



ELIISE SCHMUUL

**MAKSUMAKSJATE
KESKSE
PROFILEERIMISE
VAJALIKKUS JA
VÕIMALUSED**

FINANTSKOLLEDŽI TOIMETISED

NR 2/2021 (5)

FINANTSKOLLEDŽI TOIMETISED

NR 2/2021 (5)

ELIISE SCHMUUL

**MAKSUMAKSJATE
KESKSE
PROFILEERIMISE
VAJALIKKUS JA
VÕIMALUSED**



FINANTSKOLLEDŽ

sisekaitse.ee

Finantskollidž on tolli ja maksunduse erialal õppetööd, täiendusõpet, rakendusuuringuid ning teadus- ja arendustegevust korraldav struktuuriüksus Sisekaitseakadeemias. Finantskollidži Toimetistes avaldatakse tolli ja maksunduse erialaga seotud kirjeldavaid, analüütilisi ja uurimuslikke kirjutisi. Kirjutisi ei ole eelretsenseeritud ja nende sisu eest vastutavad autorid.

Autoriõigus: Sisekaitseakadeemia 2021

Keeletoimetaja: Siiri Soidro

Makett: Jan Garshnek

Küljendus: OÜ Flagella

ISBN 978-9985-67-357-7

ISSN 2674-3493

Finantskollidž

Sisekaitseakadeemia

Kase 61, 12012 Tallinn

e-post: fktoimetised@sisekaitse.ee

www.sisekaitse.ee/et/FK

www.sisekaitse.ee/kirjastus

SISUKORD

Sissejuhatus	5
1. Andmekaitsest ja avalikust huvist maksumaksjate kesksel profileerimisel	6
2. Maksumaksjate keskne profileerimine asutuste andmevajaduste täitmisel ja toetuste määramisel	11
2.1. Uurimismetoodika	11
2.2. Intervjuude tulemused	11
2.3. Tulemuste analüüs	14
Järeldused	17
Viidatud allikad	18

SISSEJUHATUS

Maksumaksjate keskne profileerimine on andmevahetuse suurendamine asutuste vahel, et tagada ühtsem profiil maksumaksjatest, paremate teenuste pakkumiseks ja pettuste vältimiseks, mis võimaldaks ajakohaseimat kuva maksumaksjatest. Maksumaksjate keskne profileerimine ei ole ainult andmevahetamise suurendamine, vaid ka ühtse riskiprofiili loomine riigis, et tõhustada riiklikku järelevalvet. Keskne profiil võimaldaks kiirelt reageerida isiku profiili muutustele, mis tõhustaks toetuste tagasiküsimisi või võimaldaks raskustesse sattunud isikut efektiivselt ja kiirelt aidata. Maksumaksjate keskseks profileerimiseks on vaja teada, millisel tasemel on asutuste koostöö ja andmevahetus, kuna see võib parandada riigiasutuste vahel andmete vahetamist ja nende kasutamist.

Uuringu aktuaalsus tuleneb Eesti Vabariigi Valitsuse „Eesti 2035” strateegiast, kus on välja toodud, et riigivalitsemise tõhusus peab suurenema, et pakkuda kvaliteetseid avalikke teenuseid. Seejuures on ühe väljundina mainitud 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).

Töö uurimisprobleemiks oli küsimus, kuidas saavutada mõistlik tasakaal andmekaitse normide ja avaliku huvi vahel isikuandmete töötlemisel. Uurimisprobleemi lahendamiseks tõstatati järgmised uurimisküsimused:

1. Millised probleemid on maksumaksjate kesksel profileerimisel?
2. Miks on vajalik riigiasutuste andmevahetuse suurendamine ja praeguste andmekaitsetõkete leevendamine?
3. Kuidas oleks võimalik suurendada andmevahetust riigiasutuste vahel ja luua ühtne riskiprofiil?

Uuringu eesmärk oli välja selgitada maksumaksjate keskse profileerimise vajalikkus ning leida viisid maksumaksjate keskseks profileerimiseks andmekaitse norme kahjustamata ja avalikku huvi piiramata. Eesmärgi saavutamiseks analüüsiti teaduskirjandust, õigusakte ja tehti eksperdiintervjuud asutuste esindajatega, et analüüsida maksumaksjate keskse profileerimise vajalikkust ja võimalust. Artikkel põhineb samanimelisel lõputööl.

1. ANDMEKAITSEST JA AVALIKUST HUVIST MAKSUMAKSJATE KESKSEL PROFILEERIMISEL

Selleks et mõista intervjueeritavate seisukohti ja probleeme maksumaksjate keskel profileerimisel, on oluline anda ülevaade andmekaitse nõuetest avaliku sektori teabevahetusel ja avaliku huvi olemusest. Maksumaksjana käsitletakse nii füüsilisi kui ka juriidilisi isikuid ja seetõttu on vaja maksumaksjate keskel profileerimisel juhinduda mõlema õigussubjekti andmekaitse nõuetest, mis on erinevad, kuid tihedalt seotud.

Andmete kaitsmine on sätestatud eri seadustes ja määrustes ning selle eesmärk on andmeid kaitsta igasuguse ohu eest. Peamine regulatsioon, millest Euroopa Liidus juhindutakse, on Euroopa Parlamendi ja Nõukogu määrus 2016/679 (edaspidi *GDPR*) (Euroopa Parlament ja Euroopa Nõukogu, 2016). Kui minna andmekaitsekaasuste lahendamise juurde, siis kõige olulisem on inim- või põhiõigusteteemalistel vaidlustel proportsionaalsuse põhimõte, mis võimaldab struktuurselt hinnata meetme rakendamise üldist mõistlikkust, kuid oluline on ka teadmine, et inim- ja põhiõiguste praktika Euroopas keskendub üldiselt avaliku võimu organite tegevuse põhjendamisele, lähtudes mõistlikkusest (Kumm, 2020, lk 103 ja 109).

