

# „Näita käppa“ ehk minu digiallkiri, järelikult minu tehtud tehing<sup>\*1</sup>

## 1. Sissejuhatus

Uudised selle kohta, kuidas inimeste elektrooniline identiteet (edaspidi eID) on neilt välja petetud ning seda hiljem mõne tehingu tegemiseks kasutatud, on muutunud pea iganädalaseks nähtuseks.<sup>\*2</sup> Küll saadavad petturid SMS-e, väites, et tellitud postipakk on tolli kinni jäänud või ähvardab seda tagasi müüjale saatmine, sest sisestatud kättetoimetamisadress oli vale, või jõuab telefoni või e-posti teel inimeseni info selle kohta, et tema pangakontole on tema teadmata keegi ligi pääsenud ning asunud seal omatahtsi toimetama. Ilmselt suudab ka lugeja ise mõnd sarnast hiljuti saadud sõnumit meenutada. Kõigi selliste juhtumite puhul on ühiseks jooneks, et inimest kiirustatakse sisestama kas oma pangakaardi või eID andmeid mõnele kodulehele või neid muul moel sõnumi edastajale üle andma. Petturite tegevus on üles ehitatud nutikalt, rõhutatakse kiire tegutsemise vajadust ja toetutakse hästi vormistatud sõnumitele/veebilehtedele ning sageli kasutatakse ära olukorda, kus inimese tähelepanu on hajutatud. Seetõttu satuvad selliste pettuste ohvriks mitte ainult vähe- sama digitaalse kirjaoskusega inimesed, vaid ka kõrgelt haritud ja igapäevased eID kasutajad.<sup>\*3</sup>

Tegemist ei ole seejuures sugugi vaid Eestile omase probleemiga. Analoogseid petuskeeme kasutatakse kogu Euroopas<sup>\*4</sup> ning erilist tähelepanu on need viimastel aastatel pälvinud näiteks Norras.<sup>\*5</sup>

<sup>1</sup> Käesolev artikkel on valminud Norwegian Research Council'i poolt rahastatava projekti „Societal Security and Digital Identities“ (projekti nr 320785) toetusel ning põhineb 38. õigusteadlaste päevade ettekandel 26. septembril 2024 Tartus.

<sup>2</sup> A. Pau. Riigiasutused vaatavad pealt, kuidas petturid krediidasutuste kaudu ohvritelt miljoneid lüpsavad. – Delfi Forte, 18.10.2024. Arvutivõrgus: <https://forte.delfi.ee/artikkel/120330015/riigiasutused-vaatavad-pealt-kuidas-petturid-krediidasutuste-kaudu-ohvritelt-miljoneid-lupsavad> (18.10.2024); D. Tiidema. SMS-pettus. Küberkurjategijad õngitsevad Omniva nime all kümneid tuhandeid ohvreid. – Postimees, 12.08.2024. Arvutivõrgus: <https://majandus.postimees.ee/8076566/sms-pettus-kuberkurjategijad-ongitsevad-omniva-nime-all-kumneid-tuhandeid-ohvreid> (13.09.2024); A. Täker. Uus SMS-pettus. Petturid õnnitlevad töölevõtmise puhul. – Postimees, 18.04.2024. Arvutivõrgus: <https://majandus.postimees.ee/8003651/uus-sms-pettus-petturid-onnitlevad-toolevotmise-puhul> (13.09.2024); A. Täker. Uus Taktika. Petusõnumites palutakse saata sõnum teisele platvormile. – Postimees, 20.08.2024. Arvutivõrgus: <https://majandus.postimees.ee/8080369/uus-taktika-petusonumites-palutakse-saata-sonum-teisele-platvormile> (13.09.2024); D. Tiidema. Küberkurjategijad jätkavad Omniva sõnumite levitamist: tuvastamise nipid ja ohumärgid. – Postimees, 13.08.2024. Arvutivõrgus: <https://majandus.postimees.ee/8077223/kuberkurjategijad-jatkavad-omniva-sonumite-levitamist-tuvastamise-nipid-ja-ohumargid> (13.09.2024); Hoiatus! LHV nimel saadetakse massiliselt petukirju. – Postimees, 13.07.2024. Arvutivõrgus: <https://majandus.postimees.ee/8058535/hoiatus-lhv-nimel-saadetakse-massiliselt-petukirju> (13.09.2024); A. Pihlak, J.-R. Jõesaar. „Sinu LHV kontolt tehti volitamata tehing.“ Mustamäe mees pettis õngitsussõnumitega Eesti inimestelt välja tuhandeid eurosid. – Delfi, 15.09.2024. Arvutivõrgus: <https://www.delfi.ee/artikkel/120321541/sinu-lhv-kontolt-tehti-volitamata-tehing-mustamae-meis-pettis-ongitsussõnumitega-eesti-inimestelt-valja-tuhandeid-eurosid> (16.09.2024).

<sup>3</sup> Vt nt samas.

<sup>4</sup> Vt nt The Latest Trends in Online Identity Theft in Europe. EITHOS, 28.06.2024. Arvutivõrgus: <https://eithos.eu/the-latest-trends-in-online-identity-theft-in-europe/> (16.09.2024); Study on online identity theft and identity-related crime. Final report. European Commission 2022, lk 15. Arvutivõrgus: <https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abad-11ec-83e1-01aa75ed71a1> (16.09.2024); Sorgfaltspflichten bei Zahlungsdienstleistern. Erkenntnisammlung Marktbeobachtung. Verbraucherzentrale Bundesverband e.V., 10.10.2024. Arvutivõrgus: [https://www.vzbv.de/sites/default/files/2024-10/24-10-10%20Bericht\\_vzbv\\_Sorgfaltspflichten%20Banken\\_final.pdf](https://www.vzbv.de/sites/default/files/2024-10/24-10-10%20Bericht_vzbv_Sorgfaltspflichten%20Banken_final.pdf) (02.11.2024); BEUC-i (The European Consumer Organisation) soovitusi seoses makseteenuste regulatsiooniga vt Payment Services. BEUC's recommendations on the Payment Service Regulation and the Payment Services Directive 3. BEUC, 29.09.2023. Arvutivõrgus: [https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-123\\_Payments\\_Services\\_Recommendations%20on%20the%20PSR-PSD3.pdf](https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-123_Payments_Services_Recommendations%20on%20the%20PSR-PSD3.pdf) (16.09.2024).

