ametnikel vaid nendele andmetele, mida neil on õigus näha tulenevalt seadusest.

Euroopas on teisigi riike, kus püütakse leida uusi lahendusi varimajanduse vähendamiseks ja asutuste tööprotsesside tõhustamiseks kasutades tänapäeva tehnoloogilisi võimalusi. Kuid ka nendes riikides on probleemiks andmekaitse regulatsiooni nõuete täitmine. Näiteks Dobos & Takács-György (2019, p. 473) leiavad, et illegaalse tööturu vähendamiseks Ungaris võiks luua süsteemi, kus töötajate andmed laekuvad automaatselt maksuhaldurile. Andmekaitsealaste probleemide lahendusena nähakse nii-öelda „huvide kaalumise" ja proportsionaalsuse testi, mille käigus uuritakse tööandja õigustatud huve ja töötajate õiguseid ja kas selline süsteem on vajalik ning kohane (Dobos & Takács-György, 2019, p.474). Varasemalt on töös viidatud samadele probleemidele, kui ühtedele olulisimatele aspektidele andmekaitses.

GDPR artiklis 25 on kehtestatud Euroopa Liidu andmekaitse õiguses vastutavatele töötlejatele lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete järgimise kohustus (Euroopa Parlament ja Euroopa Nõukogu, 2016). Artiklis sisalduvad nõuded panevad infosüsteemide arendamisel arvestama privaatsusega seotud huve kogu arendusprotsessis, mille tõttu neid norme peetakse andmekaitsereformi ühtedeks innovatiivseimateks ja ambitsioonikaimateks sammudeks. Sellised meetmed peaksid rohkem suunama isikuid andmekaitseõigusega kooskõlastatud käitumisele, mitte ainult uute seaduste loomisele, kuna andmekaitsepõhimõtted on IT-süsteemidesse sisse ehitatud. (Bogdanov & Siil, 2020, lk 479)

GDPR artikkel 23 lõikes 1 on toodud juhud, mil artiklite 5, 12–22 ja 34 kohaldamist võib piirata õigusaktides teatud alustel või liidu institutsioonide ja organite toimimisega seotud küsimuste puhul nende sise-eeskirjadega, kuid piirang peab austama põhiõiguste ja -vabaduste olemust ning olema proportsionaalne ja vajalik demokraatlikus ühiskonnas.

Näiteks artikli 25 lõike 1 punkti e järgi võib piirata artiklite kohaldamist, et tagada liidu või liikmesriigi muud üldist avalikku huvi pakkuvad olulised eesmärgid, eelkõige liidu ühise välis- ja julgeolekupoliitika eesmärgid või liidu või liikmesriigi oluline majanduslik või finantshuvi, sealhulgas rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus. Sama artikli lõikes 2 on toodud loetelu selle kohta, mida õigusaktid või sise-eeskirjad peavad sisaldama, et piirata nimetatud artiklite kohaldamist õiguspäraselt. (Euroopa Parlament ja Euroopa Nõukogu, 2016)

GDPR artikli 22 lõike 1 järgi on andmesubjektil õigus, et tema kohta ei võetaks otsust, mis põhineb vaid automatiseeritud töötlusel või profiilianalüüsil, mis avaldab talle märkimisväärset mõju või toob kaasa õiguslikke tagajärgi (Euroopa Parlament ja Euroopa Nõukogu, 2016). Karu (2021, lk 46) on analüüsinud artikli 22 mõju tehisintellekti rakendamisel, kuid töö autori arvates kehtib sama ka kesksel profileerimisel. Kui andmeid võimaldataks kuvada ühest kohast ja nende andmete põhjal hakatakse otsuseid tegema, siis see ei peaks olema automaatprotsessi osa. Karu (2021, lk 46) leiab, et GDPR artikli 22 lg 1 täitmiseks tuleks hinnata olemasolevate andmete mõju ning valida, milliseid otsuseid tehakse automatiseeritult ning mida mitte.

Automatiseerituid otsuseid teeb Eestis näiteks maksuhaldur teatud määral maksukorralduse seaduse (edaspidi MKS) § 46^2 lg 1 alusel ehk maksuhaldur võib anda haldusakti ja dokumendi automatiseeritult, ilma maksuhalduri ametniku vahetu sekkumiseta (Maksukorralduse seadus[1], 2002). Korraldusi antakse deklaratsioonide esitamiseks ja puuduste kõrvaldamiseks, maksuvõla lihtsustatud ajatamise otsuste tegemiseks, enammakse tagastamise otsuste ja muude toimingute tegemiseks, kui on võimalik määratleda otsuse tegemise eeldused (Lember, 2019, lk 749–752).

Peale isikuandmete kaitset reguleerivatele õigusaktidele on oluline analüüsida ka MKS-ist tulenevat maksusaladuse kaitset, mida käsitlevad MKS § 26 – § 30 (Maksukorralduse seadus[1], 2002). Paljudele riigiasutustele on antud võimalus saada maksusaladust sisaldavat teavet MKS § 29 alusel ning lisaks maksuhaldurile on ka neile teatavaks saanud info saladuses hoidmise kohustus, mis tuleneb MKS § 26 lg-st 3 (Maksukorralduse seadus[1], 2002). Lehis (2015) leiab, et praktikas puudub kontroll selle üle, kas ka kolmandad isikud, kes on saanud teavet, mis sisaldab maksusaladust, kasutavad infot sihipäraselt või levitavad seda veel kellelegi, kellel sellise info saamise õigus puudub. MKS § 29 on toodud 57 erinevat juhtu, mis puhul ja kellele võib maksusaladust sisaldavat teavet avaldada

(Maksukorralduse seadus[1], 2002). Nii Lehis (2015) kui ka Lind (2009, lk 455) nendivad, et maksusaladuse regulatsiooni ei ole Eestis põhjalikult analüüsitud.

Maksusaladuse mõiste hõlmab ka teiste seadustega kaitstud hüvesid – MKS § 26 lg-s 1 on viidatud nii äri- kui ka pangasaladusele (Lind, 2009, lk 456; Maksukorralduse seadus[1], 2002). Pangasaladus on (Krediidiasutuste seadus[1], 1999 § 88 lg 1) kõik andmed ja hinnangud, mis on krediidiasutusele teatavaks saanud tema või teise krediidiasutuse kliendi kohta. Samas paragrahvis on sätestatud juhud, mil krediidiasutus võib ja peab avaldama pangasaladust sisaldavaid andmeid, sh Maksu- ja Tolliametile (Krediidiasutuste seadus[1], 1999). Sisuliselt hõlmab pangasaladuse mõiste kõiki andmeid, mida klient krediidi asutusele teatavaks teeb, ning lisaks sellele krediidiasutuse hinnanguid, mida see kliendi kohta annab (Lind, 2009, lk 456). Ärisaladuse puhul puudus varasemalt ühene legaaldefinitsioon, kuigi mitmed õigusaktid kasutasid ärisaladuse mõistet, näiteks Eesti Vabariigi põhiseaduses, konkurentsiseaduses, patendivoliniku seaduses, ravimiseaduses, ning äriseadustikus (Lind, 2009, lk 456). Konkurentsiseaduse[1] § 63 lg 2 kohaselt loetakse ärisaladuseks teavet, mida ettevõtja peab ise põhistatult kindlaks määrama ning ära märkima (Konkurentsiseadus[1], 2001).

Ärisaladuse mõistet on käsitletud Riigikohtu 9. detsembri 2008. a otsuses tsiviilasjas 3-2-1-103-08, kus kolleegium viitas Saksamaa Liidukohtu praktikale, kus on ärisaladust defineeritud järgmiselt: "Ärisaladus on asjaolu, mis on seotud ettevõtlusega, mida teab piiratud ring isikuid ja mille saladuses hoidmise tahe ettevõtja poolt peab olema kas dokumenteeritud või vähemalt selgelt äratuntav."(OÜ LabelPrint hagi AS-i ESTOPRESS ja Eero Lattu vastu solidaarselt 2 000 000 krooni kahjuhüvitise saamiseks, AS-i ESTOPRESS vastu konkurentsi kahjustava tegevuse lõpetamiseks ning Eero Lattu vastu kohustamiseks mitte kasutama ning avaldama kolmandatele isikutele OÜ LabelPrint ärisaladusi, 2008). Riigikohtu 09.12.2008 otsuses nr. 3-2-1-103-08 kui ka Riigikohtu 10.05.2017 otsuses nr. 3-2-1-36-17 on kolleegium märkinud, et ettevõtja enda kohustus on tõendada asjaolusid, mis võimaldaks teavet lugeda ärisaladuseks ja milles seisneb ärisaladuse õigustamatu avaldamine (OÜ LabelPrint hagi AS-i ESTOPRESS ja Eero Lattu vastu solidaarselt 2 000 000 krooni kahjuhüvitise saamiseks, AS-i ESTOPRESS vastu konkurentsi kahjustava tegevuse lõpetamiseks ning Eero Lattu vastu kohustamiseks mitte kasutama ning avaldama kolmandatele isikutele OÜ LabelPrint ärisaladusi, 2008; Pindi

Kinnisvara OÜ hagi Osaühingu Sholas vastu 27 000 euro suuruse leppetrahvi ja viivise saamiseks, 2017).

17.11.2018 jõustus ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus (edaspidi EKTÄKS) ärisaladuse kaitse direktiivi üle võtmiseks Eesti siseriikliku õigusesse, kus on defineeritud muuhulgas ärisaladuse mõiste (Värv, 2020, lk 418). EKTÄKS §5 lg 2 järgi ärisaladuse teave ei tohi olla üldteada või kergesti kättesaadav, teabel peab olema kaubanduslik väärtus salajasuse tõttu ning selle üle seaduslikku kontrolli omav isik peab rakendama vajalikke meetmeid teabe saladuses hoidmiseks. (Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus[1], 2018)

Maksuhaldurile teatavaks saanud konfidentsiaalsete andmete kaitsmine on väga oluline. Riik peab austama ettevõtete ettevõtlusvabadust ja omandiõigust ning ettevõtjal on õigus eeldada, et tema ärisaladus on kaitstud. Selliste andmete avaldamine oleks ettevõtlusvabaduse ja omandiõiguse riive, milleks peab olema õiguslik alus ning andmete avaldamine peab olema vajalik. (Lind, 2009, lk 458)

Lisaks MKS-le reguleerib maksusaladust Euroopa Ühenduse tolliseadustiku (nõukogu määrus 2913/92) artikkel 15: „Kogu konfidentsiaalse või konfidentsiaalselt edastatud teabe kohta kehtib ametisaladuse hoidmise kohustus. Toll ei avalda teavet ilma seda andnud isiku või ametiasutuse otsese loata; teabe edastamine on lubatud, kui see on tolli kohustus või tollil on õigus seda teha vastavalt kehtivatele õigusaktidele, eriti andmekaitse küsimustes või seoses kohtumenetlusega.“ (Euroopa Ühenduste Nõukogu, 1992). Sellega tolliseadustiku regulatsioon maksusaladuse puhul piirdub (Lind, 2009, lk 455).

Eesti Maksumaksjate Liit esitas 25.11.2015 Maksu- ja Tolliametile teabenõude, kus sooviti teada, kui palju on aastatel 1991-2015 lahkunud ametnikke ja töötajaid Maksu- ja Tolliametist (ja tema eelkäijatest) ning kuidas MTA kontrollib maksusaladuse hoidmise kohustuse täitmist. Kas MTA-l on ülevaade, kus need inimesed elavad, töötavad, millega tegelevad, kui palju on seotud ettevõtlusega, kus saab kasutada maksuametnikuna töötamise ajal kogutud teavet jne. MTA selgitas oma vastuses, et tulenevalt MKS § 26 lg 1 alusel ei lõpe maksusaladuse hoidmise kohustus teenistus- või töösuhte lõppemisega ning sellise kohustuse rikkumise korral on ette nähtud vastutus avaliku teabe seaduse § 54^1 ja karistusseadustiku § 157 ja § 157^1 alusel, olenevalt andmete sisust. Järelevalve ja kontrolli kohustus maksusaladuse hoidmise kohustuse rikkumise korral lasub Politsei- ja

Piirivalveametil ning Andmekaitse Inspektsioonil. MTA-l puudub seaduslik alus töödelda ametist lahkunud teenistujate isikuandmeid, kui tegemist on maksusaladuse hoidmise kohustuse rikkumise kahtlusega. Kuid MTA sisekontrolli osakond kontrollib regulaarselt oma teenistujate poolt maksusaladuse hoidmise kohustusest kinnipidamist ja rikkujate suhtes rakendatakse distsiplinaarkaristust. Samuti jälgitakse, et ametnikud töötleksid piiratud juurdepääsuga teavet vaid tööalasest vajadusest lähtuvalt ja amet on rakendanud infoturbemeetmed, et kaitsta teavet volitamata töötlemise eest. (Eesti Maksumaksjate Liit, 2016, lk 8–9)

Kokkuvõtvalt, andmete kaitse on sätestatud erinevates seadustes ja määrustes ning selle eesmärk on andmeid kaitsta igasuguse ohu eest. Andmekaitsetingimused on väga ranged, kuid andmete töötlemise võimalused on autori arvates piisavalt laialdased, et ka asutustevahelist suuremat andmevahetust võimaldada, kuna töötlemine on siiski õigustatud kui tegevus on piisavalt põhjendatud ja on ära näidatud, milles seisneb töötlemise vajalikkus ning õiguste riive on väiksem kui andmete töötlemisest saadav kasu.

1.2. Võimalused maksumaksjate kesksel profileerimisel

Järgnevas alapeatükis püütakse defineerida avalikku huvi ja tuua erinevaid lahendusi andmete töötlemiseks, mida ilmestatakse võimalustega, mis suurem andmevahetus kaasa tooks ning COVID-19 perioodi andmevahetuse näidetega nii Vabariigi Valitsuse kehtestatud eriolukorra kui ka hilisemate piirangute ajal.