Andmekaitsemääruse 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 oma organisatsioonile vajalikke andmeid. Näiteks annab *GDPR* artikkel 15 andmesubjektidele õiguse taotleda juurdepääsu nende kohta kogutud andmetele ja artikkel 17 õiguse lasta need kustutada (Euroopa Parlament ja Euroopa Nõukogu, 2016).

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 tekitab seaduselünki ja erinevaid tõlgendamisvõimalusi, seetõttu on isikul, kes peab määruse nõudeid täitma, *GDPR*-i keeruline lugeda ja mõista;
- 2) andmekaitse spetsialistidele 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 ressursse;
- 4) määruses ei ole kirjeldatud minimaalseid turvanõudeid enim kasutatavatele teenustele nagu WiFi-ühendus ja eravõrgu kaudu kaugjuurdepääs.

Enamasti töötleb avalik sektor isiklikku teavet, kuna neil on selleks seaduslik kohustus või kuna töötlemine on vajalik avalikes huvides. Riigiasutused peavad avalike ülesannete täitmisel põhjendama, miks on andmete töötlemine avalikes huvides vajalik. Kui ametnik peab avalikes huvides andmeid töötleva, kehtib see kõikidele isikutele: nii neile, kes on nõus oma andmete töötlemisega, kui ka neile, kes ei ole nõus andmete töötlemisega. (Klingenberg, 2016, p. 67–69)

Sarnaselt Eesti avaliku sektori ideele suurendada asutustevahelist andmevahetust tekkis Saksamaa avaliku sektori asutustel idee luua ühine toetav süsteem asuülitaotlejatega 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 nähti peamiste probleemidena seaduste uuendamise vajadust ja andmekaitse korralduslikke probleeme, kuna keskel süsteemil puudub üks vastutaja.

Selleks, et vastata GDPR-i nõuetele, leiti järgmised lahendused (Rieger, *et al.*, 2019, pp. 268–270):

- 1) vastutusalade kindlaksmääramine;
- 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 seaduse alusel näha.

Peale isikuandmete kaitset reguleerivate õigusaktide on oluline analüüsida ka maksukorralduse seadusest (edaspidi *MKS*) tulenevat maksusaladuse kaitset, mida käsitlevad *MKS* §-d 26–30 (*Maksukorralduse seadus*¹, 2002). Paljudele riigiasutustele on antud võimalus saada maksusaladust sisaldavat teavet *MKS* § 29 alusel ning lisaks maksuhaldurile on neile teatavaks saanud info saladuses hoidmise kohustus, mis tuleneb *MKS* § 26 lõikest 3 (*Maksukorralduse seadus*¹, 2002). Lehis (2015) leiab, et praktikas puudub kontroll selle üle, kas ka kolmandad isikud, kes on saanud maksusaladust sisaldavat teavet, kasutavad infot sihipäraselt või levitavad seda veel kellelegi, kellel puudub sellise info saamise õigus. *MKS* § 29 on esitatud 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 lõikes 1 on viidatud nii ärikuu ka pangasaladusele (Lind, 2009, lk 456; *Maksukorralduse seadus*¹, 2002). Pangasaladus on (*Krediidiasutuste seadus*¹, 1999 § 88 lõige 1) kõik andmed ja hinnangud, mis on krediidiasutusele teatavaks saanud tema või teise krediidiasutuse kliendi kohta. Samas paragrahvis on sätestatud juhud, kui krediidiasutus võib ja peab avaldama pangasaladust sisaldavaid andmeid, sh Maksu- ja Tolliametile (edaspidi *MTA*) (*Krediidiasutuste seadus*¹, 1999). Sisuliselt hõlmab pangasaladuse mõiste kõiki andmeid, mida klient krediidiasutusele teatavaks teeb, ning lisaks sellele krediidiasutuse hinnanguid, mida see kliendi kohta annab (Lind, 2009, lk 456).

17.11.2018 jõustus ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus (edaspidi *EKTÄKS*) ärisaladuse kaitse direktiivi üle võtmiseks Eesti siseriikliku õigusesse, kus on defineeritud muu hulgas ärisaladuse mõiste (Värv, 2020, lk 418). *EKTÄKS* § 5 lõike 2 järgi ei tohi ärisaladuse teave 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)

Andmekaitsetingimused on ranged, kuid andmete töötlemise võimalused on piisavalt laialdased, et võimaldada asutustevahelist suuremat andmevahetust. Töötlemine on õigustatud, kui tegevus on piisavalt põhjendatud ja on ära näidatud, milles seisneb töötlemise vajalikkus. Seejuures peab õiguste riive olema väiksem kui andmete töötlemisest saadav kasu. Eeltoodust lähtuvalt on avalikul sektoril 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 lisakriteerium töötlemise seaduslikkusele (Euroopa Parlament ja Euroopa Nõukogu, 2016). Määruse järgi peavad liikmesriigi seadused vastama üldist huvi pakkuvatele eesmärkidele või olema vajalikud teiste inimeste õiguste ja vabaduste kaitseks, austama andmekaitseõiguse olemust ja olema proportsionaalsed taotletava õiguspärase eesmärgiga (Klingenberg, 2016, p. 70; Dobos & Takács-György, 2019, p. 473).