<sup>5</sup> Vt nt Advice that protects you from BankID fraud. BankID. Arvutivõrgus: <https://bankid.no/en/advice-that-protects-you-from-bankid-fraud> (16.09.2024); E. B. Brataas, M. S. Stokke, A. Svensson. Rapport om misbruk av eID. SODI-rapport 1/2022.

Kui eID kasutamiseks vajalikud andmed on sattunud petturite kätte, on selle üheks tagajärjeks paha-tihti ohvriks langenu pangakonto tühjendamise. Sellega ei pruugi aga soovimatud tagajärjed eID omajale piirduda. Nimelt kasutavad petturid ohvri eID-d sageli ka temana esinedes krediitdilepingute sõlmimiseks. Kuigi mõlema juhtumi alguspunktiks on petturite kätte sattunud eID, alluvad need erinevale õiguslikule regulatsioonile. Raha ülekandmise korral arvelduskontolt ilma kontoomaniku nõusolekuta võib kontoomanikul teatud juhtudel olla õigus oma raha tagasi saada, tuginedes makseteenuse pakkuja vastutuse regulatsioonile võlaõigusseaduses<sup>6</sup> (VÕS).<sup>7</sup> Krediitdilepingu sõlmimisel eID-d kasutades kohalduvad aga üldised tsiviilõiguse põhimõtted ja eriregulatsiooni seadusandja kirjeldatud juhtumite puhuks ette näinud ei ole. Keskseks põhimõtteks on seejuures, et lepingust saavad tuleneda kohustused vaid selle pooltele (VÕS § 8).<sup>8</sup> Seega ongi käeoleva artikli keskseks küsimuseks, kas ja kuivõrd peaksid petturi tehtud tehingu tagajärjed jääma eID omaja kanda.

## 2. Tõendamiskoormuse jagunemine krediidiandja ja eID omaja vahel

### 2.1. eID omaja tõendamiskoormus Riigikohtu praktikas

Võõra eID kasutamist tarbijakrediitdilepingu sõlmimiseks puudutavaid lahendeid on Riigikohtu tsiviilkolleegium teinud kaks. Esimese, 2019. aasta lahendi puhul esitas krediidiandja eID omaja vastu tarbijakrediitdilepingust tulenevate nõuete väljamõistmiseks hagi. Lepingu sõlmimiseks krediidiandja e-poes oli kasutatud isiku ID-kaarti ning sellele tuginedes leidis krediidiandja, et on sõlmitud kehtiv järeelmaksuga müügileping tema ja ID-kaardi omaja vahel. Kuna ID-kaardi omaja ei olnud oma lepingulisi kohustusi osaliselt täitnud, ütles krediidiandja lepingu üles ning nõudis ID-kaardi omajalt kauba kogumaksumuse jäägi, intresside ja viiviste tasumist.<sup>9</sup> ID-kaardi omaja seevastu leidis, et tema ei ole krediitdilepingu pooleks, sest ta ei ole vastavat lepingut sõlminud, vaid seda on teinud kolmas isik, kasutades ID-kaardi omaja ID-kaarti.<sup>10</sup>

Kõigepealt on Riigikohus seda asja lahendades märkinud, et kui isiku nimel tehakse tahteavaldus tema ID-kaarti ja PIN-koode kasutades, tuleb eeldada, et tahteavalduse on andnud ID-kaardi omaja. Vastupidise tõendamise koormus on isikul, kelle nimel on ID-kaarti kasutades vastav tahteavaldus tehtud.<sup>11</sup> Näiteks võib isik, näitamaks, et tema ei ole kõnealust lepingut sõlminud, tõendada, et tema eID koos PIN-koodidega läksid tema valdusest välja tema süüta ja tema tahte vastaselt.<sup>12</sup> Edasi on Riigikohus asunud seisukohale, et oma ID-kaardi ja PIN-koodide vabatahtlikult kolmandale isikule üleandmist võiks teatud juhtudel käsitada kolmandale isikule üldvolituse andmisena<sup>13</sup> ning kui konkreetse kaasuse asjaolud ei võimalda volituse andmist tuvastada, siis võib analoogiat kasutades kohalduda näivusvolituse regulatsioon (TsÜS<sup>14</sup> § 118 lg 2 teine alternatiiv).<sup>15</sup>

Seega, kui eID omaja väidab, et tema ei ole vaidlusalust lepingut sõlminud, peab ta kõigepealt tõendama, et lepingu on allkirjastanud kolmas isik tema eID-d kasutades. Kui see pole võimalik, tuleb Riigikohtu seisukoha kohaselt lugeda sõlmitud krediitdilepingu pooleks eID omaja. Samas ka juhul, kui eID omaja suudab tõendada eID kasutamist lepingu sõlmimiseks kolmanda isiku poolt, võib siiski olla tegemist näivusvolituse andmise olukorraga.

Arvutivõrgus: <https://www.jus.uio.no/ifp/forskning/prosjekter/sodi/publikasjoner/rapporter-mv/sodi-rapport-1-2022.pdf> (16.09.2024).

<sup>6</sup> RT I 2001, 81, 487; RT I, 04.07.2024, 2.

<sup>7</sup> VÕS § 733<sup>2</sup> jj.

<sup>8</sup> RKTko 07.06.2011, 3-2-1-44-11, p 27.

<sup>9</sup> RKTko 16.12.2019, 2-16-124450, p 1.

<sup>10</sup> Samas, p 2.

<sup>11</sup> Samas, p 22.

<sup>12</sup> Samas, p 22.

<sup>13</sup> Samas, p 23.