Ameerika anglosaksi õigussüsteem on erinev Eestis kasutusel olevast Mandri-Euroopa õigussüsteemist, kuid õiguse üldpõhimõtted on õigussüsteemides üldjoontes ühised. Seepärast on asjakohane välja tuua Pennsylvania kohtulahend, mis leidis, et avalik huvi ja üksikisiku andmete kaitse saavad olla tasakaalus, ilma kahjustama teineteist (Schoenberger, 2010, p. 591).

Avaliku huvi mõiste sisu lahti seletamine on keerukas ja pigem subjektiivne (Carter & Bouris, 2006, p. 5). Avaliku huvi kui õigusliku aluse eelis on see, et antud mõiste annab kasuliku mehhanismi otsuste vastuvõtmiseks, mis nõuavad erapooletut kaalumist ja omavahel konkureerivate üldsust puudutavate küsimuste hindamist (Paterson & McDonagh, 2017, p. 192). Lippmanni (1955, p. 40) arvates on avalik huvi see, mille inimesed valiksid, kui nad näeksid selgelt, mõtleksid ratsionaalselt, tegutseksid

omakasupüüdmatult ja heatahtlikult. Lippmann (1955, p. 40) osundab ka sellele, et avalik huvi on tihti segatud indiviidide isiklike huvidega. Kohtud kontrollivad avaliku huvi olemasolu nö „avaliku huvi testi“ kaudu. Testis hinnatakse erinevaid konkureerivaid aspekte ja kuidas need on tasakaalus, sealhulgas hinnatakse ka valitsuse huvisid. (Paterson & McDonagh, 2017, p. 192)

Üksikisikute huvi on nende isikuandmete eemaldamine, kuid avalik huvi on andmete eemaldamata jätmine. Avalik huvi võib olla sätestatud erinevates siseriiklikes seadustes, kus on sätestatud, et andmete säilitamine paarist aastast kuni igavesti on avalik huvi. See tuleneb omakorda huvist säilitada kultuuripärandit või hoida andmeid kättesaadavana ning andmetest, mis võivad või on olnud vajalikud avalikes aruteludes. (Klingenberg, 2016, p. 70)

COVID-19 puhangu vastu võitlemisel on valitsused üle maailma teinud koostööd erasektori tehnoloogia- ja tervishoiuasutustega, et täiendada jälgimise ja järelevalvesüsteeme, mis oluliselt vähendavad isikute privaatsust (Brough & Martin, 2021, p. 108). Paljud andmekaitse seadused lubavad kriisi ajal leevendada andmete töötlemise piiranguid, kuna see on avalikes huvides (Meyer, 2020). Näiteks Euroopa Liidu isikuandmete kaitse üldmääruse (GDPR) kohaselt on tavaliselt kaitstud kategooriateks geneetilised andmed, poliitilised ja religioossed sidemed ning kriminaalne ajalugu, kuid kriisiolukordades saab neid vabalt jagada (Meyer, 2020).

Eestis, sarnaselt teistele riikidele, võeti samuti kasutusele erinevaid meetmeid COVID-19 vastu võitlemiseks ja majanduse toetamiseks kriisi mõjude leevendamiseks eriolukorra ajal ja sellele järgneval perioodil. Näiteks täiendati MKS-i paragrahviga 168[15], mis lubab avaldada maksusaladust sisaldavat teavet valitsusasutustele ja isikutele, kes on kohustatud läbi vaatama ja rakendama meetmeid COVID-19 haigust põhjustava koroonaviiruse levikust mõjutatud ettevõtjate ja isikute toetamiseks (Maksukorralduse seadus[1], 2002). Selline meede annab võimaluse tutvuda ettevõtete finantsseisundiga ja tuvastada need ettevõtted, kes vajavad enim abi ning rakendada vajalikke toetusmeetmeid.

Ettevõtted nagu *Amazon.com, iTunes* ja *Netflix* salvestavad kasutajate klikke, vaatamisi ja tellimusi ning kaevandavad neid andmeid tähendust omava informatsiooni töötlemiseks, et mõjutada kliente soovituste, lisavalikute ja reklaamidega. Mida rohkem on ettevõte informeeritud tarbija eelistustest, seda paremini on võimalik kliente suunata võimalike

edasiste võimalusteni, mida nad muidu ei oleks pruukinud leida. (Dziuban, *et al.,* 2012, p. 21) Erasektori kogemusi saab rakendada ka avalikus sektoris, mida tõestab uue avaliku halduse kontseptsioon (inglise keelne lühend *NPM*). Kontseptsiooni eesmärk on parandada avaliku halduse tegevust, kasutades erasektoris tõhusaks osutunud lahendusi. Uue avaliku halduse kontseptsiooni aluseks on erasektori ettevõtete ärimudelite rakendamine avalike teenuste kvaliteedi parandamiseks. (Gębczyńska, & Brajer-Marczak, 2020, p. 1)

Avalik sektor on üha enam orienteeritud tulemuslikule juhtimisele, kuna kodanikud, uued IT lahendused ja kasvav majanduslik konkurents nõuavad tõhusaid ja tulemuslikke lahendusi (Gębczyńska, & Brajer-Marczak, 2020, p. 2; Bryson, *et al.,* 2014, p. 445). Riigiasutused peavad uutele väljakutsetele ja probleemidele reageerides mõtlema ja tegutsema strateegiliselt ning olema võimelised oma tulemuslikkust mõõtma nii lühi- kui pikaajalist perspektiivi arvesse võttes (Moore, 1995, p. 10). Avaliku sektori asutused ei ole orienteeritud kasumlikkusele, mille tõttu ei saa asutuste tulemuslikkust hinnata läbi kasumi. Kuid avaliku sektori asutuste loodud lisandväärtus võib olla suurem kui erasektoris, kuna lisandväärtuse loomisel on määrav avalik huvi, mitte kasumlikkus. (Gębczyńska, & Brajer-Marczak, 2020, p. 4) Lühiajalises perspektiivis tuleks avalikke teenuseid hinnata klientide rahulolu kaudu. Kui klientide hinnang on hea ja pakutav avalik teenus on tulemuslik, võib see omakorda tuua pikaajalist positiivset mõju ühiskonnale. (Gębczyńska, & Brajer-Marczak, 2020, p. 4)

Pöördudes tagasi riigiasutuste soovi juurde andmevahetust suurendada, on Eestis kavandatud ka varasemalt massandmete töötlusel põhinevaid suuri süsteeme. 2019. aastal jõudis testimisse riiklik e-majutuskaardi lahendus, kuna majutuskaartide teavet koguti paberkujul ning üldjuhul seda ei viidud ühtsele elektroonilisele kujule ega laetud ühtsesse kesksesse süsteemi. Majandus- ja Kommunikatsiooniministeeriumi kaubanduse ja teenuste talituse nõuniku K.Kikase sõnul on andmetöötlus automatiseeritud ning inimeste nimesid tuvastatud kujul ei liigu. Kui andmed langevad kokku tagaotsitava inimesega, siis jõuab registreering politseisse. Riigile edastatakse majutuskaardid, mille andmed saab ühendada tagaotsitavate loeteluga, et leida kattuvused, mille põhjal saab algatada õiguskaitsetoiminguid. Selline andmekogu sisaldab endas ka palju riske. Tehniliselt on võimalik andmestikust tuvastada inimeste omavahelisi isiklikke kontakte, mis võib viia laialdase eraelu riiveni. Kuid sellist süsteemi luues juurutatakse nii organisatoorseid kui ka

tehnilisi infoturbe meetmeid, mis kahandavad mitte-eesmärgipärase andmetöötluse tõenäosust. (Bogdanov & Siil, 2020, lk 476)

GDPR artikkel 39 käsitleb andmekaitsealast mõjuhinnangut, mis tähendab seda, et kui võetakse kasutusele näiteks uut tüüpi tehnoloogia või andmete töötlemisel tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht, isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes, tuleb vastutaval töötlejal hinnata enne isikuandmete töötlemist toimingute mõju isikuandmete kaitsele. Mõjuhinnangu tegemine on näiteks nõutav artikli 39 lg 2 p a järgi juhul, kui andmete töötlemisega teostatakse füüsiliste isikutega seotud isiklike aspektide süstemaatilist ja ulatuslikku hindamist, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut. (Euroopa Parlament ja Euroopa Nõukogu, 2016)

Üldmääruse kohaselt ei pea mõjuhinnangu dokumente, järelevalvega konsulteerimisi ega üldisemalt lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete juurutamist avalikustama. Erialakirjanduses on leitud, et andmekaitse mõjuhinnangu avalikustamine vähemalt riigi IT-lahenduste kohta on oluline, tagamaks huvipoolte õiguste kaitse. Isikuandmete kaitse üldmäärusega on loodud vajalikud mehhanismid selleks, et riik töötleks massisikuandmeid vastutustundlikult, kuid nende tegelik täitmine on raskesti hinnatav. Info puudumise tõttu ei saa hinnata, kas riik täidab andmetöötluse norme. Selle tõttu ei saa esitada muuhulgas parandusettepanekuid, kui riigi andmetöötluses esineb puudusi. (Bogdanov & Siil, 2020, lk 480)

Riigisisese andmekaitsealase õigusruumi arendamisel tuleks kaaluda, kas ja mis tingimustel avaldada informatsiooni isikute põhiõigustele kaasnevate riskide ja nende maandamise viiside kohta, mis tulenevad riiklikest IT-lahendustest. Üks võimalus selleks on kehtestada nõue, et enne IT-lahenduse arendamiseks vajaliku riigihanke korraldamist tuleb selle nõuete väljatöötamiseks teha andmekaitsealane mõjuhinnang, mille tulemused avaldatakse vähemalt arendatava IT-lahenduse hankedokumentatsioonis. Teiseks tuleks selgelt dokumenteerida ja avalikustada teave, millistel juhtudel riigi infosüsteemides isiku andmeid masstöödeldakse. Avalik huvi on teada ja mõista, kuidas kasutatakse massandmeid kui üksikisikute kohta koondatud andmeid ja kas selline kasutusviis on ühiskonnas vastuvõetav. Kolmandaks avalikkusele peaks olema läbipaistev, millistel

muudel eesmärkidel samu isikuandmeid töödeldakse. Kodaniku vaatest on oluline jälgida, et andmetele juurdepääs oleks eesmärgipärane ja piisavalt kontrollitud ega väljuks põhiseadusega kehtestatud raamidest. (Bogdanov & Siil, 2020, lk 480)

Finantsvaldkonnas on erinevad andmed kaitstud erinevalt, tulenevalt avalikust huvist, üksikisikute huvist või ettevõtete huvist. Enamasti on andmed kaitstud isikuandmete andmekaitsega, kuid ka avaliku sektori sõjalise, julgeoleku- või äritegevusega seotud andmekaitsega. Riigil on õigus kuulutada riigisaladuseks konkreetsed andmed, millega võimuorganid, asutused, ettevõtted ja institutsioonid kokku puutuvad või mida nad kasutavad oma kohustuste ja ülesannete täitmisel ning mille olemus nõuab riigisaladuse tasemel olevat konfidentsiaalsust. Teisalt on tänapäeval nõutav riiklike vahendite haldamise läbipaistvus. Läbipaistvus on üks korruptsiooni, pettuste ja rahapesu vastu võitlemise põhimõtetest ja viisidest. (Sudžuka, 2020, p. 2)

Siinkohal on oluline peatuda X-tee arendusel ja seletada lahti, mis on riigi infosüsteemide andmevahetuskiht X-tee. See on tehniline ja organisatsiooniline keskkond, mis võimaldab korraldada turvalist veebipõhist andmevahetust riigi infosüsteemide vahel. X-tee võimaldab asutustel ja inimestel turvaliselt andmeid vahetada, samuti korraldada isikute juurdepääsu riigi andmekogudes säilitatavatele ja töödeldavatele andmetele. (Tupay & Mikiver, 2015, lk 164)

X-tee rajamisel sõnastati 2003. aastal andmekogude uute normide põhipostulaadid, kus leiti, et ühe ametkonna poolt avalike ülesannete täitmiseks kogutavad andmed kuuluvad riigile tervikuna, mitte sellele ametile, kes andmeid kogus. Avaliku halduse jaoks oluline info peaks olema kättesaadav, kas ühest kohast või ühtsest integreeritud ja andmete ristkasutuses olevast süsteemist. Tänu avaliku halduse piires lõimitud infosüsteemile on asutustel võimalus pakkuda uusi innovatiivseid avalikke elektroonilisi teenuseid. Integreeritud registrite süsteem võimaldab rakendada uusi halduskorralduse põhimõtteid: kodanikukesksus, paindlikkus, kiirus, väiksem raha- ja ajakulu nii kodanikule kui ka riigile. (Tupay & Mikiver, 2015, lk 165)

Eesti Inimõiguste Keskus viis 2019. a läbi uuringu, kus üheks teemaks oli profileerimine. Uuringus kirjeldati proaktiivse teenuse tähendust, mis on uut tüüpi avalik teenus, mida riik osutab omal algatusel. Proaktiivne teenus tähendab ennetavat või ettehoolitsevat teenust. Kui tavaliselt pöördub kodanik toe saamiseks riigi poole, siis proaktiivse teenuse puhul

teeb seda riik ise. Proaktiivset teenust osutatakse automaatselt eeldades isiku tahet teenust saada või isiku nõusolekul kasutades riigi infosüsteemi kuuluvate andmekogude andmeid. (Eesti Inimõiguste Keskus, 2019, lk 14)