GDPR-i 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, tuleb isikuandmete töötlemise laadi, ulatust, konteksti ja eesmarke arvesse võttes vastutaval töötlejal hinnata enne isikuandmete töötlemist toimingute mõju isikuandmete kaitsele. Mõjuhinnangu tegemine on näiteks nõutav artikli 39 lõike 2 punkti a järgi juhul, kui andmete töötlemisega teostatakse füüsiliste isikutega seotud isiklike aspektide süstemaatilist ja ulatuslikku hindamist, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas

profiilialüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis mõjutavad samaväärselt 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, et tagada 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 parandusettepanekuid, kui riigi andmetöötles on puudusi. Avalik huvi on teada ja mõista, kuidas kasutatakse massandmeid kui üksikisikute kohta koondatud andmeid ja kas selline kasutusviis on ühiskonnas vastuvõetav. 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)

Oluline on peatuda ka 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. 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 riskisutuses olevast süsteemist. Integreeritud registrite süsteem võimaldab rakendada uusi halduskorralduse põhimõtteid: kodanikeskus, paindlikkus, kiirus, väiksem raha- ja ajakulu nii kodanikule kui ka riigile. (Tupay & Mikiver, 2015, lk 164–165)

Asutustevahelise andmevahetuse juures on oluline avaliku huvi olemasolu. Kuid 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 see avaliku huvi 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. Näiteks kontrollivad kohtud avaliku huvi olemasolu n-õ avaliku huvi testi kaudu. Seal hinnatakse konkureerivaid aspekte ja nende omavahelist tasakaalu, sealhulgas hinnatakse valitsuse huvisid. (Paterson & McDonagh, 2017, p. 192)

Kui üksikisikute huvi on isikuandmete eemaldamine, siis avalik huvi on vastupidine. Avalik huvi võib olla defineeritud siseriiklikes seadustes. Näiteks on kirjeldatud, 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 vähendavad oluliselt isikute privaatsust ehk üksikisikute huve (Brough & Martin, 2021, p. 108). Paljud andmekaitse seadused lubavad kriisi ajal leevendada andmete töötlemise piiranguid, kuna see on avalikes huvides (Meyer, 2020). Näiteks on Euroopa Liidu isikuandmete kaitse üldmääruse (GDPR) kohaselt tavaliselt kaitstud kategooriateks geneetilised andmed, poliitilised ja religioossed sidemed ning kriminaalne ajalugu, kuid kriisiolukordades saab neid vabalt jagada (Meyer, 2020).

Eestis võeti sarnaselt teistele riikidele kasutusele mitmeid meetmeid COVID-19 vastu võitlemiseks ja kriisi majandusliku mõju leevendamiseks eriolukorra ajal ja sellele järgneval perioodil. Näiteks täiendati maksukorralduse seadust paragrahviga 168¹⁵, 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 seadus¹, 2002). Selline meede annab võimaluse tutvuda ettevõtete finantsseisundiga ja tuvastada need ettevõtted, kes vajavad enim abi, ning sellest tulenevalt rakendada vajalikke toetusmeetmeid ja vältida mahhineerijaid.

Kui otsida vastust küsimusele, kuidas võiks maksumaksjate keskne profileerimine kasulik olla, siis tuleb vastuse saamiseks analüüsida suurettevõtete tegevust. Ettevõtted, nagu Amazon.com, iTunes ja Netflix, salvestavad kasutajate klikke, vaatamisi ja tellimusi ning kaevandavad neid andmeid tähendust omava informatsiooni töötlemiseks, et mõjutada kliente soovitude, lisavalikute ja reklaamidega. Mida rohkem on ettevõtte informeeritud tarbija eelistustest, seda paremini on võimalik kliente suunata 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 (inglisekeelne 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)

Eesti Inimõiguste Keskus tegi 2019. aastal uuringu, kus oli üheks teemaks profileerimine. Uuringus kirjeldati proaktiivse teenuse tähendust, mis on uut tüüpi avalik teenus, mida riik osutab omal algatusel. Proaktiivne teenus tähendab ennetavat või ettehoolitavat 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) Sisuliselt on proaktiivse teenuse olemus sama, mida kasutavad suurettevõtted, kui hindavad tarbija eelistusi, et pakkuda klientidele üha uusi valikuid, mis võiksid neile sobida.

Samas uuringus leiti profileerimise ja selle käigus pakutavate proaktiivsete teenuste plussina, et teenused aitavad tagada õigust võrdsele kohtlemisele, kuna jõuavad rohkem inimesteni, kes neid vajavad, aga ei ole teenuseid saanud kas teadmatusel 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 puutumatusel ja isikuandmete kaitse õigusele, kuna proaktiivse teenuse puhul võib olla ohustatud inimese autonoomia ja valikuvabadus. Lahendustena nähti põhjalikku eelnevat analüüsi ja 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 kavatsatud vajalike muutustena viia teenused võimalikult palju taustal toimivaks ja etteaimatavaks ehk proaktiivseks. Sealjuures tuleb arvestada inimese tahet ja põhiõigusi, kuna proaktiivsete teenuste kasutamise puhul eeldatakse kõigi riigil olemasolevate andmete turvalist kasutamist. (Eesti Vabariigi Valitsus, 2021b)

Pärast uue tehnoloogia kasutuselevõttu suureneb üldjuhul tulemuslikkus oluliselt, kuid kaasnevad teatud kulud. Targad investeeringud tehnoloogiasse aitavad tuttavaid ülesandeid lahendada efektiivsemalt ja 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 annaksid riigile suure konkurentsieelise. Asutustesse kogunenud andmeid käsitletakse kohustusliku arhiivimaterjalina ega saada tihti aru andmete vajalikkusest. (Karu, 2021, lk 44–45) Seetõttu on ka Vabariigi Valitsuse strateegias eesmärk muuta teenused taustal toimivaks, mis tähendab oluliselt suuremate andmehulkade kasutuselevõttu.

Avalik huvi on igapäevane enda defineerida, kuna see on tihti segatud isiklike huvidega. 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. Andmekaitsekaasuste lahendamisel tuleb lähtuda mõistlikkusest ja proportsionaalsuse põhimõttest. Seejuures hinnatakse avaliku huvi olemasolu kontrollimisel erinevaid konkureerivaid aspekte ja nende omavahelist tasakaalu. Sellest võib järeldada, et kui andmekaitsetingimusi ja avaliku huvi olemasolu hinnatakse ja kontrollitakse sama objektiivselt, siis on võimalik saavutada olukord, kus üks ei pea kahjustama teist. Seda on järeldanud ka USA Pennsylvania osariigi kohtulahend (Schoenberger, 2010, p. 591). Maksumaksjate keskne profileerimine on avalikes huvides, kuna see loob lisandväärtust, avaldades positiivset mõju avalikele teenustele ja teenuste tarbijatele. Näiteks oleks võimalik hinnata toetuse saamisel isikuga seotud riske, ilma et toetuse saaja peaks esitama hulgaliselt tõendeid mõnest muust asutusest, ning menetlusi saaks tänu sellele kiiremini läbi viia.