<sup>14</sup> Tsiviilseadustiku üldosa seadus. – RT I 2002, 35, 216; RT I, 06.07.2023, 6.

<sup>15</sup> RKTko 16.12.2019, 2-16-124450, p 24. Näivusvolituse kohta lähemalt vt P. Kalamees, T. Uusen-Nacke. Eneselegi ootamatult tehingupartneriks. Kommentaar Riigikohtu 16. veebruari 2022. a otsusele asjas 2-18-8699 ja 16. detsembri 2019. a otsusele asjas 2-16-124450. – *Juridica* 2023/7, lk 527–536.

Ka oma 2024. aasta suvises lahendis on Riigikohus samadele seisukohadele jäänud ning leidnud, et eID omaja peab tõendama, et tema ise ei ole teinud lepingu sõlmimiseks tahteavaldust ning temalt on eID kasutamiseks vajalikud koodid välja petetud.<sup>\*16</sup> Selle kaasuse asjaolud olid küll eelnevast mõnevõrra erinevad. Nimelt oli seekord eID omaja väidetavalt oma ID-kaardi ja Smart-ID andmed ning koodid koos temast tehtud fotoga edastanud isikule, kes esitles end politseiametnikuna. eID omaja, olles jäänud kolmandat isikut uskuma, edastas talle soovitud andmed.<sup>\*17</sup> Selles olukorras on Riigikohtu tsiviilkolleegium märkinud, et kui eID omajalt on eID kasutamiseks vajalikud koodid välja petetud, ei ole tegemist olukorraga, kus koodid on vabatahtlikult kolmandale isikule tehingute tegemiseks üle antud. Seetõttu puudub kirjeldatud juhul eID omajal ka tahe koodide edastamisega tehingute tegemiseks volitus anda.<sup>\*18</sup>

Sisuliselt tähendab eelnev, et eID omaja peab esitama teavet, mis võimaldaks kindlaks teha lepingu allkirjastamise kolmanda isiku poolt.<sup>\*19</sup> Selliseid fakte on aga eID omajal sageli äärmiselt keeruline kohtu ette tuua. Riigikohus seoses võõra eID kasutamisega tõendamisküsimusi sisuliselt analüüsinud ei ole. Küll aga on alamate astmete kohtute praktikast näha tendents, et eID väärkasutust on võimalik reeglina tõendada vaid kriminaalasja raames leitud tõenditele tuginedes.<sup>\*20</sup> Muul moel ei ole eID omajatel oma tõendamiskoormust üldiselt täita õnnestunud.<sup>\*21</sup> eID omajal on aga kriminaalmenetluse kaudu tõendite hankimine sageli raskendatud. Esiteks ei pruugi eID omaja kohe arugi saada, et on pettuse ohvriks langenud<sup>\*22</sup>, ega mõista vajadust politsei poole pöörduda või ise tõendeid koguma hakata (nt kuvatõmmiste tegemine saadetud sõnumitest, kirjavahetuse salvestamine jne). Kui vastav pöördumine teha hiljem, on omakorda jällegi uurimisorganitel sedavõrd keerulisem konkreetse juhtumi asjaolusid kindlaks teha. Ka juhul, kui kohe pettusele reageerida, ei pruugi see endaga kaasa tuua uurimise alustamist või edukat lõpuleviimist. Ka Eesti politsei mõnab, et petturite tabamine on keeruline protsess, mis ei pruugi õnnestuda.<sup>\*23</sup>

Kirjeldatud moel tõendamiskoormuse jaotumine eID omaja ja lepingu teise poole vahel toob kaasa selle, et eID omajad ei pruugi olla motiveeritud lepingu kehtivust vaidlustama, sest kohtute poolt oodatavate tõendite hankimine käib neile lihtsalt üle jõu. Olukorras, kus kohtumenetluse edulootus ei ole suur, riskivad eID omajad lisaks ka kohtus käimise kulude tasumisega. Sel moel jääb sageli eID omaja kanda lepinguline kohustus maksta krediidiandjale tagasi raha, mida eID omaja pole soovinud saada ja mis tihti ka tema kontole jõudnud pole.

## 2.2. Tõendamiskoormuse jaotus eID omaja ja krediidiandja vahel tsiviilkohtumenetluse seadustikust lähtuvalt

Kui eID omaja väidab, et krediidilepingu on sõlminud keegi kolmas temana esinedes, vaidlustab ta sisuliselt dokumendi (krediidilepingu) ehtsuse. Paraku pole Riigikohus eespool kirjeldatud lahendite puhul dokumendi ehtsuse vaidlustamise reeglitele tähelepanu pööranud ning on lähtunud TsMS §-s 230 sätestatud üldisest tõendamiskoormuse jaotusest. Situatsioon iseenesest on väga sarnane sellega, kui isiku omakäeline allkiri oleks lepingul ning isik väidaks, et tegemist on võltsinguga.

Selliseid olukordi reguleerib tsiviilkohtumenetluse seadustiku<sup>\*24</sup> (TsMS) § 277 lõige 1, mis näeb ette, et dokumendi ehtsuse vaidlustamiseks peab menetlusosaline dokumendi võltsituse põhistama. Omakäelise

<sup>16</sup> RKTkm 12.06.2024, 2-23-11584, p 10.

<sup>17</sup> Samas, p 4.

<sup>18</sup> Samas, p 11.

<sup>19</sup> Tsiviilkohtumenetluse seadustik I. Kommenteeritud väljaanne. V. Kõve, I. Järvekül, J. Ots, M. Torga (koost.). Juura 2017, § 229 komm. 1 p a (A. Kangur).

<sup>20</sup> Vt nt Harju MKo 08.10.2021, 2-21-100379; Harju MKo 25.02.2019, 2-18-104244; Harju MKo 26.01.2024, 2-23-126678.

<sup>21</sup> Vt nt Harju MKo 30.11.2021, 2-18-113623, kus eID omaja on üritanud tõendada, et tema ei ole lepingut digitaalselt allkirjastanud, esitades kohtule oma uksekaardi logid, veebiväljaande logi, kirjavahetuse, teekonna kuvatõmmised jne.