Samas uuringus leiti profileerimise ja selle käigus pakutavate proaktiivsete teenuste plussina, et teenused aitavad tagada õigust võrdsele kohtlemisele, kuna teenused jõuavad rohkem inimesteni, kes neid vajavad, aga ei ole teenuseid saanud, kas teadmatusest või muudel põhjustel. Teisalt leiti, et profileerimine võib ohustada õigust olla mitte diskrimineeritud, kuna andmed võivad olla ebatäpsed, mittetäielikud või ajalooliste andmete tõttu eelarvamustega. Samuti toodi negatiivsena ohu võimalikkust eraelu puutumatuse õigusele ja isikuandmete kaitse õigusele, kuna proaktiivse teenuse puhul võib ohustatud olla inimese autonoomia ja valikuvabadus. Proaktiivsete teenuste pakkumisel tekkivate ohtude kõrvaldamiseks nähti lahendustena põhjalikku eelnevat analüüsi ning isikuandmete kasutamise terviklahenduse loomist, kust nähtuks isikuandmete kasutamine riigis teenuste lõikes ning mis võimaldaks loobuda isikuandmete kasutamise nõusolekust või esitada vastuväiteid automatiseeritud profileerimisel. (Eesti Inimõiguste Keskus, 2019, lk 15 – 16)

Vabariigi Valitsuse „Eesti 2035“ strateegias on kavatsetud vajalike muutustena viia teenused võimalikult palju taustal toimivaks ja etteaimatavaks ehk proaktiivseks. Sealjuures tuleb arvestada inimese tahte ja põhiõigustega, kuna proaktiivsete teenuste kasutamise puhul eeldatakse kõigi riigil olemasolevate andmete turvalist kasutamist. (Eesti Vabariigi Valitsus, 2021b)

Peale uue tehnoloogia kasutuselevõttu üldjuhul kasvab oluliselt tulemuslikkus, kuid kaasnevad ka teatud kulud. Targad investeeringud tehnoloogiasse aitavad meil tuttavaid ülesandeid lahendada efektiivsemalt ning asuda lahendama uusi ülesandeid, mis valdkonna või terviku võimekust suurendavad. Kuid riigid ja ettevõtted pole harjunud suurte andmehulkade ligipääsuga, mida oleks võimalik kasutada oluliste ja kiirete otsuste tegemisel, mis annaks riigile suure konkurentsieelise. Asutustele kogunenud andmeid käsitletakse kohustusliku arhiivimaterjalina ning tihti ei saada aru andmete vajalikkusest. (Karu, 2021, lk 44–45)

Avalik huvi on igaühe enda defineerida, kuna see on tihti segatud isiklike huvidega. COVID-19 kriisiga kaasnev vajadus toetada ühiskonda andis võimalused kiireks

andmevahetuseks ja koostööks, mida alljärgnevas peatükis uuritakse ka intervjueeritavatelt.

Varasemates peatükkides jõuti järelduseni, et avalikus sektoris lisandväärtuse loomisel on määrav avalik huvi, mitte kasumlikkus ja kui avaliku sektori pakutav teenus on tulemuslik, võib see tuua pikaajalist positiivset mõju ühiskonnale. Autor peab avalike teenuste positiivset mõju avalikuks huviks, mis loob lisandväärtust. Andmekaitsekaasuste lahendamisel tuleb lähtuda mõistlikkusest ja proportsionaalsuse põhimõttest. Avaliku huvi olemasolu kontrollimisel hinnatakse erinevaid konkureerivaid aspekte ja kuidas need on tasakaalus, mida tehakse ka andmekaitsekaasuste lahendamisel. Sellest võib järeldada, et kui andmekaitsetingimusi ning avaliku huvi olemasolu hinnatakse ja kontrollitakse sama objektiivselt, siis on võimalik saavutada olukord, kus üks ei pea kahjustama teist, mida leidis ka Pennsylvania kohtulahend. (käesolev töö, lk 16, 18)

Kui arvestada riigiasutuste varasemaid kogemusi massandmete töötlusel, mis võivad põhjustada laialdast eraelu riivet, võib öelda, et andmetöötluse tingimuste rikkumisi on võimalik vähendada, kui süsteemi loomisel juba juurutatakse nii organisatoorseid kui ka tehnilisi infoturbemeetmeid. (käesolev töö, lk 18) Maksumaksjate keskse profileerimise puhul on kindlasti vajalik ka andmekaitsealase mõjuhinnangu koostamine, et hinnata asutuste vahelise andmevahetuse suurendamise kooskõla andmekaitsetingimustega, mida soovitatakse teaduskirjanduses avalikustada selleks, et tagada huvitatud isikute õiguste kaitse. Erialakirjanduses rõhutatakse riigi läbipaistvust, mille tõttu on avaliku huvi tõttu näiteks finantsõiguse valdkonnas andmed kaitstud erinevalt. (käesolev töö, lk 19) Maksumaksjate profileerimisel kaasnevad kindlasti teatud ohud, mida ka Eesti Inimõiguste keskuse läbiviidud uuringus mainiti. Autori arvates on võimalik olukorda lahendada samas uuringus pakutud võimalustega, milleks oli põhjalik eelnev analüüs ja isikuandmete terviklahenduse loomine, kus on võimalik loobuda isikuandmete kasutamise nõusolekust või esitada vastuväiteid, mis omakorda suurendaks riigi läbipaistvust. (käesolev töö, lk 20-21)

2. MAKSUMAKSJATE KESKNE PROFILEERIMINE ASUTUSTE ANDMEVAJADUSTE TÄITMISEL JA TOETUSTE MÄÄRAMISEL

2.1. Uurimismetoodika kirjeldus

Alapeatükis antakse ülevaade lõputöös kasutatud andmekogumise ja andmeanalüüsi metoodikast. Uurimismeetodina kasutatakse lõputöö eesmärgi saavutamiseks kvalitatiivset uurimismetoodikat, mille puhul tõlgendatakse asju nii, nagu neist aru saadakse ja püütakse ennekõike leida ja avalikkuse ette tuua tõsiasju, mitte tõestada olemasolevaid väiteid (Hirsjärvi, *et al.*, 2007, lk 151–152).

Andmeanalüüsi meetodina kasutatakse kvalitatiivset sisuanalüüsi (Laherand, 2008, lk 45). Andmekogumise meetodina kasutatakse ekspertintervjuusid, sest lõputöö eesmärgi saavutamiseks on oluline teada erinevate riigiasutuste arvamust teemast, et välja selgitada maksumaksjate keskse profileerimise vajalikkus ja võimalused selle teostamiseks, kuna ekspertidel on olemas teadmised praegusest andmevahetuse toimimisest ja seeläbi on neil ka paremad ideed või nägemused andmevahetuse parendamiseks olemasoleva süsteemi pinnalt. Valimiks on mittetõenäosuslik eesmärgistatud valim, milleks on ekspertintervjuud EAS, Haigekassa, KIK, MTA, PRIA, Sotsiaalkindlustusameti, Töötukassa, ning Tallinna Kesklinnavalitsuse Sotsiaalhoolekandeosakonna esindajatega. Mittetõenäosusliku eesmärgistatud valimi eesmärk on saada tulemused asutuste ametnikelt, kes on ettekavatsetult valitud kindlate kriteeriumite alusel, kuna muud meetodid ei annaks autorile tõepäraseid tulemusi (Õunapuu, 2012; Bryman, 2012, p. 418). Kriteeriumiteks on: intervjueeritav on avaliku sektori asutuse ametnik, kes on töötanud vähemalt 3 aastat enda asutuses või omab kogemust sarnases valdkonnas vähemalt üle 5 aasta, ning asutus, kus intervjueeritav töötab, väljastab rahalisi toetusi või peab järelevalvet asutuste töö üle. Töö autor otsis asutuste kodulehelt kontaktid tutvudes kõigepealt asutuse struktuuri ja tegevustega ning seeläbi valis autor sobiva osakonna ja isiku tutvudes eelnevalt isiku ametijuhendiga. Intervjueeritavatele saadeti interjuus osalemise kutse e-kirjana, kus küsiti isiku tööstaaži, et veenduda intervjueeritava sobivuses. Kui isik ei sobinud valimisse, siis soovitas ta enda teist kolleegi, kes kõige paremini tunneb autori lõputöö teema valdkonda. Kokku intervjueeriti 13 eksperti, intervjuud kestsid 40 kuni 89 minutit (vt tabel 1). Üldjuhul

peetakse optimaalseks intervjueeritavate arvuks 12, mil hakkab tekkima saturatsioon (Bryman, 2012, p. 426). Seega peab autor 13 intervjuud piisavaks, et saada ülevaade maksumaksjate keskse profileerimise vajalikkusest ja võimalustest. Autoril oli ettevalmistatud 21 küsimust, millele lisandus lisaküsimusi sõltuvalt eksperdi tegevusalast (vt lisa 1).

Tabel 1. Intervjueeritavate nimekiri (autori koostatud)

Nimi	Asutus	Ametikoht	Tööstaaž (aastates)	Intervjuu pikkus (minutites)
Kristo Kraanat	Ettevõtluse Arendamise Sihtasutus	järelevalve osakonna valdkonnajuht	3,0	45,0
Pille Banhard	Haigekassa	juhatuse liige	13,0	89,0
Kadri Haller-Kikkatalo	Haigekassa	analüütika osakonna juhataja	4,0	55,0
Sander Klaos	Keskkonna Investeeringute Keskus	riskiosakonna juht	1,5+10,0	48,0
Herje Vahemäe	Maksu- ja Tolliamet	maksuauditi osakonna üksuse juht	19,5	40,0
Kaili Veiksaar	Maksu- ja Tolliamet	avalike teenuste valdkonna teenusejuht	1,5+15,0	59,0
Külli Külm-Kivistik	Maksu- ja Tolliamet	avalike teenuste valdkonna teenusejuht	22,0	77,0
Kadri Koel	Põllumajanduse Registrite ja Informatsiooni Amet	eelarve- ja analüüsiosakonna juhataja	17,0	58,0
Rando Undrus	Põllumajanduse Registrite ja Informatsiooni Amet	nõunik	9,0	58,0
Kati Kümnik	Sotsiaalkindlustusamet	hüvitiste osakonna juhataja	15,0	60,0
Monika Roosnupp	Tallinna Kesklinna Valitsus	sotsiaalhoolekande osakonna juhataja asetäitja	26,0	-
Raigis Urban	Tallinna Kesklinna Valitsus	toetuste talituse vanemspetsialist	7,0	45,0
Siiri Koplimaa	Töötukassa	siseauditi juht	3,0	63,0
		KESKMINE:	11,7	58,1

Intervjuud viidi läbi peamiselt video vahendusel kasutades *MS Teams* või *Skype for Business* keskkonda. Üks intervjueeritav edastas oma vastused e-kirja teel ning ühe intervjueeritavaga viidi läbi kohtumine intervjueeritavale sobivas kohas. Intervjueeritavate keskmine tööstaaž oma asutuses on 11,7 aastat ning keskmise intervjuu kestvus oli 58,1 minutit (vt tabel 1). Kõik intervjueeritavad andsid loa nende nimede avaldamiseks lõputöös.

Intervjuude tulemused transkribeeriti ja neid hoiustatakse autori valdustes, kuna transkriptsioonid on väga mahukad. Sisuanalüüsi käigus koostati kategooriate ja koodide tabel selleks, et saada vastused uurimisküsimustele (vt käesoleva töö lisa 2). Kokku moodustati 5 kategooriat, mis jaotusid järgmiselt: praegused probleemid andmevahetusel (14 koodi), andmekaitsega seotud probleemid (7 koodi), avalik huvi andmevahetuse suurendamisel (11 koodi), riigiasutuste andmevahetuse vajadused (10 koodi) ja riigiasutuste suurema andmevahetuse ja ühtse riskiprofiili loomise võimalused (15 koodi).

Hirsjärvi, *et al*. (2007, lk 193) toovad välja intervjuu usaldusväärsuse ohuna intervjueeritavate kalduvuse anda sotsiaalselt soovitatavaid vastuseid. Kuna ametnikuna ei saa alati avaldada oma arvamust, kui see võib kahjustada asutuse mainet, on vajalik töö autori arvates ekspertide vastuseid teatud küsimustes põhjalikumalt hinnata.

2.2. Andmevahetuse suurendamise probleemid

Autor uuris, millised võimalused on asutustel tutvuda maksumaksjatega seotud andmetega teise asutuse juures ning millistest andmetest nad oma ülesannete täitmisel enim puudust tunnevad. Järgnevas alapeatükis analüüsitakse ekspertide hinnanguid hetkel andmevahetust takistavate probleemide ja andmekaitsenõuetest tingitud mõjutuste osas, mille tõttu on asutuste vaheline koostöö andmete vahetamisel autori arvates pigem ebaühtlane, ebapiisav ja ajas maha jäänud.

Sissejuhatuses defineeris töö autor „maksumaksjate keskset profileerimist“ andmevahetuse suurendamisena erinevate asutuste vahel, et tagada ühtsem profiil maksumaksjatest, paremate teenuste pakkumiseks ja pettuste vältimiseks, mis võimaldaks ajakohaseimat kuva maksumaksjatest (käesolev töö, lk 5). Ekspertidelt küsiti samuti, kuidas nemad defineeriksid „maksumaksjate keskset profileerimist“ selleks, et teada, milline on ekspertide nägemus ja mõista paremini nende hinnanguid.

Eksperdid defineerivad maksumaksjate keskset profileerimist maksumaksjaga seotud andmete mustritena kasutamist või maksumaksja info kogumisena, mis on samu hindamispõhimõtteid kasutav ning mida on võimalik kasutada ka teistel asutustel peale andmete haldaja. Seejuures peaks saama seda ühes aknas kuvada (inglise keelne väljend *single window*) ja läbi maksumaksjate keskse profileerimise määrata kliendile parima teeninduskanali.