Maksumaksjate keskse profileerimise puhul on vajalik andmekaitsealase mõjuhinnangu koostamine, et hinnata asutustevahelise andmevahetuse suurendamise kooskõla andmekaitsetingimustega. Teaduskirjanduses soovitakse mõjuhinnang avalikustada selleks, et tagada huvitatud isikute õiguste kaitse. Maksumaksjate profileerimisel kaasnevad ka teatud ohud, mida Eesti Inimõiguste Keskuse uuringus mainiti. Kuid neid on võimalik lahendada samas uuringus pakutud võimalustega, milleks oli põhjalik eelnev analüüs ja isikuandmete terviklahenduse loomine, kus on võimalik loobuda isikuandmete kasutamise nõusolekust või esitada vastuväiteid; see suurendaks omakorda riigi läbipaistvust. Läbipaistvus on üks korruptsiooni, pettuste ja rahapesu vastu võitlemise põhimõtetest ja viisidest, mis on nõutav riiklike vahendite haldamisel (Sudžuka, 2020, p. 2).

2. MAKSUMAKSJATE KESKNE PROFILEERIMINE ASUTUSTE ANDMEVAJADUSTE TÄITMISEL JA TOETUSTE MÄÄRAMISEL

2.1. Uurimismetoodika

Uurimismeetodina kasutati kvalitatiivset uurimismetoodikat ja andmeanalüüsi viidi läbi kvalitatiivse sisuanalüüsiga. Andmekogumise meetodina kasutati eksperdiintervjuusid asutuste esindajatega, kuna uuringu eesmärgi saavutamiseks oli oluline teada eri asutuste arvamust, et välja selgitada maksumaksjate keskse profileerimise vajalikkus ja võimalused. Ekspertidel on teadmised praegusest andmevahetuse toimimisest ja seeläbi on neil ka paremad ideed andmevahetuse parandamiseks olemasoleva süsteemi pinnalt. Valimiks oli mittetõenäosuslik eesmärgistatud valim, milleks olid eksperdiintervjuud Ettevõtluse Arendamise Sihtasutuse, Haigekassa, Keskkonnainvesteeringute Keskuse, MTA, Põllumajanduse Registrite ja Informatsiooni Ameti, Sotsiaalkindlustusameti, Töötukassa ning Tallinna Kesklinna Valitsuse sotsiaalhoolekandeosakonna esindajatega. Kriteeriumid olid järgmised: intervjuueeritav on avaliku sektori asutuse ametnik, kes on töötanud vähemalt 3 aastat praeguses asutuses või kellel on kogemus sarnases valdkonnas üle 5 aasta, ning asutus, kus intervjuueeritav töötab, väljastab rahalisi toetusi või peab järelevalvet asutuste töö üle. Kokku intervjuueeriti 13 eksperti, kelle keskmine tööstaaž oli 11,7 aastat, intervjuud kestsid 40–89 minutit

2.2. Intervjuude tulemused

Alapeatükis esitatakse intervjuueeritavate peamised seisukohad. Ekspertid annavad hinnangu maksumaksjatega seotud andmetega tutvumise võimaluste kohta teise asutuse juures ja nimetavad, millistest andmetest asutused oma ülesannete täitmisel enim puudust tunnevad. Millised on andmevahetust takistavad probleemid ja andme-kaitsenõuetest tingitud mõjutused andmete vahetamisel. Milliseid positiivseid ja negatiivseid tagajärgi võiks kaasa tuua asutustevahelise andmevahetuse suurendamine ja milliseid võimalusi näevad andmevahetuse parendamiseks ekspertid ise ning milline on avalik huvi asutuste esindajate jaoks andmevahetuse suurendamisel.

Ekspertid defineerivad maksumaksjate keskset profileerimist maksumaksjaga seotud andmete muustritena kasutamist või maksumaksja info kogumisenä, mis kasutab samu hindamispehimõtteid ja mida on võimalik kasutada ka teistel asutustel peale andmete haldaja. Seejuures peaks saama seda ühes aknas kuvada (inglisekeelne väljend *single window*) ja maksumaksjate keskse profileerimise abil määrata kliendile parima teeninduskanali.

Ekspertidelt uuriti, millistest andmetest nad oma töös puudust tunnevad ja kuidas nad hindavad andmete vahetust asutuste vahel. Üldiselt leidsid ekspertid, et neil on piisavalt andmeid tööülesannete täitmiseks, kuid siiski ilmnes palju andmeid, millest oleks nende töös kasu. Enim tuntakse puudust toetuste infost ehk kui palju ja millisest asutusest on keegi toetust saanud või millised probleemid ja võimalikud pettuse riskid on toetuse taotlejal tuvastatud. Toetustega seotud info on vajalik näiteks riigiabi suuruse hindamiseks, et oleks võimalik jälgida, millal võib olla tegemist keelatud riigiabiga, samuti selleks, et tagada toetuste väljamaksmine õigustatud isikutele ja vältida mahhinatsioone toetuste taotlemisel. Põhimõtteliselt võib isik taotleda toetust mitmest asutusest ja lõpuks

võib toetuse summa ületada asja maksumust, kuid asutustel ei ole selliste pettuste jälgimiseks süsteemset kontrolli. Samuti oleks asutustel kasu maksumaksjate maksualase käitumise ja tuvastatud maksuriskide infost, milles saaksid asutused oma protsessides ja töös lähtuda.