<sup>22</sup> Vt nt Harju MKo 26.01.2024, 2-23-126678.

<sup>23</sup> Kurjategijad petsid Eesti inimestelt välja vähemalt 8,3 miljonit eurot. Politsei- ja Piirivalveamet, 16.01.2024. Arvutivõrgus: <https://www.politsei.ee/et/uudised/kurjategijad-petsid-eesti-inimestelt-vaelja-vaehemalt-8-3-miljonit-eurot-11725> (25.09.2024); S. Rajamäe. Politsei näeb kurja vaeva petturite tabamisega. Varastatud raha tagasi saamine on keeruline protsess. – Delfi Ärileht, 30.08.2021. Arvutivõrgus: <https://arileht.delfi.ee/artikkel/94447709/politsei-naeb-kurja-vaeva-petturite-tabamisega-varastatud-raha-tagasi-saamine-on-keeruline-protsess> (25.09.2024).

<sup>24</sup> RT I 2005, 26, 197; RT I, 22.03.2024, 1.

allkirja puhul on Riigikohtu praktika kohaselt põhistamiseks piisav, kui dokumendile väidetavalt alla kirjutatud isik kohtus väidab, et tema dokumendile alla kirjutatud ei ole.<sup>\*25</sup> Digitaalallkirjaga varustatud elektroonilise dokumendi ehtsuse vaidlustamine on samuti võimalik, põhistades seejuures asjaolusid, mille põhjal võib eeldada, et dokumenti ei ole koostanud digitaalallkirja omaja (TsMS § 277 lg 3). Põhistamisega peab isik looma olukorra, kus tema esitatud asjaolude valguses on kohtuniku jaoks esitatud väide pigem ülekaalukalt tõene kui vale.<sup>\*26</sup> Ehk digitaalallkirjaga varustatud dokumendi ehtsuse vaidlustamiseks peab dokumendi väidetav allkirjastaja looma olukorra, kus tema väide dokumendi võltsituse kohta on kohtuniku jaoks pigem ülekaaluka tõenäosusega tõene. Omaette küsimuseks on, kas omakäelise allkirja ehtsuse vaidlustamise puhul peaks põhistamiseks piisama vaid isiku väitest, et tegemist ei ole tema allkirjaga. Ilmselt ei tohiks siiski pelgalt isiku vastav väide panna kohut uskuma, et tegemist on ülekaalukalt tõenäoliselt õige väitega. Igal juhul on seadusandja dokumendi ehtsuse vaidlustamiseks ette näinud tavapärases (TsMS § 230) võrreldes madalama tõendamisstandardi – põhistamisega ei pea saavutama kohtu säärast veendumuse määra nagu tavapärase tõendamise puhul.<sup>\*27</sup>

TsMS-s ei täpsusta ja ka kohtupraktikast ei selgu, millised peaksid olema need asjaolud, mille põhjal võib järeldada, et dokumendi on digiallkirjaga allkirjastanud kolmas isik ja mitte digiallkirja omaja. Õiguskirjanduses leitakse, et dokumendi allkirjastamist võõra digiallkirjaga on võimalik põhistada näiteks juhul, kui isik on oma ID-kaardi ja digiallkirjastamiseks vajaliku autentimiskoodi jätnud lohakile või andnud need teisele isikule või on autentimisvahend ja ID-kaart temalt varastatud.<sup>\*28</sup> Ilmselt ei saa siiski asuda seisukohale, et pelgalt eID ja selle kasutamiseks vajalike koodide lohakile jätmine (isegi, kui kohut suudetakse veenda, et selline tegevus on aset leidnud) on piisavaks asjaoluks, mis võimaldaks põhistada digiallkirja andmist teise isiku poolt. Kui ID-kaarti, Mobiil-ID-d või Smart-ID-d on hoitud lohakalt, siis ei ole selge, kas tehingu tegemise hetkel oli eID selle omaja või kellegi teise valduses. Põhistamiseks, et lepingu on allkirjastanud keegi muu kui digiallkirja omaja, tuleb viimasel tuua kohtu ette muid täiendavaid asjaolusid, mis kohut kolmanda isiku poolt lepingu allkirjastamises veenaksid. Näiteks võiks kohtu ette tuua asjaolusid, mis näitavad, et eID omajal ei olnud võimalik konkreetset lepingut sõlmida (nt viibis ta haiglas ning ei omanud ligipääsu nutiseadmetele, oli parasjagu lennukis, kulges punktist A punkti B autoroolis vms). Ka eID andmine teisele isikule ei tohiks kohut tingimata veenda, et krediitdilepingu on allkirjastanud keegi muu kui eID omaja. Isegi juhul, kui sellise sündmuse asetleidmine õnnestub kohtu jaoks usutavaks teha, ei saa selle pinnalt järeldada, et tegemist on võltsitud digiallkirjaga. Pigem kerkib vabatahtlikult eID teisele isikule üleandmise korral küsimus, kas ehk võib olla tegemist volituse andmisega sellele isikule.<sup>\*29</sup>

Seevastu olukorras, kus eID omaja suudab põhistada, et ta on langenud petturite ohvriks ning seetõttu on tema eID kasutamine saanud võimalikuks teise isiku poolt, on see piisav tõendamiskoormuse asetamiseks krediitandjale. Näiteks võib pettuse ohvriks langenu esitada kohtule talle saadetud peturkirja või -sõnumi, mis on saadetud vahetult enne eID-d kasutades krediitdilepingu sõlmimist; lisada sinna juurde politseile esitatud avalduse; logifaile tema arvutis/telefonis toimunu kohta; põhjendada, miks ei oleks krediidi võtmine olnud kuidagi tema huvides jne. Nimetatud asjaolude kohtu ette toomine on eID omaja jaoks märkimisväärselt kergem kui TsMS § 230 lõike 1 kohase tõendamiskoormuse kandmine. Seevastu on aga kriteerium, et kohtul peab tekkima põhjendatud kahtlus allkirja ehtsuse suhtes, piisav, et ära hoida enamik olukordi, kus eID omajad võiksid proovida madalamat tõendamisstandardit ära kasutada.