Esimene kategooria, mida töö autor analüüsis oli **praegused probleemid andmevahetusel**. Üldiselt hindavad asutused olemasolevat infot maksumaksjatega seotud andmete osas piisavaks, kuid intervjuude käigus toodi välja mitmeid erinevaid andmeid, millest nad oma töös puudust tunnevad (kood 1). Intervjueeritavad tõdesid, et ajakohasemad ja täpsemad andmed parendaksid nende asutuste protsesse ja aitaksid teha paremaid otsuseid eriti toetuste määramisel. Kohaliku omavalitsuse esindaja sõnul võib teatud juhtudel mõne paarikümne eurose toetuse väljamaksmiseks olla vajalik mitme ametniku kaasamine, kes võivad tegeleda ühe juhtumiga terve päev, mis toob kaasa ebaproportsionaalse halduskoormuse (Urban, 2021).

Mitmed asutused tõid näiteid dubleerimistest (kood 2) ja ressursside raiskamisest. Näiteks on võimalik rehabilitatsiooniteenuseid saada erinevate asutuste kaudu, kuid isik võib lõpuks minna ühte kohta teenust saama. Selleks, et seda teenust saada, peavad erinevad asutused menetlema sisuliselt sama asja ja samuti peab klient asju ajama erinevates asutustes. Asutused on üksmeelel, et rehabilitatsiooni teenuse andmisel võiksid asutused rohkem koostööd omavahel teha ja maksumaksja kui ka asutuste enda koormust selle läbi vähendada. Eksperdid mainisid ka seda, et andmeid kirjeldatakse liigselt erinevatesse kohtadesse ning samu andmeid saadetakse erinevaid kanaleid pidi. Ressursside raiskamise näitena tõi PRIA, et sageli kui hakatakse arendama mingit andmebaasi või andmeid ühendama ei kaasata teisi asutusi, vaid suurarendaja teeb seda iga asutuse juures eraldi ja küsib sama raha kliendihaldusbloki arendamise eest, kuigi see on korduvkasutatav (Undrus, 2021). Uue andmevahetuse kanali loomisel on tihti vajalik ehitada uus X-tee juurdepääs, mis on keerukas ja aeganõudev protsess, seega hea lahendus võib omakorda jääda rahastuse puudumise taha.

Autori arvates saaks halduskoormust vähendada teatud andmete parema kättesaadavusega ning maksumaksja peaks seejuures mõistma ja tolereerima, et kvaliteetse abi saamiseks on vajalik abistajal ehk riigil kõige ajakohasemat ja täpsemat infot sarnaselt olukorras, kui helistatakse hädaabi numbrile. Kui andmeid vahetada suuremal määral kui praegu, siis väheneksid oluliselt halduskulud. Näiteks on ametnikul võimalik lahendada samas ajaühikus olulisemalt rohkemate maksumaksjate vajadusi, kui ta ei pea kulutama tarbetult palju aega sellele, et otsida, kuidas isikuga kontakti saada, kuna tema kasutuses olevas registris on andmed vananenud. Vaid tal on olemas kõige ajakohasemad ja uuemad andmed, mida teised asutused on isiku kohta tuvastanud.

Viimati kirjeldatust tuleneb järgmine probleem ehk andmed on ühes asutuses hoiul ja ei jõua vajalikus ulatuses või ajal teise asutuseni (kood 4). Enim tuntakse puudust toetuste infost ehk kui palju ja millisest asutusest on keegi toetust saanud või millised probleemid ja võimalikud pettuse kahtluse riskid on toetuse taotlejal tuvastatud (kood 3). Toetustega seotud info on vajalik näiteks riigiabi suuruse hindamiseks, et oleks võimalik jälgida, millal võib olla tegemist keelatud riigiabiga, samuti tagamaks toetuste väljamaksmine õigustatud isikutele ning vältida skeeme toetuste taotlemisel.

„Võib juhtuda olukord, kus taotletakse mitmest asutusest toetust, toetuse summa ületab asja maksumust ja meil ei ole nii head süsteemset kontrolli, ehk kui palju on keegi toetuseid maksnud.“ (Klaos, 2021).

Mitmed asutused sooviksid ka paremat maksudega seotud infot, mis oleks ajakohasem ja detailsem, kui nad seda tänasel kujul avaandmete kaudu saavad. PRIA esindajate hinnangul on neil hulk avaandmeid, kuid kehv X-tee (käesolev töö, lk 20) kaudu andmete vahetamise võimalus MTA-ga. Nii EAS, KIK kui ka PRIA esindajad leidsid, kui neil oleks ajakohane ülevaade maksumaksjatest maksualasest käitumisest ja tuvastatud maksuriskidest, tooks see nende protsessides kasu ja nad lähtuksid oma töös saadud infost.

Andmete koondumine eraldi asutuste kätte tuleneb nii seadusandluse piirangutest andmete vahetamisel (kood 5) kui ka asutuste eriarvamustest (kood 13) õiguse tõlgendamisel. Asutuste vahel toimub koostöö nii otsekontaktide kui andmebaaside põhiselt sõltuvalt infovahetuse liigist, samas on asutuste vahelise koostöö hindamisel andmete vahetamisel asutuste arvamused väga erinevad. Suurima puudusena tuuakse välja seadusandluse piiranguid andmete saamisel, kirjeldades järgmist:

1) andmevahetust ei ole õigusaktides piisavalt reguleeritud;
2) MKS-s sätestatud maksusaladuse kaitse ei lase andmeid avaldada ehk andmete avaldamise võimalused ei kata piisavalt asutuste andmevahetuse vajadusi ;
3) pangasaladuse avaldamise piirang ja erinevad muud andmekaitsealased piirangud takistavad andmevahetust, mida töö autor käsitles ka varasemates peatükkides andmevahetuse takistustena.

Autori ja ekspertide arvates on suureks probleemiks ka see, et asutustel puudub ühtne ülevaade, kust mingit infot on võimalik saada ja millist infot on üldse võimalik saada (kood 6).

„*Peaks olema hügieenireegel või standard, kes iganes hakkab e-riigis oma teenuseid arendama, siis tal on olemas teine vihik või fail, kus on näha, et neid andmeid ma saan sealt, neid ma saan sealt.“* (Undrus, 2021).

Kui pöörduda tagasi eriarvamuste probleemi püstituse juurde, siis autori arvates tekivad eriarvamused sellest, et ühe asutuse sees ei vaadata ega hinnata tulemuslikkust riigis tervikuna, vaid asutused mõtlevad rohkem sellele, kuidas saavutada enda organisatsioonis eesmärkide täitmine. Eriarvamused tekivad ka personali liikumise tõttu. Kui üks jurist näiteks lahkub, kelle arvates teatud andmevahetus teatud eesmärgil oli lubatav varasemalt, siis järgmine jurist ei pruugi enam nii arvata. Nii autori kui ka intervjueeritavate arvates võiks andmevahetust parandada ühtse vastutaja olemasolu (kood 8), kes otsustaks, kuidas, millal ja milliste andmete vahetamine on lubatud. Praegune ühtse vastutaja puudumine raskendab andmete kättesaadavust, kuna asutustel ei ole kindlat teadmist kõikidel juhtudel, kas andmeid võib vahetada ja pigem keeldutakse andmete edastamisest teisele asutusele, kuna kardetakse võimalikke sanktsioone ja andmekaitsenõuete rikkumist. Ühtse vastutaja olemasolu tagaks autori arvates muuhulgas teadmise, kust mingeid andmeid oleks võimalik saada.

Teatud asutuste vahelisi häid ja tihedaid kokkupuutepunkte nii inimeste vahel kui ka protsesside toimimisel (kood 10) tõid välja mitmed intervjueeritavad asutustevahelise koostöö tugevusena andmete ja info vahetamisel. Kuid autori arvates võib see omakorda tekitada probleemi, kuna ei soovita kaasata teisi asutusi peale nende, kellega juba on olemas toimivad kontaktid ja koostöö on lahendatud sujuvalt varasema suhtluse pinnalt. Autori hinnangul tuleneb sellest üleüldine asutuste vahelise koostöö vähesus (kood 9), kuna püütakse ise hakkama saada otsekontaktidega mõne üksiku protsessi toimima saamiseks. Asutused võiksid jagada üksteisega kogemusi ja lahendusi tsentraalselt toimima panna, tekitades seeläbi suuremat lisandväärtust ja mõju.

Praegust koostööd andmete vahetamisel kirjeldab muuhulgas üleüldise automaatsuse ja süsteemsuse puudumine (kood 7), kuna asutustel on erinev IT võimekus (kood 11) ja kõik ei ole võimelised automatiseeritult edastama masintöödeldavaid andmeid. Seetõttu on väiksemad avaliku sektori asutused ebavõrdsel positsioonil suuremate asutustega, kuna andmete jagamisel ei pruugi nad olla valmis võtma vastu X-tee kaudu andmeid ega edastama andmeid tänapäeva uudsemaid lahendusi kasutades. Andmevahetusel tekivad mõnikord vead (kood 12), kas inimliku eksimuse, liigse kiirustamise või mõne süsteemi

vea tõttu, mida mainisid EAS-i, KIK-i kui ka MTA esindajad. Alapeatükis 1.1. leiti, et organisatsiooni tehnoloogia piiride laienemisel on raskem tagada andmekaitsenõuete täitmist ehk väiksem IT võimekus annab teisalt eelise andmekaitsenõuete järgimisel, kuna andmekaitse vastutusala on lihtsam määratleda (käesolev töö, lk 9). Esindajad leidsid, et mõnikord saadakse teatud andmeid liiga hilja ehk selleks hetkeks, kui asutus saab andmed, on need juba liiga vanad. Näiteks vahel tuleb teisele asutusele saata meeldetuletus e-kirjaga selle kohta, et nad lubasid andmeid saata, teatud andmed laekuvad kvartaalselt, kuid kvartaalsete andmete puhul võib andmevajadus andmete saamise hetkeks olla kadunud.

Kontrollpäringute vähene rakendamine on autori arvates samuti andmevahetuse probleem (kood 14), mida samas juurutavad edukalt näiteks MTA ja Sotsiaalkindlustusamet. Kontrollpäringud tähendavad seda, et kui üks kord on mingid andmed asutusele antud, siis teatud hetkel või enne andmete kustutamist kontrollitakse, kas antud andmed klapivad teise asutuse andmetega, kellel on vajalik kontrollida nende andmete õigsust ja veenduda ega andmed ei ole vahepeal muutunud. Näiteks on vajalikud MTA tulu- ja sotsiaalmaksu deklaratsioonil kajastuvad andmed Sotsiaalkindlustusametile, kes peab neid andmeid hoidma, kuni isik läheb pensionile, aga kahe asutuse andmete säilitamise põhimõtted ei ühildu. MTA andmebaasides kustuvad andmed varem, kuid Sotsiaalkindlustusametil on vajalik veenduda, kas nad on saanud korrektsed maksuandmed selleks, et isiku pensioniea saabudes veenduda isiku varasemate maksuandmete õigsuses. Seetõttu on kaks asutust lahendanud omavahelised andmevahetuse vajadused konkreetse protsessiga, mis tagab et enne andmete kustutamist jõuaks vajalik info Sotsiaalkindlustusametisse. Kuna andmed on pidevas muutumises ja maksumaksjate kokkupuude erinevate asutustega toimub erineval ajal, arvab autor, et asutustele on vajalik tagada keskne lahendus kõige ajakohasematele andmetele tuginemiseks.

Teiseks kategooriaks oli **andmekaitsega seotud probleemid**. Autor uuris intervjueeritavatelt, milliseid ohte nähakse andmekaitsenõuete täitmisel, kui füüsiliste ja juriidiliste isikute andmeid võimaldataks asutuste vahel piiramatult vahetada, kuid andmed peaksid olema vajalikud tööülesannete täitmiseks. Peamise ohuna nähti inimest, kelle kaudu võivad andmed lekkida (kood 6), kuna võrk, kust andmeid vaadatakse ei ole piisavalt turvatud. Inimese all mõeldi nii klienti, kes enda andmeid vaatab kui ka töötajat, kes näiteks töötab kodukontoris, kus interneti ühendus ei pruugi olla nii turvaline kui töökohal. Kuna GDPR-is ei ole samuti kirjeldatud minimaalseid turvanõudeid WIFI ühendusele ja eravõrgu

kaudu kaugjuurdepääsule, siis autori arvates tuleks organisatsiooni siseselt määratleda interneti ühenduse ja kaugjuurdepääsu turvalisuse tagamise nõuded, mis peaks olema riigiasutustel ühetaoline (käesolev töö, lk 10). Ohuna nähti ka töötajat, kes vaatab andmeid kogemata või uudishimust (kood 5) ning asutuste erinevat võimekust andmekaitse ja IT tingimusi tagada (kood 4, käesolev töö, lk 10). Töötukassa esindaja sõnul nähtub nende statistikast, et kõige suuremad rikkumised on tööülesanneteta isikuandmete vaatamine (Koplimaa, 2021).

Autori arvates ei ole asutuste jaoks andmekaitse ohuks klient, kes andmeid vaatab, kuna võrgu turvalisuse tagamine, kust klient andmeid vaatab, on tema enda vastutus ja piisava turvalisuse tagamine peaks olema tema huvi, sest need on temaga seotud andmed. Inimese andmeid võib käsitleda kui tema vara, sarnaselt autole või sülearvutile, mille kaotsi mineku või hävimise kahju korvamiseks sõlmib inimene kindlustusleppe ning teeb kõik endast oleneva, et oma vara hoida. Nii peaks iga inimene suhtuma ka enda andmetesse ja tegema kõik, et andmed ei lekiks tahtmatult tema kaudu.