Mitu asutust tõid näiteid dubleerimistest ja ressursside raiskamisest. Näiteks on võimalik rehabilitatsiooniteenuseid saada eri asutuste kaudu, kuid isik võib lõpuks minna ühte kohta teenust saada. Selleks et seda teenust saada, peavad eri asutused menetlema sisuliselt sama asja, samuti peab klient asju ajama mitmes asutuses. Ollakse üksmeelel, et rehabilitatsiooniteenuse pakkumisel võiksid asutused rohkem koostööd teha ning vähendada seeläbi nii maksumaksja kui ka asutuste enda koormust. Ekspertid mainisid ka seda, et andmeid kirjeldatakse liigselt eri kohtades ja samu andmeid saadetakse eri kanaleid pidi. Üks ekspert tõi ressursside raiskamisena järgmise näite: „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 kliendihaldusploki arendamise eest, kuigi see on korduvkasutatav. 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.”

Suur probleem on asutustes ühtse ülevaate puudumine, kust on mingit infot võimalik saada ja millist infot on üldse võimalik saada. Probleemiks on ka eriarvamused andmete vahetamise lubatavusel. Ekspertide hinnangul tekivad eriarvamused näiteks personali liikumise tõttu. Kui lahkub jurist, kelle arvates oli teatud andmevahetus teatud eesmärgil lubatav, siis järgmine jurist ei pruugi enam nii arvata. Praegust koostööd andmete vahetamisel iseloomustab üleüldise automaatsuse ja süsteemsuse puudumine, kuna asutustel on erinev IT-võimekus ja kõik ei ole võimelised automatiseeritult edastama masintöödeldavaid andmeid.

Esindajate hinnangul saadakse mõnikord andmeid liiga hilja ehk selleks hetkeks, kui asutus saab andmed, on need juba liiga vanad. Vahel tuleb teisele asutusele saata meeldetuletus e-kirjaga selle kohta, et nad lubasid andmeid saata, teatud andmed laekuvad korra kvartalis, kuid andmete saamise hetkeks võib andmevajadus olla juba kadunud.

Andmekaitsealase ohuna nähti aga töötajat, kes vaatab andmeid kogemata või uudishimust ning asutuste erinevat võimekust andmekaitse ja IT-tingimusi tagada. Ühe eksperdi sõnul nähtub nende statistikast, et kõige suuremad rikkumised on tööülesanneteta isikuandmete vaatamine.

Suurima puudusena andmevahetuse suurendamisel nähakse seadustest tulenevaid piiranguid andmete saamisel. Seda kirjeldati järgmiselt:

- 1) andmevahetust ei ole õigusaktides piisavalt reguleeritud;
- 2) maksukorralduse seaduses sätestatud maksusaladuse kaitse ei lase andmeid avaldada ehk andmete avaldamise võimalused ei kata piisavalt asutuste andmevahetuse vajadusi;
- 3) pangasaladuse avaldamise piirang ja muud andmekaitsealased piirangud takistavad andmevahetust.

Ühe eksperdi hinnangul tuleks andmekaitseexpertidel luua ühtne teadmine, mis on aktsepteeritav ja mis mitte, kuna andmekaitsele lähenetakse väga erinevalt.

Lisaks eelmainitule paluti ekspertidel hinnata andmevahetuse suurendamise ja maksumaksjate keskse profileerimise kasutegureid, sh miks on andmete saamine avalikes huvides. Ekspertid tõi avaliku huvi objektiks olevate teemadena, mis andmevahetuse suurendamisel paraneksid, välja järgmise:

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

Enim nimetati avaliku huvi ja riigiasutuste andmevahetuse vajaduste näitena skeemide vältimise võimalust tänu suuremale andmete töötlemisele. Nii on võimalik tuvastada ebakõlad andmetes juba eelmenetluses ning vältida põhjendamatuid otsuseid, jõuda rohkemate abivajajateni ja maksta toetuseid võrdsematel alustel. Seetõttu peaks just riskiinfo jagamine olema avalikes huvides.

Andmevahetuse suurendamise tulemusena oleks võimalik kiireid lahendusi kasutades määrata maksumaksjale parim teeninduskanal lähtudes just tema vajadustest, tõhustada tööprotsesse, ühtlustada kvaliteeti, tagada parem järelevalve ning kasutada avaliku sektori ressursse targalt. Üks ekspertidest tõi näite vaktsineerimisprotsessist, kus oli väga oluline näidata avalikkusele töödeldud aruandeid, kui palju on vaktsineeritud ja millistel ametipostidel, kuid neil ei olnud selleks vajalikke töötajate registri andmeid, kus oleks saanud välja valida eri ametite esindajaid. Üha suurema vaktsineerimisvõimekuse tõttu ilmselt mingi hetk see vajadus kaob, kuid teatud olukorras peaks olema edaspidi võimalik riigiasutustel kokkuleppeid sõlmida selliste andmete jagamisel, et olla riigina läbipaistev.

Eksperdid olid bürokraatia suurenemise või vähenemise suhtes vastakal seisukohal. Negatiivse külje pealt võib ekspertide arvates andmevahetuse suurendamine ja maksumaksjate keskne profileerimine suurendada bürokraatiat ning seeläbi kasvatada asutuste töömahtu, sest maksumaksja profiilis võivad sisalduda andmed, mida ei oska teised asutused põhjendada. Selleks et mõista, miks isik ei kvalifitseerunud näiteks toetuse saajaks, võib maksumaksja liikuda eri asutuste vahel.

Kuidas luua riigiasutuste suurem andmevahetus ja ühtne riskiprofiil? Leiti, et esiteks tuleks andmevahetuse suurendamisel veenduda andmekaitsetingimuste tagamises, milleks töid eksperdid mitmeid lahendusi:

- 1) kasutusõiguste selgelt määratlemine;
- 2) andmete edastamine krüpteeritult;
- 3) kliendi nõusoleku küsimine;
- 4) põhjendamine, miks andmeid vaadatakse;
- 5) vajaduse korral andmete kustutamise võimaluse tagamine;
- 6) nõuete täitmise kontroll;
- 7) teavitustöö ja koolitamine.