Tõendamiskoormust on varem samamoodi jaotanud ka Riigikohus oma lahendis 2016. aastast.<sup>\*30</sup> Selles kaasuses oli tegemist omakäelist allkirja kandva võlatunnistuse ehtsuse vaidlustamisega ning peamiseks vaidlusaluseks küsimuseks oli, kes peab tõendama, et võlakiri ja sellel olev allkiri on ehtsad.<sup>\*31</sup> Mõlemas madalama astme lahendis olid kohtud leidnud, et väidetavalt võlakirja allkirjastanud isik peab tõendama,

<sup>25</sup> RKTko 23.09.2015, 3-2-1-79-15, p 10; RKTko 14.09.2016, 3-2-1-63-16, p 10; RKTko 11.12.2019, 2-17-1722, p 10.2.

<sup>26</sup> Tsviilkohutemenetluse seadustik I. Kommenteeritud väljaanne (viide 19), § 235 komm. 3.2 (M. Tasa).

<sup>27</sup> Samas.

<sup>28</sup> Samas, § 277 komm. 3.8.2 (A. Kangur).

<sup>29</sup> Vt käesoleva artikli p 2.1.

<sup>30</sup> RKTko 23.09.2015, 3-2-1-79-15, p 10; RKTko 14.09.2016, 3-2-1-63-16. Sama põhimõtet on Riigikohus korranud ka oma 11.12.2019 otsuses 2-17-1722.

<sup>31</sup> RKTko 23.09.2015, 3-2-1-79-15, p 10; RKTko 14.09.2016, 3-2-1-63-16, p 9.

et tegemist ei ole tema allkirjaga.<sup>\*32</sup> Riigikohus tõendamiskoormuse sellise jaotamisega ei nõustunud ning märkis, et tsiviilkohtumenetluse üldise põhimõtte kohaselt peab võlausaldaja tõendama, et võlgnik on andnud kehtiva võlatunnistuse. Kui väidetavalt võlakirja allkirjastanud isik esitab vastuväite ja vaidlustab allkirja ehtsuse (TsMS § 277), peab võlausaldaja kehtiva võlakirja olemasolu tõendama.<sup>\*33</sup> Tegemist on küll omakäelist allkirja kandva dokumendi ehtsuse vaidlustamisega, kuid sama põhimõtet tuleks kohaldada ka digitaalselt allkirjastatud dokumentide ehtsuse vaidlustamisel. Kirjeldatud viisil tõendamiskoormuse jagamisel eID omaja ja krediidiandja vahel koheldaks tsiviilkohtumenetluses sarnaselt isikuid, kes vaidlustavad omakäelise allkirja ehtsuse ja digiallkirja ehtsuse.

### 2.3. Digiallkirja tõendusjõud Euroopa Kohtu otsuses asjas C-466/22

Küsimust, millist tõendusjõudu omab kvalifitseeritud digitaalne allkiri võrreldes omakäelise allkirjaga, on analüüsinud ka Euroopa Kohus. Kaasuses C-466/22<sup>\*34</sup> oli küsimuseks, kas eIDAS-määruse<sup>\*35</sup> artiklit 25 tuleb tõlgendada nii, et kvalifitseeritud e-allkirja olemasolu ja väidetavat autorsust tuleb pidada vaieldamatult tõendatuks, kui kvalifitseeritud e-allkirjale esitatavad nõuded on täidetud, või on e-allkirjal tõendusjõud vaid raamides, mida näevad ette asjakohased riigisisised normid omakäelise allkirja puhul.<sup>\*36</sup> Nii ID-kaarti, Mobiil-ID-d kui ka Smart-ID-d kasutades antavad digiallkirjad on kvalifitseeritud e-allkirjad eIDAS-määruse artikli 3 punkti 12 tähenduses.<sup>\*37</sup> Ehk siis tegeles Euroopa Kohus selles asjas analüüsimisega, kas digitaalallkirjal on absoluutne tõendusjõud või kehtivad ka sellise allkirja suhtes samad reeglid nagu omakäelise allkirjagi puhul.

eIDAS-määruse artikli 25 lõige 1 näeb ette, et e-allkirja ei tunnista õiguslikult kehtetuks ega kohtumenetluses tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele. Kõnealuses otsuses leidis Euroopa Kohus, et selle sätte mõtteks ei ole kehtestada liikmesriikide kohtutele keeldu tunnista digitaalallkiri kehtetuks, vaid selles kajastub üldpõhimõte, mis ei luba kohtutel keelduda digitaalallkirja õigusliku toime ja tõendusjõu tunnistamisest üksnes põhjusel, et need allkirjad on elektroonilised.<sup>\*38</sup> Seega nentis Euroopa Kohus, et digiallkirja kehtivuse vaidlustamine ja kehtetuse tuvastamine liikmesriikide kohtute poolt on lubatud.

Edasi märkis Euroopa Kohus, et kvalifitseeritud e-allkirjade õiguslik toime peaks olema kindlaks määratud riigisiseses õiguses, tingimusel et järgitakse kvalifitseeritud e-allkirja samastamist omakäelise allkirjaga, nagu on ette nähtud eIDAS-määruse artikli 25 lõikes 2.<sup>\*39</sup> Seejärel on kõnealuses lahendis eraldi rõhutatud, et puudub alus käsitleda kvalifitseeritud e-allkirja soodsamalt omakäelisest allkirjast<sup>\*40</sup> ning kvalifitseeritud e-allkirja tõendusjõu kahtluse alla seadmine peab olema riigisisese õiguse kohaselt võimalik samaväärselt omakäelise allkirja ehtsuse vaidlustamisega.<sup>\*41</sup> Seejuures peab olema riigisiseses õiguses ette nähtud identne menetlus mõlemat liiki allkirjade ehtsuse vaidlustamiseks.<sup>\*42</sup> Lõppkokkuvõttes asus Euroopa Kohus seisukohale, et eIDAS-määruse artiklit 25 tuleb tõlgendada nii, et kvalifitseeritud e-allkirjal on omakäelise allkirjaga samaväärne tõendusjõud vastavalt konkreetse liikmesriigi seadustele.<sup>\*43</sup> Ehk vaidlustada saab nii digiallkirja kui ka omakäelise allkirja ehtsust ning vaidlustamise võimalus peab mõlema allkirja puhul olema samasugune.