Klaos (2021) sõnul tuleks andmekaitseekspertidel luua ühtne teadmine, mis on aktsepteeritav ja mis mitte, kuna lähenemised andmekaitsele on spetsialistidel väga erinevad (kood 2). Tegelikkuses ühildub see probleem eriarvamuste probleemiga, mida autor käsitles esimeses kategoorias, mille tõttu asutused pigem keelduvad andmevahetusest, sest nad kardavad võimalikke negatiivseid tagajärgi. Kuna andmekaitse reeglid on ranged ja nende rikkumise puhul kohaldatakse suuri trahve (kood 1). Sama probleemi tõid välja muuhulgas Dakić ja Ribarić (2020, pp. 190–195) , kes leidsid, et GDPR-is ei ole määratud standardseid nõuded andmekaitsespetsialistidele (käesolev töö, lk 10). Autori arvates on väga oluline, et rakendatakse ühtset lähenemist ja seatakse standardsed nõuded andmekaitse spetsialistidele, mille läbi tekiks selgus andmekaitse valdkonnas ja paraneks andmevahetus. Kuigi andmekaitsenõuded on ranged, ei peaks avaliku sektori asutused piirama selles kartuses andmete kasutamist või jagamist asutuste vahel. Riigis kogutakse andmeid reguleeritult, mistõttu risk andmete väärkasutamiseks on oluliselt madalam kui erasektoris.

Kuigi andmekaitse ohtudena nähakse teiste asutuste vähest võimekust andmekaitsetingimusi täita ja IT-turvalisust tagada, siis asutused ise hindavad oma andmekaitsetingimuste täitmise tagamise võimekust heaks ja arvavad, et nad suudaksid tagada piisavad andmekaitsetingimused selliseks laiendatud andmevahetuseks. Ükski

intervjueeritavatest ei arvanud, et nende asutus ei ole võimeline tagama piisavaid andmekaitsetingimusi. Eelmises alapeatükis tõi töö autor välja Hirsijärvi, *et al.* (2007) kirjeldatud ühe intervjuu ohuna kalduvuse anda sotsiaalselt soovitatavaid vastuseid (käesolev töö, lk 24). Kuigi viidatust lähtudes ei pruugi ekspertide hinnangud olla kindlust andvad väited intervjueeritavate asutuste andmekaitsetingimuste täitmise võimekuse kohta, usub autor, et asutustel on siiski võimekus täita andmekaitsetingimusi, kuna kõikidel asutustel on teenistuses andmekaitsespetsialistid ning rakendatakse infoturbe- ja järelevalvemeetmeid andmekaitsenõuete täitmise osas.

Autor uuris ekspertidelt, milliseid tugevusi nähakse süsteemis, mis kujutab endast andmete kättesaadavust ja andmete jagamist, sest tegeliku olukorra hindamisel andmete vahetamisel ei annaks vaid probleemide otsimine tõepärast vaadet süsteemi hetkeseisust. Eksperdid leidsid, et andmete jagamisel ei ole seadusandluses puuduseid ning teatud asutuste vahel on väga hea koostöö. Samuti mainiti andmebaaside ning vanade lahenduste hästi toimimist. Näiteks teatud teenuseid on võimalik juba praegu automaatselt pakkuda (käesolev töö, lk 20). Sotsiaalkindlustusameti esindaja tõi automaatsete lahenduste osas perehüvitiste näite: „*Perehüvitise puhul, isik ise ei pea taotlust esitama. Kui laps ära sünnib, siis Sotsiaalkindlustusamet saadab isikule pakkumise, sest meil on teada, et laps on sündinud. Meil on olemas see info, mis palka on vanemad saanud…Me saame selle kõik kokku siduda ja inimestele saata.“* (Kümnik, 2021).

Alapeatükis 1.2. kirjeldati uuringu tulemusi, kus leiti et proaktiivsed teenused aitavad tagada õigust võrdsele kohtlemisele, mida ilmestab ka Sotsiaalkindlustusameti näide (käesolev töö, lk 21). Samuti hinnati plussina hetke koostöös X-tee olemasolu ja mugavust ning asutuste ekspertlust ja tugevat andmekaitset. Autori hinnangul hetke koostööd ilmestavate tugevuste pinnalt tuleks praegust süsteemi edasi arendada, kuna asutustel on tegelikkuses võimalused lahendusteks olemas, kuid neid ei julgeta kasutada täies mahus, sest kardetakse asutustevaheliste piiride kadumist keskse andmevahetuse suurenemisel ja maksumaksja ühtse riskiprofiili loomisel (kood 3).

Lisaks võib keskse süsteemi loomine riivata ekspertide hinnangul liigselt maksumaksjate õigusi, kui asutustel on olemas maksumaksjast info, mida ta on andnud teisel eesmärgil teisele asutusele (kood 7). Autori hinnangul vajab see seisukoht põhjalikumat õiguslikku analüüsi, mis on samuti nõutav GDPR artikli 39 lg 2 p a järgi, kui füüsiliste isikute andmetest tehakse ulatuslikku ja süstemaatilist hindamist, mis põhineb profiilianalüüsil ja

mille põhjal tehakse otsuseid, mis mõjutavad oluliselt füüsilist isikut (käesolev töö, lk 18). Lähtudes üldisest mõistlikkusest ei ole autor ekspertide väitega nõus, sest asutused juhinduvad oma töös seadustest ning riik peaks olema ühtne, mille tõttu ei peaks riigil olema nii-öelda riigi ees saladusi, kui need on vajalikud tööülesannete täitmiseks ja aitavad suurendada riigi tõhusust ning vähendada kulusid. Tulemuseks on rahulolevamad inimesed ja efektiivne ning läbipaistev avalik sektor. Läbipaistvuse olulisust rõhutas ka Sudžuka (2020, p.2) käesoleva töö lk-l 20. Andmekaitsealase mõjuanalüüsi tegemine ja sealhulgas analüüsi avaldamine, mis ei ole nõutav, kuid annaks maksumaksjatele kindlama teadmise nende andmete kasutamisest, on autori arvates heaks võimaluseks andmekaitsetingimuste tagamises veenduda (käesolev töö, lk 19). Mitmete esindajate sõnul mõned maksumaksjad soovivadki teadlikult esitada erinevaid andmeid asutustele.

„*Inimesed tahavad oma privaatmulli säilimist, sest sa kunagi ei tea, kuna riigi võim pöördub näiteks ja siis kasutatakse neid andmeid sinu vastu kurjasti ära. See tähendab, et usaldus andmestike osas peab olema tagatud selliselt, et inimesel on võimalik teatud hetkel oma konto tühjendada. Ma ei taha, et riik mu andmetele juurde pääseks ja ma saan sellest täiest aru.“* (Undrus, 2021).

Ekspertide arvates võib andmevahetuse suurendamine ja maksumaksjate keskne profileerimine suurendada bürokraatiat ning seeläbi suurendada asutuste töömahtu, sest maksumaksja profiilis võivad sisalduda andmed, mida ei oska teised asutused põhjendada. Loomaks arusaama, miks isik ei kvalifitseerunud näiteks toetuse saajaks, võib maksumaksja pendeldada erinevate asutuste vahel. Autori hinnangul on vajalik jagada omavahel kompetentse, sest maksukompetents on MTA-l, kes oskab määrata maksuriske ja nõustada asutusi, kuidas nemad saavad kaasa aidata maksukuulekusele ja ennetada pettusi. Samaväärset kompetentsi ei ole teisel asutusel. Kui asutused kasutaksid teiste asutuste loodavat lisandväärtust, mis tuleneb nende teenistujate teadmistest ja oskustest, aitaks see oluliselt säästa riigi kuludelt, efektiivistada protsesse ja prognoosida tuleviku meetmeid erinevate teenuste pakkumisel ning toetuste määramisel. Autori hinnangul asutused peaksid jagama oma teadmisi arusaadavas keeles ning korraldama enne uue süsteemi kasutusele võttu koolitusi, kus selgitatakse, kuidas tekib ühes asutuses profiil maksumaksjast, et maksumaksjad ei peaks alati pöörduma erinevate asutuste poole leidmaks selgitusi.

Alapeatükis 1.2. kirjeldati 2003. aastal sõnastatud andmekogude uute normide põhipostulaate, mille kohaselt andmed kuuluvad riigile tervikuna ja info peaks olema kättesaadav, kas ühest kohast või andmete ristkasutuses olevast süsteemist (käesolev töö, lk 20). Kui analüüsida ekspertide arvamust andmete kättesaadavuse ja andmevajaduse osas, siis töö autori arvates on 2003.a sõnastatud andmekogude normid 18 aastat hiljem osaliselt unustatud, kuna asutustel ei ole täna kogu info üheselt kättesaadav, isegi kui seadus seda võimaldab, kas siis põhjendamise oskamatuse, tehnilise võimekuse puudumise tõttu või teadmatusest, et selliseid andmeid on võimalik saada. Tehnilise võimekuse puudumist võib autori arvates põhjendada sellega, et mida kiiremini toimub areng, seda suurema tõenäosusega ei pruugi kõik arenguga kaasa jõuda, mille tõttu ka andmevahetus ei ole täna ühtlasel tasemel.

Vastates lühidalt uurimisküsimusele: „Millised probleemid on maksumaksjate kesksel profileerimisel?“ saab kokkuvõtvalt väita, et kõikidel asutustel on olemas juurdepääsud maksumaksjatega seotud andmetele, kuid erinevas ulatuses ja esineb mitmeid puuduseid, mida asutused sooviksid oma töö tõhustamiseks kõrvaldada ning andmevajadusi, mida peetakse oluliseks lahendada. Enim soovitakse saada isikute kohta toetuste ja pettustega seotud infot, mille põhjal tõhustada järelevalve protsesse ja tagada õigemad otsused eelarvete jaotamisel. Peamine probleem on asutuste hinnangul seadustes toodud andmekaitse alased piirangud, mida töö autor samuti käsitles varasemates peatükkides, kuid jõudis järeldusele, et seadusandluse juures asutuste vahelise andmevahetuse osas ei ole liigseid piiranguid. Vaja on põhjendada piisavalt andmete saamise huvi, andmete jagamise eesmärki ja tõsta esile kasu riigile tervikuna. Suurima andmekaitsealase ohuna nähti inimest, kelle kaudu võivad andmed lekkida, kuid samasugune oht on ka praeguses süsteemis ja autori arvates maksumaksjate keskne profileerimine ei suurendaks tõenäosust andmete lubamatuks töötlemiseks.

Autori arvates on suurim probleem maksumaksjate kesksel profileerimisel asutuste erinev IT võimekus, mille tõttu ei ole hetkel võimalik kõigil asutustel ühetaoliselt andmeid jagada ja vastu võtta. Autori hinnangul tuleks alustada maksumaksjate keskset profileerimist asutuste IT võimekuse ühtlustamisest, mis eeldaks ühise IT toe loomist.

2.3. Andmevahetuse suurendamise võimalused ja tagajärjed

Alapeatükis analüüsitakse, milliseid positiivseid ja negatiivseid tagajärgi võiks kaasa tuua asutustevaheline andmevahetuse suurendamine ja milliseid võimalusi näevad andmevahetuse parendamiseks eksperdid ise ning milline on avalik huvi asutuste esindajate jaoks andmevahetuse suurendamisel.

Kolmandaks kategooriaks oli intervjuude analüüsimisel **avalik huvi andmevahetuse suurendamisel**. Autor palus ekspertidel avaldada oma arvamust selle kohta, miks andmevahetuse suurendamine asutuste vahel peaks olema avalikes huvides ja tuua võimalikke positiivseid ning negatiivseid tagajärgi andmevahetuse suurendamisel. Eelnevates peatükkides analüüsiti, et avaliku huvi lahti seletamine on keerukas ja pigem subjektiivne (käesolev töö, lk 16-22). Seega jätab töö autor iga lugeja enda otsustada, kas ekspertide arvamused andmevahetuse suurendamise vajalikkuse kohta on avalikes huvides. Eksperdid tõid avaliku huvi objektiks olevate teemadena, mis andmevahetuse suurendamisel paraneks:

1) ressursside targem kasutamine (kood 1);
2) jõudmine abivajajateni (kood 2);
3) riigi maine suurendamine (kood 3);
4) riigiabi suuruse teadmine (kood 4);
5) head ja mugavad teenused (kood 5);
6) paremad prognoosimis ja otsustusvõimalused erinevates valdkondades (kood 6);
7) läbipaistvuse tagamine (kood 8);
8) võrdsetel alustel toetuste maksmine (kood 10).

Kõike eelmainitut saaks teha paremini, kui riigiasutustel oleksid ajakohased ja õiged andmed (kood 7), mis on autori arvates kogu andmevahetuse olulisim alus ja avaliku huvi objektiks olev teema. Kui asutustel ei ole ajakohaseid ja õigeid andmeid, siis ei ole võimalik autori hinnangul midagi parendada. Andmevahetuse suurendamisel oleks asutustel suurem kindlus selles, et neil on kõige täpsem informatsioon maksumaksja kohta.

Autor uuris ekspertidelt COVID-19 kriisi mõjutusi, kuna vajadus protsesse muuta tuleb esile enim kriisiolukordades, kui probleem on juba tekkinud ja vajadus selle lahendamiseks kriitiline (kood 11). Kriisiolukorras seadustati kiirelt uued võimalused andmete

vahetamiseks, mille tulemusel said asutused jagada toetuseid reaalselt abi vajavatele taotlejatele kiiremini ja vajalikule andmestikule tuginedes, vältides skeemitajatele väljamaksete tegemist. COVID-19 kriisi mõjul toimunud muudatused siseriiklikus regulatsioonis ilmestavad autori arvates suurepäraselt andmevahetuse parendamise vajadust riigis pikas perspektiivis ja seda, et tegelikult ei ole seadusandluse juures piiranguid asutustel omavahel andmeid jagada, kui see on vajalik ja eesmärgipärane ning samuti ei sea andmekaitsenõuded piiranguid selliseks andmevahetuseks, kui täita kõiki andmekaitsetingimusi.