Andmevahetuse suurendamise võimalustena nähti ka seaduste muutmist, mis võimaldaks riigiasutuste vahel lihtsamini andmeid vahetada. Andmevahetuse suurendamise eeldusteks on ühes standardis või keeles suhtlemine andmete vahetamisel, andmevahetuse piiri määramine, mis ulatuses andmeid vahetada, Andmekaitse Inspeksiooni kaasamine lahenduste loomisesse, rahalise ja tööjõuressursi olemasolu, asutusesiseste regulatsioonide muutmise või loomine 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.

Eksperptide hinnangul on maksumaksjate keskel profileerimisel oluline riskide vaate kuvamine ja toetuse saamine võiks olla seotud maksukuulekusega. Laiemalt nähakse riigipoolse profiili loomist maksumaksjast ehk kõikide riigiasutuste keskse riskiprofiili loomist, mis peaks olema jaotatud osadeks, mida on võimalik eraldada vastavalt asutuste vajadustele. Kuid selline profiil võib minna liialt keeruliseks.

Kuidas tehniliselt suuremat andmevahetust korraldada, selles osas usuvad eksperdid X-tee toimimisse, kuid võimalusena nähakse ka kesket andmebaasi, 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 keskel andmebaasil haldamise küsimus, võimalik teiste andmebaaside duubeldamine ja andmekaitsetingimuste keerulisem tagamine.

Lisaks eespool toodule nähakse võimalusena riigiasutuste andmevahetust suurendada MTA maksukäitumiste hinnangute teenuse kaudu, mis on MTA väljatöötatud uus e-teenus ettevõtetele ja põhineb ettevõtete esitatud andmete analüüsil. Selle teenuse kaudu saavad ettevõtted oma maksukäitumises oluliste andmete kohta regulaarselt ajakohast tagasisidet.

2.3. Tulemuste analüüs

Halduskoormust saaks vähendada teatud andmete parema kättesaadavusega ning maksumaksja peaks seejuures mõistma ja taluma, et kvaliteetse abi saamiseks on vajalik abistajal ehk riigil kõige ajakohasemat ja täpsemat infot sarnaselt olukorraga, kui helistatakse hädaabinumbrile. Kui andmeid vahetada suuremal määral kui praegu, siis väheneksid oluliselt halduskulud. Näiteks on ametnikul võimalik lahendada sama aja jooksul 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. Selle asemel on tal olemas kõige uuemad andmed, mida teised asutused on isiku kohta kogunud. Seejuures tuleb mainida varem viidatud Klingenbergi (2016, p. 67–69), kelle sõnul peavad riigiasutused põhjendama, miks on andmete töötlemine avalikes huvides vajalik. Sellest võib järeldada, et riigil ei saakski olla muid andmeid peale nende, mis on vajalikud avalikes huvides.

Ühe probleemina nimetasid eksperdid eriarvamusi andmete vahetamisel. Eriarvamusel võivad tekkida sellest, et ühe asutuse sees ei vaadata ega hinnata tulemuslikkust riigis tervikuna, vaid asutused mõtleavad rohkem sellele, kuidas saavutada enda organisatsiooni eesmärgid. Ühe probleemina toodi välja andmekaitsepetsialistide erinev lähenemine, mida on mainitud ka teaduskirjanduses (vt nt Dakić & Ribarić, 2020, pp. 190–195). Vajadus luua andmekaitsepetsialistidele ühine teadmine, millal on andmekaitse tingimuste piires lubatav andmete vahetamine ja jagamine, kattub osaliselt eriarvamuste probleemiga, mille tõttu asutused pigem keelduvad andmevahetusest, sest kardavad võimalikke negatiivseid tagajärgi. Andmekaitse reeglid on ranged ja nende rikkumise puhul kohaldatakse suuri trahve. Väga oluline on, et rakendatakse ühtset lähenemist ja seatakse standardsed nõuded andmekaitse spetsialistidele, nii tekib selgus andmekaitse valdkonnas ja paraneb andmevahetus. Kuigi andmekaitse nõuded on ranged, ei peaks avaliku sektori asutused piirama selle kartuses andmete kasutamist või jagamist asutuste vahel.

Andmevahetust võiks parandada ühtse vastutaja olemasolu, kes otsustaks, kuidas, millal ja milliste andmete vahetamine on lubatud. Praegune ühtse vastutaja puudumine raskendab andmete kättesaadavust, kuna asutustel ei ole alati kindlat teadmist, kas andmeid võib vahetada, ja pigem keeldutakse andmete edastamisest teisele asutusele, kuna kardetakse võimalikke sanktsioone ja andmekaitse nõuete rikkumist. Ühtse vastutaja olemasolu tagaks muu hulgas teadmise, kust mingeid andmeid oleks võimalik saada. GDPR-i nõuete täitmist saaks keske süsteemi puhul lahendada vastutusala kindlaksmääramisega (Rieger, *et al.*, 2019, pp. 268–270).

Vastates lühidalt uurimisküsimusele, millised probleemid on maksumaksjate kesksel profileerimisel, saab kokkuvõtvalt väita, et kõikidel asutustel on olemas juurdepääs maksumaksjatega seotud andmetele, kuid eri ulatuses ja leidub mitmeid puudusi, mida asutused sooviksid oma töö tõhustamiseks kõrvaldada, ning andmevajadust, mida peetakse oluliseks lahendada. Enim soovitakse saada isikute kohta toetuste ja pettustega seotud infot, mille põhjal tõhustada järelevalveprotsesse ja tagada paremad otsused eelarve jaotamisel. Peamine probleem on asutuste hinnangul seadustest tulenevad andmekaitsepiirangud, mida käsitleti ka varasemates peatükkides. Võttes kokku intervjuude tulemused ja varasema teoreetilise käsitluse, saab järeldada, et seadustes ei ole asutustevahelise andmevahetuse kohta liigseid piiranguid, kui andmete vahetamine on õigustatud ja vajalik. 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 maksumaksjate kesksel profileerimisel ei suurendaks tõenäosust andmete lubamatuks töötlemiseks.