<sup>32</sup> RKTko 23.09.2015, 3-2-1-79-15, p 10; RKTko 14.09.2016, 3-2-1-63-16, p 10.

<sup>33</sup> Samas, samuti RKTko 11.12.2019, 2-17-1722, p 10.1.

<sup>34</sup> EKo C-466/22, *V.B. Trade OOD vs. Direktor na Direktsia 'Obzhalvane i danachno-osiguritelna praktika' – Veliko Tarnovo*.

<sup>35</sup> Euroopa Parlamendi ja nõukogu määrus (EL) 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldus-teenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257, 28.08.2014, lk 73–114.

<sup>36</sup> EKo C-466/22, p 32.

<sup>37</sup> L. Kask. E-Eestist e-Euroopasse: elektrooniline allkiri riigisiseses ja piiriüleses suhtluses. – *Juridica* 2017/10, lk 678. Smart-ID kohta vt <https://www.smart-id.com/et/e-teenuste-pakkujale/smart-id-kui-qscd/> (08.10.2024).

<sup>38</sup> EKo C-466/22, p 34.

<sup>39</sup> Samas, p 36.

<sup>40</sup> Samas, p 37.

<sup>41</sup> Samas, p 38.

<sup>42</sup> Samas, p 39.

<sup>43</sup> Samas, p 40.



Eesti õigus lubab mõlemat liiki allkirja ehtsust vaidlustada TsMS § 277 kohaselt.<sup>44</sup> Sisuliselt erineb aga digiallkirja tõendamisväärtus omakäelise allkirja omast märgatavalt. Nagu eespool näidatud, on Riigikohus korduvalt tõendamiskoormuse allkirja ehtsuse vaidlustamisel jätnud eID omaja kanda<sup>45</sup> ehk isik, kes väidab, et tema pole konkreetset dokumenti digiallkirjastanud, peab tõendama, et allkirjastaks oli keegi teine. Seevastu omakäelise allkirja kohta sama väite esitamisel ei pea väidetav allkirja andja tõendama, et tegemist on kellegi teise antud allkirjaga, vaid piisab, kui ta põhistab kohtule allkirja võltsituse. Seejuures piisab põhistamiseks pelgalt väitest, et allkirja ei ole tema andnud.<sup>46</sup> Ilmselgelt ei oma Eesti praeguse kohtupraktika kohaselt omakäeline allkiri ja digiallkiri samaväärset tõendusjõudu. Digiallkirja ehtsuses on kohtud kahtlemata rohkem veendunud ja seega tuleb asuda seisukohale, et Eesti kohtupraktika ei ole Euroopa Kohtu vastava praktikaga kooskõlas.

Kirjeldatud moel eri liiki allkirjadele erineva tõendamisväärtuse omistamist võimaldaks vältida nii eID vahendusel antud allkirja kui ka omakäelise allkirja ehtsuse vaidlustamisel TsMS §-s 277 sätestatud reeglite ühetaoline kohaldamine. Mõlemat liiki allkirja puhul piisaks selle ehtsuse vaidlustamiseks allkirja andja poolt kohtule asjaolude põhistamisest, mis viitavad sellele, et allkirja on andnud keegi teine.

Päris probleemitu ei pruugi aga olla Euroopa Kohtu otsuse valguses ka see lahendus. Nagu näha, siis leiab Euroopa Kohus, et nii digiallkirjal kui ka omakäelisel allkirjal peab olema täpselt samasugune tõendamisväärtus ning nende ehtsuse vaidlustamise menetluski peaks olema identne. Kui digitaalallkirjaga dokumendi puhul näeb TsMS § 277 lõige 3 ette konkreetset reeglid, milliseid asjaolusid tuleb põhistada, et saaks kahtluse alla seada digitaalallkirja andmist eID omaja poolt, siis omakäelise allkirja kohta vastavad juhtnõõrid seaduses puuduvad. Kuigi seaduse tekst võimaldab järeldada, et ka omakäelise allkirja ehtsuse vaidlustamise puhul võiks lähtuda samadest kriteeriumitest, siis kohtupraktikas on lähtutud põhistamisel palju madalamast kriteeriumist – pelgalt väidetava allkirjastaja väitest, et allkirja pole andnud tema.<sup>47</sup> Seega, isegi kui kohaldada nii digitaalallkirja kui ka omakäelise allkirja ehtsuse vaidlustamisele TsMS §-s 277 sisalduvaid reegleid, ei pruugi kumbagi liiki allkirja ehtsuse vaidlustamise protsess kohtumenetluses olla väidetava allkirjastaja jaoks samasugune.

Eesti kohtupraktika aitaks Euroopa Kohtu vastava praktikaga kooskõlla viia see, kui ka omakäelise allkirja ehtsuse vaidlustaja peaks kandma ulatuslikumat põhistamiskoormust kui vaid vastava väite esitamine menetluses. Teiseks alternatiiviks kaht liiki allkirjadele samaväärse tõendamisväärtuse andmiseks oleks langetada digitaalallkirja ehtsuse vaidlustamisel põhistamisele kehtestatud standardit, kuid see seaks väga tugeva kahtluse alla käibekindluse olukorras, kus valdav osa tehingutest tänasel päeval tehakse eID-d kasutades. Seega oleks mõistlik TsMS § 277 lõiget 1 muuta nii, et ka omakäelise allkirjaga varustatud dokumendi ehtsust oleks võimalik vaidlustada üksnes selliste asjaolude põhistamisega, mille põhjal võib eeldada, et dokumendil olevat allkirja ei ole andnud selleks õigust omav isik. Näiteks saaks omakäelise allkirja andmist vaidlustav isik selgitada, et allkirja andmine ei oleks olnud kooskõlas tema huvidega või kui on teada konkreetse dokumendi allkirjastamise aeg, siis ka seda, et ta ei viibinud sel ajal dokumendi allkirjastamist võimaldavas asukohas vms.