Kui võrrelda COVID-19 tingitud eriolukorra perioodi andmevajadust asutustevahelise koostöö ja põhiprotsesside muudatuste osas, siis mingeid mõjutusi oli igas asutuses. Asutustevaheline koostöö suurenes asutustel, kellel oli vaja koostööd teha toetuste väljamaksmisel, vaktsineerimisega ja haigestumisega seotud info jagamisel. Töökorralduslikud muutused toimusid kõikides asutustes, tekkis kõrgem vajadus digitaliseeritud protsesside järele, kuna kliente ei olnud võimalik enam samaväärselt koha peal vastu võtta ning tööd tehti peamiselt kodukontorist. Kiirelt ülesehitatud andmevahetusele suunatud koostöö MKS §168[15] alusel toetusmeetmeid rakendanud asutuste ja MTA vahel võimaldas selliseid skeeme kiirelt tuvastada, kus püüti alusetult toetust välja petta ja seeläbi soovimatuid väljamakseid vältida. Meyer (2020) hinnangul avalikes huvides on võimalik leevendada kriisi ajal andmete töötlemise piiranguid, tänu millele sai ka MKS-i täiendada kriisimeetmete kiireks rakendamiseks (käesolev töö, lk 16).

Kõige suurem teadmine kriisiperioodil saadi selles, et teatud protsesse on võimalik palju kiiremini teha, kui tavaolukorras. Kui tavaliselt võtavad arendused aega osade ekspertide sõnul 1,5-2 aastat, mõnede arvates isegi 2-3 aastat, siis COVID-19 perioodil suudeti tänu andmete olemasolule kuu ajaga ja isegi päevadega välja töötada toetusmeetmed, täiendada seaduseid ja luua uusi lahendusi. Kriisi välisel ajal pidid asutused ootama teatud juhtudel mitu aastat, et andmetele juurepääse saada, milleks võis olla juba huvi ja vajadus kadunud (käesolev töö, lk 17).

Neljandaks kategooriaks **oli riigiasutuste andmevahetuse vajadused**, mis on suuresti seotud avaliku huviga, kuid ilmestab ka üldist riigiasutuste vajadust andmevahetust suurendada. Kuna eksperdid ei toonud antud intervjuudes konkreetseid vastuseid avaliku huvi näidete ja riigivajaduste osas andmevahetuse suurendamisel ning rääkisid teemadest segamini, ei käsitle autor neid teemasid eraldi. Eeltoodu tõestab töö teoorias toodud Carter

& Bouris (2006, p.5) väidet avaliku huvi keerukuse ja subjektiivsuse kohta. Enim toodi avaliku huvi ja riigiasutuste andmevahetuse vajaduste näitena skeemide vältimise võimalust tänu suuremale andmete töötlemisele (kood 2), millest tulenevalt oleks võimalik tuvastada ebakõlad andmetes juba eelmenetluses ja seeläbi vältida põhjendamatuid otsuseid ja jõuda rohkemate abivajajateni ning maksta toetuseid võrdsematel alustel Seetõttu just riskiinfo jagamine peaks olema avalikes huvides.

„*See on kindlasti avalikes huvides, sest kui asutused saavad andmeid vahetada mõlemas suunas, siis on võimalik luua riigi vaatest ühtne profiil, mis võtaks arvesse kõikide asutuste sisendit (riski)profiili loomisel. Näiteks COVID-19 toetusmeetmete raames Töötukassaga infovahetusel jõudsime tõdemuseni, et ilma andmete vahetamiseta oleks toetusi makstud isikutele, kes MTA vaatest on kõrge riskiga, kui Töötukassal poleks olnud neid andmeid kuskilt võtta kontrollimaks toetuse taotlejate poolt taotluses esitatut.“* (Vahemäe, 2021).

Andmevahetuse suurendamise tulemusena oleks võimalik kiireid lahendusi kasutades määrata maksumaksjale parim teeninduskanal lähtudes just tema vajadustest (kood 7, kood 8), tõhustada tööprotsesse (kood 3), ühtlustada kvaliteeti (kood 6), tagada parem järelevalve (kood 1) ning kasutada avaliku sektori ressursse targalt (kood 9, käesolev töö, lk 20-21). Eelnimetatud punktidest sõltub ka riigi maine tervikuna, mis on oluline nii Eestis elavatele inimestele ja ettevõtetele. Kui maksumaksjal on vaja asjaajamiseks kulutada arvestatav hulk aega, tuua tõendeid ja pidevalt suhelda riigiga, siis võidakse kaotada huvi tegeleda ettevõtlusega Eestis.

„*Ma arvan, et riik võiks olla ühtne, nii-öelda riik kui organisatsioon ja kui taotleja suhtleb, siis ta ei pea ühte ja sama infot andma mitmesse kohta ja ei tohi ka eeldada, et kui ta seda infot annab, siis see kuhugi edasi ei liigu riigi organisatsiooni sees.“* (Klaos, 2021).

Haigekassa juhatuse liige tõi näite vaktsineerimise protsessist, kus oli väga oluline näidata avalikkusele töödeldud aruandeid, kui palju on vaktsineerituid ja millistel ametipostidel, kuid neil ei olnud selleks vajalikke töötajate registri andmeid, kus oleks saanud välja selekteerida erinevate ametite esindajad. Üha suurema vaktsineerimisvõimekuse tõttu ilmselt mingi hetk see vajadus kaob, kuid teatud situatsioonides peaks olema edaspidi võimalik riigiasutustel kokkuleppeid sõlmida selliste andmete jagamisel, et olla riigina läbipaistev. (Banhard, 2021)

Eksperdid olid bürokraatia suurenemise või vähenemise suhtes vastakatel seisukohtadel (kood 10). Kuid töö autor nõustub pigem nende ekspertidega, kes leidsid, et riigiasutuste andmevahetuse suurendamine ja maksumaksjate keskse profiili loomine vähendaks bürokraatiat, kui andmevahetuse suurendamist alustada koordineeritult ja põhjalikku eeltööd tehes, et vältida võimalikke probleeme. Maksumaksjate keskne profileerimine vähendaks bürokraatiat, kuna asutused saaksid ajakohasemate ja õigete andmete abil tegeleda probleemidega enne nende tekkimist, mille tulemusel väheneks nii riigi kui maksumaksja tõendamiskoormus.

Vastates uurimisküsimusele: „Miks on vajalik riigiasutuste andmevahetuse suurendamine ja praeguste andmekaitse tõkete leevendamine?“, võib öelda, et andmevahetuse suurendamine on vajalik eelkõige maksumaksjate heaolu tõstmiseks paremate ja mugavamate avalike teenuste läbi, mida toetab andmevahetuse suurendamine. Samuti on andmevahetuse suurendamine ja maksumaksjate keskse profiili loomine oluline riigi eelarve tõhusamal majandamisel, mille tulemusel oleks autori hinnangul võimalik pikaajaliselt säästa erinevatelt administratiivsetelt kuludelt ja suunata riigi raha rohkemate toetuse vajajateni. Autori arvates tuleks asjakohaste seaduste sõnastusi täpsustada võimaldamaks keskse profiili kasutuselevõttu asutuste otsustusprotsessides, kuid sellise regulatsiooni puudumine ei ole oluliseks takistuseks andmevahetuse suurendamiseks asutuste vahel nende andmete osas, mis on asutuste ülesannete täitmisel vajalikud ja põhjendatud. COVID-19 viiruse levikuga seotud kriisiolukord tõhustas oluliselt asutuste protsesse ja suurendas asutustevahelist koostööd andmevahetuses. Autor usub, et asutused said sellest positiivse lükke omavahelise koostöö ja andmehalduse paremaks muutmiseks ka pikas perspektiivis.

Viimaseks kategooriaks oli **riigiasutuste suurema andmevahetuse ja ühtse riskiprofiili loomise võimalused**. Esiteks tuleks andmevahetuse suurendamisel veenduda andmekaitsetingimuste tagamises (kood 4), milleks tõid eksperdid mitmeid erinevaid lahendusi:

1) kasutusõiguste selgelt määratlemine,
2) andmete edastamine krüpteeritult,
3) kliendi nõusoleku küsimine,
4) põhjendamine, miks andmeid vaadatakse,
5) vajadusel andmete kustutamise võimaluse tagamine,

6) nõuete täitmise kontrollimine,
7) teavitustöö ja koolitamine.

Andmekaitsetingimuste tagamist, mis toodi lahendustena ka ekspertide poolt, kirjeldas autor töö eelnevates peatükkides (käesolev töö, lk 10–12 ja 19). Andmevahetuse suurendamise võimalustena toodi välja ka seadusandluse muutmine (kood 3), mis võimaldaks lihtsamini andmeid vahetada riigiasutuste vahel. Andmevahetuse suurendamise eeldusteks on ühes standardis või keeles suhtlemine andmete vahetamisel, andmevahetuse piiri määratlemine, mis ulatuses andmeid vahetada, Andmekaitse Inspektsiooni kaasamine lahenduste loomisesse, rahalise ja tööjõuressursi olemasolu (kood 10), asutusesiseste regulatsioonide muutmine või loomine (kood 8) ja ühe vedaja või vastutaja olemasolu maksumaksjate keskse profileerimise projektis, kes suudaks asutusi kokku tuua ja näidata, et suurem andmevahetus ja ühtse riskiprofiili loomine on võimalik.

„Maandamiseks ongi mõeldud, et asutus ise, kes käib küsimas neid andmeid on ise oma struktuuris paika pannud infoturbenõuded, kellel on õigus küsima tulla ja et neid andmeid kasutatakse puhtalt tööülesannete täitmiseks.“ (Kivistik, 2021).

Ekspertide hinnangul on maksumaksjate kesksel profileerimisel oluline riskide vaate kuvamine (kood 15) ning toetuse saamine võiks olla seotud maksukuulekusega (kood 12). Laiemalt nähakse riigi poolse profiili loomist maksumaksjast ehk kõikide riigiasutuste keskse riskiprofiili loomist, mis peaks olema jaotatud osadeks (kood 14) ja on võimalik eraldada vastavalt asutuste vajadustele. Kuid nii ekspertide ja autorite arvates võib selline profiil minna liialt keeruliseks.

Tehniliselt, kuidas suuremat andmevahetust korraldada usuvad eksperdid X-tee toimimisse (kood 5, käesolev töö, lk 20), kuid võimalusena nähakse ka keskset andmebaasi (kood 6, käesolev töö, lk 11, 12, 18), mille positiivsete argumentidena tuuakse üldiselt head ligipääsu ka väiksema IT võimekusega asutuse jaoks. X-tee suhtluskanali kaudu ei ole võimalik kohe edastada *Exceli* formaadis infot, kuid seda infot saaks sellises formaadis andmebaasi näiteks kord päevas üles laadida. Negatiivne külg oleks kesksel andmebaasil haldamise küsimus, võimalik teiste andmebaaside duubeldamine ja andmekaitsetingimuste keerulisem tagamine. Andmevahetuse võimalusena leiti variandina ka aruandlusmudelite kasutusele võttu läbi *Microsoft SharePoint* tarkvara (kood 9). Kuna X-tee loodi selleks, et avalik sektor saaks kasutada innovatiivseid lahendusi tänu avaliku halduse piires lõimitud

infosüsteemile ja X-tee lahendus on täna üldiselt hästi toimiv, siis autori arvates oleks ekspertide pakutud variantidest X-tee parim ja innovaatilisem lahendus andmevahetuse suurendamiseks.

Lisaks eespool toodule nähakse võimalusena riigiasutuste andmevahetust suurendada MTA maksukäitumiste hinnangute teenuse (edaspidi hinnangud) kaudu (kood 7), mis on MTA poolt väljatöötatud uus e-teenus ettevõtetele ja põhineb ettevõtete esitatud andmete analüüsil. Selle teenuse kaudu saavad ettevõtted oma maksukäitumises oluliste andmete kohta regulaarselt ajakohast tagasisidet. (Maksu- ja Tolliamet, 2021) MTA hinnangud oleks autori arvates alternatiiv ühisele riskiprofiilile, andmete kuva on ühe vastutaja käes (antud juhul MTA) ja see lahendus ei suurendaks autori arvates bürokraatiat, vaid pigem läbipaistvust, sest maksuandmed on mõtestatud ja teenuse kasutajale hõlpsalt loetavad. Hinnangute teenuse kuva saaks tehniliselt jagada teistele asutustele ja sarnaseid kuvasid saaks luua ka teiste asutuste riske kaasates. Hinnangut peavad eksperdid parema otsustamise indikaatoriks kui pelgalt maksuvõla olemasolu fakti, mida nad on senini kasutanud toetuste määramisel (kood 12).

„Kui ma sihitult mõtlen, siis maksumaksjate keskne profileerimine peaks toimuma MTA-s, kellel on maksude maksmise vaatest koondhinnang ettevõtja või eraisiku kohta olemas ja kes ütleb, mis on selle maksumaksja maksualane taust ja käitumine. Ühtlasi mitte me ise ainult ei omaks seda profiili tulevikus, vaid meil oleks ka õigus andmeid edastada ja teistel asutustel on huvi seda profiili ka oma andmetes ära kasutada.“ (Veiksaar, 2021).