Pigem on suurim probleem maksumaksjate kesksel profileerimisel hoopis asutuste erinev IT-võimekus, mille tõttu ei ole praegu võimalik kõigil asutustel ühetaoliselt andmeid jagada ja vastu võtta ning väiksemad avaliku sektori asutused on ebavõrdsel positsioonil suuremate asutustega, kuna andmete jagamisel ei pruugi nad olla valmis võtma vastu X-tee kaudu andmeid ega edastama andmeid uuemaid lahendusi kasutades. Maksumaksjate kesksel profileerimisel tuleks alustada asutuste IT-võimekuse ühtlustamisest. Samas on leitud, et organisatsiooni tehnoloogia piiride laienemisel on raskem tagada andmekaitse nõuete täitmist ehk väiksem IT-võimekus annab teisalt eelise andmekaitse nõuete järgimisel, kuna andmekaitse vastutusala on lihtsam määratleda (Chavalit & Hohler, 2020, pp. 36–38). Kuid väiksema IT-võimekusega ei oleks maksumaksjate kesksel profileerimisel võimalik.

Ekspertide hinnangul paraneksid andmevahetuse suurenemisel mitu olulist valdkonda. Kõike ekspertide mainitud saaks teha paremini, kui riigiasutustel oleksid ajakohased ja õiged andmed, mis on kogu andmevahetuse olulisim

alus ja avaliku huvi objektiks olev teema. Kui asutustel ei ole ajakohaseid ja õigeid andmeid, siis ei ole võimalik midagi parendada. Andmevahetuse suurendamisel oleks asutustel suurem kindlus selles, et neil on kõige täpsem informatsioon maksumaksja kohta.

Ekspertide mainitud paranduskohtadest andmevahetusel sõltub ka riigi maine tervikuna, mis on oluline 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.

Oli eksperte, kes leidsid, et riigiasutuste andmevahetuse suurendamine ja maksumaksjate keskse profiili loomine suurendaks bürokraatiat. Kuid oli ka neid, kelle arvates andmevahetuse suurendamine ja keskne profiil vähendaks bürokraatiat. Selleks et bürokraatia väheneks maksumaksjate keskse profileerimise tulemusena, tuleks andmevahetuse suurendamist alustada koordineeritult ja põhjalikku eeltööd tehes, et vältida võimalikke probleeme. Asutused saaksid ajakohasemate ja õigete andmete abil tegeleda probleemidega enne nende tekkimist, mille tulemusel väheneks nii riigi kui ka maksumaksja tõendamiskoormus. Kompetentside jagamine on asutuste vahel vajalik, sest maksukompetents on MTA-l, kes oskab määrata maksuriske ja nõustada asutusi, kuidas nad 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, muuta protsesse efektiivsemaks ning prognoosida tuleviku meetmeid teenuste pakkumisel ja toetuste määramisel. 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 selgituste saamiseks pöörduma eri asutuste poole.

COVID-19 kriisi mõjul toimunud muudatused siseriiklikus regulatsioonis ilmestavad suurepäraselt andmevahetuse parendamise vajadust pikas perspektiivis ja seda, et tegelikult ei ole seadustest piiranguid, mis keelavad asutustel omavahel andmeid jagada, kui see on vajalik ja eesmärgipärane. Samuti ei sea andmekaitseõuded piiranguid selliseks andmevahetuseks, kui täita kõiki andmekaitsetingimusi.

Vastates uurimisküsimusele, miks on vajalik riigiasutuste andmevahetuse suurendamine ja praeguste andmekaitse tõkete leevendamine, võib öelda, et andmevahetuse suurendamine on vajalik eelkõige maksumaksjate heaolu suurendamiseks paremate ja mugavamate avalike teenuste abil, mida toetab andmevahetuse suurendamine. Samuti on andmevahetuse suurendamine ja maksumaksjate keskse profiili loomine oluline riigieelarve tõhusamal majandamisel, mille tulemusel oleks võimalik pikaajaliselt säästa administratiivsetelt kuludelt ja kasutada riigi raha muuks otstarbeks. Asjakohaste seaduste sõnastust tuleks täpsustada, et võimaldada keskse profiili kasutuselevõttu asutuste otsustusprotsessides, kuid sellise regulatsiooni puudumine ei ole oluliseks takistuseks andmevahetuse suurendamiseks asutuste vahel nende andmete puhul, mis on asutuste ülesannete täitmisel vajalikud ja põhjendatud.

Viimasena uuriti ekspertidelt, milliseid tehnilisi lahendusi nähakse andmevahetuse suurendamisel ja maksumaksjate keskel profileerimisel. Kuna X-tee loodi selleks, et avalik sektor saaks kasutada innovatiivseid lahendusi tänu avaliku halduse piires lõimitud infosüsteemile, ja X-tee lahendus on üldiselt hästi toimiv, oleks ekspertide pakutud tehnilistest võimalustest andmevahetuse suurendamiseks X-tee parim ja innovaatilisim lahendus. X-tee võimaldab suurendada kodanikukesksust, paindlikkust, kiirust ja vähendada raha- ja ajakulu nii kodanikule kui ka riigile (Tupay & Mikiver, 2015, lk 164–165).