### **3. Tõendamiskoormuse jaotus makseteenuste puhul, kui makseinstrumendina on kasutatud teise isiku eID-d**

#### **3.1. Autoriseerimata makse**

Nii nagu petturid kasutavad eID andmeid krediitdilepingute sõlmimiseks eID omajana esinedes, kasutavad nad samu andmeid ka eID omaja pangakontolt ülekannete tegemiseks. Petturid võivad end näiteks esitleda pangaametniku või politseitöötajana, kirjeldada eID omajat väidetavalt varitsevat ohtu ning paluda eID omajal edastada oma PIN-koodid petturitele või lasta vajalikud koodid ise spetsiaalselt pettuse tarvis

<sup>44</sup> Vt lähemalt käesoleva artikli p 2.2.

<sup>45</sup> Vt p 2.1.

<sup>46</sup> Vt p 2.2.

<sup>47</sup> Vt p 2.2.

asjakohasele veebileheküljele sisestada. Selle kõige tulemuseks on, et eID omaja pangakontolt tehakse ülekandeid, mille tegemist ta teadlik ei ole olnud ja milleks ta pole oma teadlikku nõusolekut andnud. Nagu käesoleva artikli sissejuhatuses mainitud, kohalduvad sellisele juhule makseteenuse kohta käivad VÕS-i sätted. Kuna nii krediidilepingute allkirjastamiseks kui ka makseteenuse kasutamiseks antava nõusoleku edastamiseks kasutatakse sageli sama vahendit (ID-kaart, Mobiil-ID, Smart-ID), peaks mõlemal juhul sarnaselt jaotuma ka eID omaja tõendamiskoormus, näitamaks, et tema pole konkreetse tehingu tegemiseks tahteavaldust teinud.

VÕS § 724<sup>1</sup> lõike 1 kohaselt on maksetehing maksjale siduv, kui ta on selle täitmiseks andnud nõusoleku (maks autoriseerinud). Maksja on VÕS § 709 lõike 5 kohaselt isik, kellele on avatud maksekonto ja kes annab maksejuhise maksekonto debiteerimiseks, siinse artikli kontekstis nimetagem seda isikut jätkuvalt eID omajaks. eID kasutamise kontekstis tähendab eelnev, et maksetehing on siduv siis, kui eID omaja on andnud maksetehingu täitmiseks nõusoleku. Vastava nõusoleku puudumisel on tegemist autoriseerimata maksega ja makseteenuse pakkuja on kohustatud tagastama maksesumma eID omajale viivitamata (VÕS § 733<sup>2</sup> lg 2). Autoriseerimise viisis ja korras saavad makseteenuse pakkuja ja maksja kokku leppida (VÕS § 724<sup>1</sup> lg 2), kuid seda, mida tuleb mõista „nõusolekuna“, VÕS ei täpsusta. Samuti ei ole nõusoleku olemust põhjalikumalt defineeritud ka VÕS-i vastava regulatsiooni aluseks olevas Euroopa Parlamendi ja nõukogu direktiivis 2015/2366<sup>\*48</sup> (edaspidi makseteenuste direktiiv).

Võlaõigusseaduse kommentaari kohaselt käsitatakse nõusolekuna tegevust või toimingut, millega maksja annab makseteenuse pakkujale maksejuhise maksetehingu tegemiseks ja samal ajal kinnitab maksejuhise oma allkirja või makseinstrumenti kasutamiseks ettenähtud isikustatud turvaelemendiga.<sup>\*49</sup> Sellest definitsioonist lähtuvalt võiks eespool kirjeldatud, pettuse tagajärjel tehtud maksetehingud lugeda autoriseerituks. Pettuse tulemusena jõuavad makseteenuse pakkujani nii väidetav eID omaja soov teha maksetehing kui ka selle tehingu kinnitamiseks vajalik digiallkiri. Sellise lähenemise puhul jääb aga tähelepanuta asjaolu, et tegelikult ei ole eID omajal olnud mingit soovi konkreetset sellise maksetehingu tegemiseks (nt väljamakse tegemiseks petturi kontole). Nõusolek on oma olemuselt tahteavaldus (TsÜS § 67 lg 1), sest selle kaudu väljendatakse õigusliku tagajärje kaasatoomisele suunatud tahet.<sup>\*50</sup> Tahteavaldusega väljendab isik tahet olla konkreetse õigusliku tagajärjega seotud<sup>\*51</sup> ehk siinse artikli kontekstis peaks eID omaja väljendama nõusolekuga oma soovi teha kindel maksetehing. Nagu on märgitud ka tsiviilseadustiku üldosa seaduse kommentaaris, siis tahteavalduse kaudu muudetakse isiku tahe talle õiguslikult siduvaks ning tahteavaldus on tehingu tuumaks.<sup>\*52</sup> Olukorras, kus eID omajal puudub igasugune soov maksetehingu tegemiseks, tuleb seega asuda seisukohale, et nõusolekut VÕS § 724<sup>1</sup> lõike 1 mõttes maksetehingu tegemiseks antud ei ole ja seega pole maksetehing ka maksjale siduv. Eesti kohtupraktikas pole paraku senini nõusoleku mõiste sisustamisega makseteenuste kontekstis tegeletud.