Vastates uurimisküsimusele: „Kuidas oleks võimalik suurem andmevahetus riigiasutuse vahel ning ühtne riskiprofiili loomine?“, leiab autor, et andmevahetuse suurendamise ja ühtse riskiprofiili loomisel tuleb esmalt välja selgitada andmevajadused ehk milliseid andmeid on mingil asutusel vaja ja seejärel tuvastada kõige sobivamad kanalid nende andmete saamiseks ning veenduda andmekaitsetingimuste tagamises kõikides asutustes viies läbi andmekaitsealane mõjuhinnang ning seeläbi põhjaliku eeltöö tulemusel alustada andmevahetuse suurendamist arendades X-tee juurdepääse andmetele. Samuti tuleks andmekaitse spetsialistidele luua ühine teadmine, milline andmete töötlus on riigiasutustes lubatud. Selleks, et võtta kasutusele ühtne riskiprofiil leiab autor, et parim lahendus on hetkel MTA maksukäitumiste hinnangute teenus, mida soovisid ka eksperdid oma töös kasutada ning leidsid, et toetuste saamine peaks olema seotud maksukuulekusega. Kui MTA suudab teha piisavat koolitustööd asutustele, kes MTA profiili oma töös kasutusele

võtavad ning nende profiil parandab teiste asutuste tööprotsesse ilma, et asutuste töökoormus oluliselt suureneks. Autori arvates sarnaselt maksuandmetele, võiks kaasata järgmise etapina hinnangutesse ka teiste asutuste olulist infot, näiteks toetuste kohta. Selliselt jääksid asutused enda kogutud andmete andmekogude omanikeks, aga andmevahetuse tulemusena saaks luua keskse riskiprofiili kuva, mis tagab ühetaolise vaate maksumaksjale, mida iga asutus saab oma töös rakendada.

Kokkuvõtvalt on palju erinevaid situatsioone, mille lahendamiseks on vajalik suurem andmevahetus ja koostöö asutuste vahel, autori arvates mõnel juhul lausa hädavajalik. Autor järeldab töös analüüsitu põhjal, et andmevahetuse suurendamine asutuste vahel on vajalik ja võimalik. Järeldust ilmestab MKS § 168[15] loomine kriisiajal toetamaks laialdast andmevahetust eelarveliste otsuste langetamiseks. Eksperdid tõid andmevajaduse kõrval välja mitmeid andmekaitsealaseid ohtusid andmete jagamise suurendamisel, kuid samad ohud on autori arvates ka praeguses süsteemis olemas, seega ei suurendaks andmekaitse riski andmete jagamise suurendamine, kui asutused rakendavad kehtivaid andmekaitsenõudeid samaväärselt kõikide andmete töötlemisele. Ka intervjueeritavad tõid omapoolsed lahendused andmekaitse ohtude maandamiseks.

Kui avalik huvi on see, mille inimesed valiksid Lippmanni (1955, p.40) kirjeldatud viisil, siis autori hinnangul oleks andmevahetuse suurendamine ning riskiprofiilide jagamine asutuste vahel võimalik teostada ilma avalikku huvi piiramata, kuna autori arvates andmete vahetamisest saadav kasu on ühiskonnale tervikuna kasulikum kui üksikisikute tajutav võimalik põhiõiguste riive. Oluline on veelkord välja tuua ka Pennsylvania kohtulahend, mis leidis, et andmete kaitse ja avalik huvi saavad olla üksteist kahjustamata tasakaalus (käesolev töö, lk 16). Kuna avalik huvi on teada, kuidas andmeid riigis kasutatakse, on vajalik maksumaksjate kesksel profileerimisel andmekaitsealase mõjuhinnangu koostamine ning avaldamine ja teabe avalikustamine, millistel juhtudel isikute andmeid jagatakse teiste asutustega (käesolev töö lk 19).

KOKKUVÕTE

Lõputöö uurimisprobleemiks oli küsimus: „Kuidas saavutada mõistlik tasakaal andmekaitse normide ja avaliku huvi vahel isikuandmete töötlemisel?“ Lõputöö eesmärk oli välja selgitada maksumaksjate keskse profileerimise vajalikkus ning leida viisid maksumaksjate keskseks profileerimiseks andmekaitse norme ja avalikku huvi kahjustamata. Lõputöö eesmärgi saavutamiseks kasutati kvalitatiivset uurimismetoodikat.

Töö esimeses osas analüüsiti erialast teaduskirjandust leidmaks võimalikke andmekaitsealaseid probleeme maksumaksjate kesksel profileerimisel, avaliku huvi defineerimiseks ja toomaks erinevaid võimalusi ning näiteid kasutades ka COVID-19 perioodi mõjutusi andmevahetuse suurendamise vajalikkuse kohta. Lõputöö autor viis läbi ekspertintervjuud 13 esindajaga 8 erinevast riigiasutusest (vt tabel 1), mille tulemused ja järeldused toodi lõputöö teises osas. Intervjuude eesmärk oli leida praktilised probleemid maksumaksjate kesksel profileerimisel ja saada ekspertide kaudu teada maksumaksjate keskse profileerimise vajalikkus ja võimalused.

Esimeseks uurimisküsimuseks oli: „Millised probleemid on maksumaksjate kesksel profileerimisel?“ Sünteesides teooriat ja ekspertintervjuude tulemusi on maksumaksjate keskse profileerimise probleemideks seadusandluse piirangud ja andmekaitsealaste tingimuste rikkumise oht, kuid autori arvates on suurimaks probleemiks asutuste erinev IT võimekus, mille tõttu ei ole kõik asutused võimelised ühtlasel tasemel andmeid vahetama.

Teiseks uurimisküsimuseks oli: „Miks on vajalik riigiasutuste andmevahetuse suurendamine ja praeguste andmekaitse tõkete leevendamine?“. Autor sai ekspertide toodud vajadusi ja praeguse andmevahetuse puuduseid analüüsides teadmise, et maksumaksjate keskne profileerimine on vajalik selleks, et vältida pettuseid, jõuda abivajajateni pakkudes häid ja mugavaid teenuseid ja mis kõige olulisem, vähendada oluliselt ressursside raiskamist ehk riigi eelarvet tõhusamalt majandada.

Kolmandaks uurimisküsimuseks oli: "Kuidas oleks võimalik suurem andmevahetus riigiasutuse vahel ning ühtne riskiprofiili loomine?“. Eksperdid tõid andmevahetuse suurendamisel parima võimaliku lahendusena X-tee kaudu andmete vahetamist, mille tõttu ka autor jääb oma hinnangus X-tee juurde. Maksumaksjate keskset profileerimist on võimalik autori arvates teostada ilma andmekaitse norme kahjustamata ja avalikku huvi

piiramata, kui täiendatakse ja parandatakse seaduse sõnastusi ning viiakse läbi andmekaitsealane mõjuhinnang ning kaasatakse eksperdid, kellel on parimad teadmised oma asutuste tööst. Ühtse riskiprofiili loomise juures on oluline andmete eraldamise võimalus, kuna riskiprofiil võib minna liiga keeruliseks, kuid esialgu tuleks autori arvates luua võimalus asutustel näha juba MTA loodud riskiprofiili maksumaksjatest maksukäitumise hinnangute näol, kuhu tulevikus võiks asutuste kohanemisel ja IT võimekuse suurenemisel ühendada teiste asutuste riskiprofiilid, mis peaks olema võimalik üksteisest eraldada selleks, et iga asutus näeks seda andmete kogumit, mis tema töös vajalik on.

Töös leiti, et maksumaksjate keskne profileerimine on võimalik ilma andmekaitse norme kahjustamata ja avalikku huvi piiramata tulenevalt COVID-19 kriisimeetmete väljatöötamisel nähtunud praktikast, kuid autori arvates tuleks koostada täpse projekti kohta eelnevalt andmekaitsealane mõjuhinnang. Samuti leiti töö teooria osas, et avalik huvi ja andmete kaitse saavad olla tasakaalus üksteist kahjustamata. Seega hindab töö autor lõputöö eesmärgi täidetuks.

SUMMARY

The research problem for the thesis was the question: "How to achieve a reasonable balance between data protection standards and the public interest in the processing of personal data?". The aim of the thesis was to identify the need for central profiling of taxpayers and to find ways to centrally profile taxpayers without compromising data protection standards and the public interest. To achieve this objective, a qualitative research methodology was used.

In the first part of the thesis, the scientific literature was analyzed to identify potential data protection issues in the central profiling of taxpayers, to define the public interest and to provide different options and examples of the implications of the COVID-19 period for the need to increase data sharing. The author of the thesis conducted expert interviews with 13 representatives from 8 different public authorities (see Table 1), the results and the conclusions thereof were presented in the second part of the thesis. The aim of the interviews was to identify problems with central profiling of taxpayer and to learn from the experts about the necessity and possibilities of central profiling of taxpayers.

The first research question was: "What are the problems with central profiling of taxpayers?" Synthesizing the theory and the results of the expert interviews, the problems with central profiling of taxpayers are the legislative limitations and the risk of breach of the data protection conditions. But the author believes that the biggest problem is the different IT capabilities of the institutions, which means that not all of the public sector institutions are able to exchange data at a consistent level.

The second research question was: "Why there is a need to increase data sharing between public authorities and to alleviate current data protection barriers?". By analyzing the needs identified by the experts and the shortcomings of the current data exchange, the author came to the conclusion that a central profiling of taxpayers is necessary to prevent fraud better, proactively provide support to those in need by providing good and convenient public services and, most importantly, significantly reduce waste of administrative resources and manage the state budget more efficiently.

The third research question was: "How could greater data exchange between national authorities and the creation of a single risk profile be achieved?". The experts identified the

best possible solution for the increase of data exchange among public sector organizations being the exchange of data via X-Road, which is why the author stays to X-Road in her evaluation. In the opinion of the author, central profiling of taxpayers can be carried out without undermining data protection standards and the public interest by improving and amending the wording of the legislation, by carrying out a data protection impact assessment and by involving experts with the best knowledge of the work of their institutions. The possibility of separating data is an important element in the creation of a single risk profile, as the risk profile may become too complex, but initially, in the author's opinion, the possibility should be created for the authorities to see the risk profile already created by the MTA in the form of taxpayer behaviour assessments, into which, in the future, as the authorities adapt and the IT capacity increases, the risk profiles of other authorities could be merged. The risk profiles should be able to be separated from each other so that every organization could see only the data set, which is necessary to perform their work assignments.

It was found in the thesis that central profiling of taxpayers is possible without undermining data protection standards and without limiting the public interest, based on the practice seen in the development of the COVID-19 crisis measures, but the author considers that the exact project should be subject to a prior data protection impact assessment. The theory of the work also concluded that public interest and data protection can be balanced without undermining each other. Therefore, the author considers that the objective of the thesis has been met.

VIIDATUD ALLIKATE LOETELU

Avaliku teabe seadus[1] (2000) RT I, 15.03.2019, 11.

Bogdanov, D. & Siil, T., 2020. Infotehnoloogilised võimalused põhiõiguste kaitsel. *Juridica,* VI, lk 474–481.

Brough, A.R. & Martin, K.D., 2021. Consumer Privacy During (and After) the COVID-19 Pandemic. *Journal of Public Policy & Marketing*, 40(1), pp. 108–110.

Bryman, A., 2012. *Social Research Methods. 4th edition.* Oxford: Oxford University Press.

Bryson, J.M., Crosby, B.C, Bloomberg, L., 2014. Public Value Governance: Moving Beyond Traditional Public Administration and the New Public Management. *Public Administration Review,* 74(4), pp. 445–456.

Carter, M. & Bouris, A., 2006. *Freedom of Information: Balancing the Public Interest*. *2nd edition.* United Kingdom: The Constitution Unit.

Chavalit, V. & Hohler, L., 2020. Data Protection in a GDPR World. *Internal Auditor*, 77(3), pp. 35–38.

Dakić, V. & Ribarić, S., 2020. Judical and Technical Improvement of General Data Protection Regulation. *Annals of DAAAM & Proceedings*, 7(1), pp. 189–196.

Dobos, P. & Takács-György, K., 2019, Possible Smart City Solutions in the Fight against Black Economy. *Interdisciplinary Description of Complex Systems*, 17(3–A), pp. 468–475.

Dziuban, C., Moskal, P., Cavanagh, T. & Watts, A., 2012, Analytics that Inform the University: Using Data You Already Have. *Journal of Asynchronous Learning Networks*, 16(3), pp. 21–38.

Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus[1] (2018) RT I, 07.12.2018, 2.

Eesti Inimõiguste Keskus, 2019. *Inimõigused, infoühiskond ja Eesti: esialgne kaardistus.* [Võrgumaterjal] Leitav: https://humanrights.ee/materjalid/inimoigused-infouhiskond-ja-eesti-esialgne-kaardistus/ [Kasutatud 27.02.2021]

Eesti Maksumaksjate Liit, 2016. Kas maksusaladus on heades kätes? *MaksuMaksja,* I, lk 6–9.

Eesti Vabariigi põhiseadus (1992) RT I, 15.05.2015, 2.

Eesti Vabariigi Valitsus, 2021a. *Arenguvajadused*. [Võrgumaterjal] Leitav: https://valitsus.ee/strateegia-eesti-2035-arengukavad-ja-planeering/strateegia/arenguvajadused [Kasutatud 21.03.2021]

Eesti Vabariigi Valitsus, 2021b. *Riigivalitsemine.* [Võrgumaterjal] Leitav: https://valitsus.ee/strateegia-eesti-2035-arengukavad-ja-planeering/vajalikud-muutused/riigivalitsemine [Kasutatud 21.03.2021]

Euroopa Parlament ja Euroopa Nõukogu, 2016. *Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). Määrus. ELT, 27.04.2016, 2016/679.*

Euroopa Ühenduste Nõukogu, 1992. *Millega kehtestatakse ühenduse tolliseadustik*. *Määrus.* EÜT, 12.10.1992, 2913/92.