MTA maksukäitumiste hinnangute teenus oleks alternatiiv ühisele riskiprofiilile, kuna andmete kuva on ühe vastutaja käes (antud juhul MTA) ja see lahendus ei suurendaks bürokraatiat, vaid pigem läbipaistvust, sest maksuandmed on mõtestatud ja teenuse kasutajale hõlpsalt loetavad. Hinnangute teenuse kuva saaks tehniliselt jagada teistele asutustele, et sarnaseid kuvasid saaks luua ka teiste asutuste poolt tuvastatud riske kaasates. Maksukäitumiste hinnangut peavad eksperdid parema otsustamise indikaatoriks kui pelgalt maksuvõla olemasolu fakti, mida nad on senini kasutanud toetuste määramisel.

Seejuures on maksumaksjate keskel profileerimisel oluline andmekaitsealase mõjuhinnangu koostamine, kuna teaduskirjanduses on leitud, et avalikkusele peaks olema läbipaistev, millistel muudel eesmärkidel samu isikuandmeid töödeldakse (Bogdanov & Siil, 2020, lk 480). Läbipaistvus on ka nõutav ja vajalik korruptsiooni, pettuste ja rahapesu vastu võitlemisel (Sudžuka, 2020, p. 2).

Vastates uurimisküsimusele, kuidas oleks võimalik suurem andmevahetus riigiasutuse vahel ning ühtne riskiprofiili loomine, saab öelda, et andmevahetuse suurendamisel ja ühtse riskiprofiili loomisel tuleb esmalt välja selgitada andmevajadus ehk milliseid andmeid on mingil asutusel vaja. Seejärel saab tuvastada kõige sobivamad kanalid nende andmete saamiseks ja veenduda andmekaitsetingimuste tagamises kõikides asutustes. Selleks tuleb koostada andmekaitsealane mõjuhindang ja põhjaliku eeltöö järel alustada andmevahetuse suurendamist, arendades X-tee juurdepääse andmetele. Samuti tuleks andmekaitse spetsialistidele luua ühine teadmine, milline andmete töötlus on riigiasutustes lubatud. Parim lahendus ühtse riskiprofiili kasutusele võtuks on praegu MTA maksukäitumiste hinnangute teenus, mida soovisid ka eksperdid oma töös kasutada ja leidsid, et toetuste saamine peaks olema seotud maksukuulekusega. Kui MTA suudab teha piisavat koolitustööd asutustele, kes MTA profiili oma töös kasutusele võtavad, siis paranevad teiste asutuste tööprotsessid, ilma et töökoormus oluliselt suureneks. Sarnaselt maksuandmetele võiks kaasata järgmise etapina hinnangutesse ka teiste asutuste olulist infot, näiteks toetuste kohta. Nii jääksid asutused enda kogutud andmete andmekogude omanikeks, aga andmevahetuse käigus saaks luua keskse riskiprofiili kuva, mis tagab ühetaolise vaate maksumaksjale, mida iga asutus saab oma töös rakendada.

JÄRELDUSED

On palju olukordi, mille lahendamiseks on vajalik suurem andmevahetus ja koostöö asutuste vahel. Ekspertide nimetatud vajadusi ja praeguse andmevahetuse puudusi analüüsidest võib järeldada, et maksumaksjate keskne profileerimine on vajalik selleks, et vältida pettusi, jõuda abivajajateni ja seejuures pakkuda häid ja mugavaid teenuseid ning mis kõige olulisem, vähendada oluliselt ressursside raiskamist ehk majandada riigieelarvet tõhusamalt.

Uuringus analüüsi põhjal saab järeldada, et andmevahetuse suurendamine asutuste vahel on vajalik ja võimalik. Järeldust ilmestab MKS § 168¹⁵ vastuvõtmine kriisiajal, et toetada laialdast andmevahetust eelarveotsuste langetamiseks. Ekspertid töid andmevajaduse kõrval välja mitmeid andmekaitsealaseid ohtusid andmete jagamise suurendamisel, kuid samad ohud on ka praeguses süsteemis olemas, seega ei suurendaks andmete jagamise suurendamine andmekaitseriski, kui asutused rakendavad kehtivaid andmekaitsemeetmeid samaväärselt kõikide andmete töötlemisele.

Maksumaksjaid on võimalik keskselt profileerida ilma andmekaitsenorme kahjustamata ja avalikku huvi piiramata, kui täiendatakse ja parandatakse seaduse sõnastust ning koostatakse andmekaitsealane mõjuhindang ja 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 luua võimalus, et asutused saaksid kasutada MTA juba olemasolevat riskiprofiili, kust nad saavad hinnangu maksumaksjate maksukäitumise kohta. Sinna võiks tulevikus 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 on tema töös vajalik.

Kui avalik huvi on see, mille inimesed valiksid Lippmanni (1955, p. 40) kirjeldatud viisil, siis oleks andmevahetuse suurendamine ja riskiprofiilide jagamine asutuste vahel võimalik ilma avalikku huvi piiramata, kuna andmete vahetamisest saadav kasu on ühiskonnale tervikuna suurem kui üksikisikute tajutav võimalik põhiõiguste riive. Oluline on veel kord välja tuua ka Pennsylvania kohtulahend, mis leidis, et andmete kaitse ja avalik huvi saavad olla üksteist kahjustamata tasakaalus. Kuna avalik huvi on teada, kuidas andmeid riigis kasutatakse, on vajalik maksumaksjate kesksel profileerimisel andmekaitsealase mõjuhindangu koostamine ja avaldamine. Samuti tuleb avalikustada teave, millistel juhtudel jagatakse isikute andmeid teiste asutustega.

VIIDATUD ALLIKAD

- Bogdanov, D. & Siil, T., 2020. Infotehnoloogilised võimalused põhiõiguste kaitsel. *Juridica*, VI, lk 474–481.
- 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. Judicial 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 seadus¹ (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 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.
- 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.
- 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.
- Krediidasutuste 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.
- 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].
- 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
- Maksukorralduse seadus*¹ (2002) RT I, 30.06.2020, 30.

- 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].
- 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.
- 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.
- 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.