Gębczyńska, A. & Brajer-Marczak, R., 2020. Review of Selected Performance Measurement Models Used in Public Administration. *Administrative Sciences (2076-3387),* 10(4), pp.1–21.

Hirsjärvi, S., Remes, P., & Sajavaara, P., 2007. *Uuri ja kirjuta.* Tallinn: Medicina.

Isikuandmete kaitse seadus (2018) RT I, 04.01.2019, 11.

IT Governance Privacy Team, 2017. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide.* United Kingdom: IT Governance Ltd.

Karistusseadustik[1] (2001) RT I, 03.03.2021, 3.

Karu, K., 2021. Tehisintellekti keerukad küsimused. *Juridica,* I, lk 43–54.

Klingenberg, A.M., 2016. Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities. *International Review of Law, Computers & Technology,* 30(1/2), pp. 67–75.

Konks, M., 2014. *Kriminaalmenetluses kogutud isikuandmete kaitse avaliku sektori teabe taaskasutamisel. Magistritöö.* Tartu: Tartu Ülikool.

Konkurentsiseadus[1] (2001) RT I, 13.03.2019, 92.

Krediidiasutuste seadus[1] (1999) RT I, 21.11.2020, 9.

Kumm, M., 2020. Institutsionaliseerides sokraatilist vaidlustamist: ratsionaalne inimõiguste paradigma, legitiimne autoriteet ja põhiseaduslikkuse järelevalve eesmärk. *Juridica,* Riigiõiguse aastaraamat 2020, lk 100–117.

Laaring, M., 2019. Haldusjärelevalvest läbi riikliku järelevalve prisma. *Juridica*, IV, lk 252-263.

Laherand, M.-L., 2008. *Kvalitatiivne uurimisviis.* Tallinn: Sulesepp.

Lehis, L., 2015. *Maksumaksja. Kuku raadio saade 08.09.2015.* [Võrgumaterjal] Leitav: http://podcast.kuku.postimees.ee/saated/maksumaksja/page/8/ [Kasutatud 28.12.2020]

Lember, K., 2019. Tehisintellekti kasutamine haldusakti andmisel[*1]. *Juridica,* X, lk 749–760.

Lind, K., 2009. Maksusaladus kehtivas õiguses. *Juridica,* VII, lk 455–464.

Lippmann, W., 1955. *Essays in the Public Philosophy*. A *Mentor Book.* New York: The New American Library.

Llanillo, L.L & Baustista, K.Y., 2017. Zones of Privacy: How Private? *Defense Counsel Journal,* 84(3), pp. 1–28.

Maksukorralduse seadus[1] (2002) RT I, 30.06.2020, 30.

Maksu- ja Tolliamet, 2020. *Maksu- ja Tolliameti arengukava 2020*. [Võrgumaterjal] Leitav: https://www.emta.ee/sites/default/files/kontaktid-ja-ametist/ameti-struktuur-ulesanded-strateegia/strateegia/arengukava_2020.pdf [Kasutatud 29.10.2020]

Maksu- ja Tolliamet, 2021. *Maksukäitumise hinnagud.* [Võrgumaterjal] Leitav: https://www.emta.ee/et/maksukaitumise-hinnangud [Kasutatud 04.04.2021]

Meyer, D., 2020. *More Surveillance and Less Privacy Will Be the New Normal After the Coronavirus Pandemic*. [Web Material] Found: https://fortune.com/2020/04/20/privacy-surveillance-corona virus-pandemic-covid-19-tracking/ [Used 03.01.2021]

Moore, M.H., 1995. *Creating Public Value: Strategic Management in Government.* Cambridge: Harvard University Press.

OÜ LabelPrint hagi AS-i ESTOPRESS ja Eero Lattu vastu solidaarselt 2 000 000 krooni kahjuhüvitise saamiseks, AS-i ESTOPRESS vastu konkurentsi kahjustava tegevuse lõpetamiseks ning Eero Lattu vastu kohustamiseks mitte kasutama ning avaldama kolmandatele isikutele OÜ LabelPrint ärisaladusi. (2008) 3-2-1-103-08.

Parma, J., 2017. *Maksuvõla sissenõudmine kolmandatest riikidest OECD haldusabi konventsiooni alusel. Lõputöö.* Tallinn: Sisekaitseakadeemia.

Patendivoliniku seadus (2001) RT I, 22.12.2020, 44.

Paterson, M. & McDonagh, M., 2017. Freedom of information and the public interest: the Commonwealth experience. *Oxford University Commonwealth Law Journal,* 17(2), pp. 189–210.

Pindi Kinnisvara OÜ hagi Osaühingu Sholas vastu 27 000 euro suuruse leppetrahvi ja viivise saamiseks. (2017) 3-2-1-36-17.

Ravimiseadus[1] (2004) RT I, 01.07.2020, 11.

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F. & Fridgen, G., 2019. Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive,* 18(4), pp. 263–279.

Riigikontroll, 2020. *Andmete kättesaadavus ja kasutamine riigi targaks juhtimiseks.* 29.04.2020 märgukiri nr. 2-1/80031/3. [Võrgumaterjal] Leitav: https://www.riigikontroll.ee/tabid/206/Audit/2505/language/et-EE/Default.aspx [Kasutatud 29.10.2020]

Riigisaladuse ja salastatud välisteabe seadus (2007) RT I, 06.05.2020, 36.

Rockenbach, B., Sadrieh, A. & Schielke, A., 2020. Providing personal information to the benefit of others. *PloS one*, 15(8), pp. 1–15.

Salumaa, K., 2018. Andmesubjekti õigused uue isikuandmete kaitse üldmääruse foonil. *Juridica,* 2018/2, lk 83–93.

Schoenberger, L.M., 2010. Striking a Balance between Public Interest of Transparency of Government and the Privacy of Personal Identification and Security Information: An Examination of Tribune-Review Publishing Co. V. Bodack. *Widener Law Journal*, 19(2), pp. 577–591.

Sudžuka, E., 2020. Public Interest, Personal Data Protection and Bank Secrecy: A Brief Look at the Legal System of Bosnia and Herzegovina and Federation of Bosnia and Herzegovina. *Pregled*, 61(1), pp. 1–23.

Tupay, P.K. & Mikiver, M., 2015. E-Riik ja põhiõigused. *Juridica,* III, lk 163–176.

Värv, A., 2020. Ärisaladuse kaitse uus nägu. *Juridica,* V, lk 418–428.

Äriseadustik[1] (1995) RT I, 22.12.2020, 50.

Õunapuu, L., 2012. *Valimid kvantitatiivsetes ja kvalitatiivsetes uurimustes*. Tartu Ülikool. [Võrgumaterjal] Leitav : https://dspace.ut.ee/bitstream/handle/10062/27764/index.html [Kasutatud 29.11.2020]

Quinn, P., 2017. The Anonymisation of Research Data — A Pyric Victory for Privacy that Should Not Be Pushed Too Hard by the EU Data Protection Framework? *European Journal of Health Law*, 24(4), pp. 347–367.

Yin, R.K., 2011. *Qualitative Research from Start to Finish.* London: The Guilford Press.

Lisa 1. Ekspertintervjuude küsimused

1. Kas teie asutusel on olemas oma tööks vajalikud juurdepääsud maksumaksjatega seotud andmetele (ilma, et maksumaksja peaks ise need andmed teile esitama)?
2. Kas peate olemasolevat infot piisavaks enda ülesannete täitmisel? Kui vastus on eitav, millistest andmetest tunnete enim puudust?
3. Kuidas hindate erinevate asutuste vahelist koostööd maksumaksjatega seotud andmete vahetamisel?
4. Kuidas defineeriksite mõistet „maksumaksjate keskne profileerimine“?
5. Millised puudused on teie arvates praegusel andmevahetusel?
6. Kas teie asutuses on kasutusel riskiprofiilid maksumaksjatest ning kuivõrd on see protsess automatiseeritud?
7. Palun teie arvamust maksumaksjatega seotud andmete kättesaadavusest riskiprofiili loomisel. Kui arvate, et see vajaks parendamist, siis millised oleksid teie soovitused?
8. Milliseid tugevusi näete hetkel süsteemis, mis kujutab endast andmete kättesaadavust ja andmete vahetamist asutuste vahel?
9. Milliseid ohte te näete andmekaitsenõuete täitmisel, kui füüsiliste ja juriidiliste isikute andmeid võimaldataks asutuste vahel piiramatult vahetada?
10. Kuidas hindate enda asutuse valmisolekut selliseks andmevahetuseks, kas te suudaksite praegusel hetkel tagada piisavad andmekaitsetingimused?
11. Milline on teie arvamus selle kohta, et andmevahetuse suurendamine asutuste vahel on avalikes huvides?
12. Kuidas mõjutasid teie asutuse põhiprotsesse COVID-19 seotud Vabariigi Valitsuse otsused piirangute seadmisel ja toetuste määramisel?
13. Kas vajadus andmete kättesaadavusele, sh automatiseerituse tasemele kasvas või jäi samaks?
14. Milliseid uusi lahendusi ja võimalusi tõi kaasa teie asutusele COVID-19 kriis nt toetuste määramisel ja muudes menetlustes?
15. Millistel tingimustel saaks neid ka tulevikus rakendada?
16. Palun võrrelge praegust olukorda ja enne märts 2020 aegseid võimalusi andmevahetuse ning andmetöötlemise võimaluste osas ning andke oma hinnang toimunud muutustele?

17. Milline on teie arvamus asutuste vahelise andmevahetuse suurendamise vajalikkuse kohta? Palun põhjendage oma arvamust konkreetsemalt.
18. Milliseid võimalusi teie näete andmevahetuse suurendamisel, kuidas või mil moel seda teostada?
19. Kuidas muudaks teie asutuse põhiprotsesse võimalus lähtuda riigis maksumaksja riskiprofiilist, mis on loodud kõiki olulisi isikuandmeid arvesse võttes ja see uueneks konkreetse sammuga (igapäevaselt, igakuiselt jne)?
20. Kas teie asutusel oleks võimekus sellise profiili integreerimiseks enda otsustusprotsessidesse?
21. Milliseid positiivseid ja negatiivseid tagajärgi võiks andmevahetuse suurendamine asutuste vahel kaasa tuua asutustele, maksumaksjatele ning maksuhaldurile?

Lisa 2. Kategooriate ja koodide tabel

Kategooriad	Koodid
Kategooria 1 praegused probleemid andmevahetusel	Kood 1 tööks vajalike andmete puudumine Kood 2 dubleerimine Kood 3 pettuste info puudumine Kood 4 andmeid hoitakse ühes asutuses Kood 5 seadusandluse piirangud andmete vahetamisel ja töötlemisel Kood 6 ühtse ülevaate puudumine andmete olemasolust Kood 7 vähene automaatsus ja süsteemsus Kood 8 ühtse vastutaja puudumine Kood 9 vähene asutuste vaheline koostöö Kood 10 teatud asutuste vahel head ja tihedad kokkupuutepunktid Kood 11 asutuste erinev IT võimekus Kood 12 vead infovahetusel Kood 13 eriarvamused Kood 14 kontrollpäringute puudumine
Kategooria 2 andmekaitsega seotud probleemid	Kood 1 ranged andmekaitse reeglid Kood 2 andmekaitseekspertide erinev lähenemine Kood 3 asutuste vaheliste piiride võimalik kadumine keskse süsteemi loomisel Kood 4 asutuste erinev võimekus andmekaitsenõuete tagamisel Kood 5 ametnike ja töötajate poolne andmete kuritarvitamine Kood 6 andmete lekke oht vähe turvalise võrgu kaudu Kood 7 võimalik liigne isiku õiguste riive keskse süsteemi loomisel

Kategooria 3 avalik huvi andmevahetuse suurendamisel	Kood 1 ressursside tark kasutamine Kood 2 jõudmine abivajajateni Kood 3 riigi maine suurendamine Kood 4 riigiabi suuruse teadmine Kood 5 head ja mugavad teenused Kood 6 paremad prognoosimis- ja otsustusvõimalused erinevates valdkondades Kood 7 ajakohased ja õiged andmed Kood 8 läbipaistvuse tagamine Kood 9 kiiremad lahendused Kood 10 võrdsetel alustel toetuste maksmine Kood 11 COVID-19 kriisi mõjud andmevajadusele
Kategooria 4 riigiasutuste andmevahetuse vajadused	Kood 1 parema järelevalve tagamine Kood 2 skeemide vältimine Kood 3 tööprotsesside tõhustamine Kood 4 paremad prognoosimis ja otsustus võimalused erinevates valdkondades Kood 5 ajakohaste ja õigete andmete olemasolu Kood 6 riigiasutuste kvaliteedi ühtlustamine Kood 7 kiiremad lahendused Kood 8 parima teeninduskanali määramine maksumaksjale Kood 9 ressursside ühendamine Kood 10 bürokraatia vähendamine
Kategooria 5 riigiasutuste suurema andmevahetuse ja ühtse riskiprofiili loomise võimalused	Kood 1 ühes aknas kuvamine Kood 2 erinevate andmete olemasolu kokku grupeerimine Kood 3 vajalik seadusandluse muutmine Kood 4 andmekaitsetingimuste tagamine Kood 5 suhtluskanal (nt X-tee)

	Kood 6 keskne andmebaas Kood 7 MTA Hinnangute projekt Kood 8 asutusesiseste regulatsioonide muutmine, kehtestamine Kood 9 läbi Sharepoint´i aruandlusmudelite Kood 10 rahaliste ja inimressursside olemasolu Kood 11 samade hindamispõhimõtete kasutamine riskiprofiilis Kood 12 maksuandmete kasutamine toetuste määramise alusena Kood 13 koondhinnangu kasutamine maksumaksjast Kood 14 osadeks jaotatud riskiprofiil Kood 15 varasemate eksimuste kuvamine riskiprofiilina