Nõusoleku mõiste makseteenuste direktiivi artikli 64 lõikes 1 (mis on VÕS § 724<sup>1</sup> lg 1 aluseks) viitab sellele, et eID kasutaja peab nõustuma tehingu tegemisega, milleks ta oma nõusolekut väljendab.<sup>\*53</sup> Otsustav ei saa seejuures olla, et sisuliselt vale sisuga „nõusoleku“ andmiseks on kasutatud korrektselt makseinstrumenti.<sup>\*54</sup> Teistsugune mõiste „nõusolek“ sisustamine muudaks sisutühjaks ka tõendamiskoormuse jaotumise reeglid makseteenuste direktiivi artikli 72 lõikes 2.

<sup>48</sup> Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta. – ELT L 337, 23.12.2015, lk 35–127.

<sup>49</sup> Võlaõigusseadus IV. Kommenteeritud väljaanne. P. Varul, I. Kull, V. Kõve, M. Käerdi, K. Sein (koost.). Juura 2020, § 724<sup>1</sup> komm. 3.1 (M. Ulp).

<sup>50</sup> RKTkm 02.12.2020, 2-18-9475, p 13.1.

<sup>51</sup> P. Varul, I. Kull, V. Kõve, M. Käerdi, K. Saare, K. Sein. Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne. Juura 2023, § 67 komm. 3.1.2 (K. Sein, P. Varul).

<sup>52</sup> Samas.

<sup>53</sup> M. R. Guimaraes, R. Steennot. Allocation of Liability in Case of Payment Fraud: Who Bears the Risk of Innovation? A Comparison of Belgian and Portuguese Law in the Context of PSD2. – European Review of Private Law 2022 (1), lk 38.

<sup>54</sup> Samas, lk 39.

### 3.2. Makseteenuse pakkuja tõendamiskoormus

Makseteenuste direktiivi artikli 72 lõike 2 kohaselt, kui maksja väidab, et ta ei ole täidetud maksetehingut autoriseerinud, ei piisa üksnes asjaolust, et makseteenuse pakkuja on dokumenteerinud makseinstrumendi kasutamise, et tõendada maksetehingu autoriseerimist. Tõendamiskoormus autoriseerimata maksete puhul on seega asetatud makseteenuse pakkujale. Ka VÕS § 733<sup>4</sup> lõige 2 näeb ette, et kui on vaieldav, kas makseinstrumendi abil tehtud maksetehing on autoriseeritud, ei piisa maksetehingu autoriseerituse tõendamiseks sellest, et makseteenuse pakkuja on eID kasutamise dokumenteerinud. Ehk juhul, kui on kaheldav, kas eID omaja on konkreetse maksetehingu tegemiseks nõusoleku andnud, peab makseteenuse pakkuja esitama täiendavaid tõendeid, näitamaks, et vastav nõusolek on antud.

Omaette küsimuseks on, kui põhjalikult peab eID omaja sellisel juhul oma väidet põhjendama. Ilmselt ei saa tõendamiskoormuse makseteenuse pakkujale panemiseks piisata pelgalt eID omaja väitest. Sellisel juhul oleks eID kasutajatel võimalik vaidlustada põhimõtteliselt iga maksetehingut ning makseteenuste pakkujad peaksid kulutama suurel hulgal ajalist ja rahalist ressursi vastavate väidete ümberlukkamiseks. Küll aga oleks asjakohane tõendamiskoormuse makseteenuse pakkujale asetamine siis, kui eID omaja suudab näidata, et suure tõenäosusega ei olnud tehingule nõusolekut andnud tema ise.<sup>55</sup> Seejuures oleks näiteks asjakohane näidata, et eID omaja on saanud pettusele viitavaid sõnumeid ning ilmselt ei oleks vastava tehingu tegemine tema huvides.

Milliseid tõendeid tehingu autoriseerituse kohta peaks makseteenuse pakkuja esitama, seadus ei reguleeri. Eesti õiguskirjanduses on asutud seisukohale, et makseteenuse pakkuja peaks kirjeldatud tõendamiskoormuse kandmiseks näitama, et tehing on tehtud kliendi tugevat autoriseerimisvahendit kasutades või et klient on rikkunud tahtlikult või raske hooletuse tõttu makseinstrumendi väljastamise või kasutamise tingimust või makseinstrumenti on kasutatud pettuse teel.<sup>56</sup> Seega piisab selle seisukoha kohaselt makseteenuse pakkuja tõendamiskoormuse täitmiseks näitamisest, et ID-kaart, Mobiil-ID või Smart-ID ja nende kasutamiseks vajalikud koodid on väljastatud ja kuuluvad konkreetsele eID omajale ning et tehingu tegemise ajal oli eID kehtiv ja selle turvaelemendid vastasid makseteenuse pakkuja süsteemis olevatele. Edasi on võlaõigusseaduse kommentaarides märgitud, et kuna makseteenuse pakkujate infosüsteemid on sertifitseeritud ja auditeeritud, siis seetõttu on üldiselt tagatud ka vastavate süsteemilogide tõepärasus.<sup>57</sup> Kokkuvõtvalt ollakse Eesti õiguskirjanduses seega makseteenuste puhul seisukohal, et eID kasutamise korral piisab makseteenuse pakkujal tõendamiskoormuse kandmiseks näidata, et tehingu tegemiseks on kasutatud konkreetsele isikule väljastatud kehtivat eID-d.

Selle seisukohaga ei saa nõustuda, sest juba seaduse sõnastus viitab vastupidisele (VÕS § 733<sup>4</sup> lg 2). Kui lähtuda sellest, et tehingu tegemiseks nõusoleku andmiseks (ja selleks, et tegemist oleks autoriseeritud maksega) piisab vaid eID kasutamisest ning ka maksetehingu autoriseerituse tõendamiseks näitamisest, et maksetehingu tegemiseks on kasutatud eID-d, oleks sisuliselt pea võimatu olukord, kus maksetehing ei oleks autoriseeritud.<sup>58</sup> Selline lahendus ei sobiks aga kuidagi kokku makseteenuste direktiivi eesmärkidega riskide jaotamisel makseteenuste pakkujate ja maksjate vahel.

Nimelt, makseteenuste direktiivi artikli 73 lõike 1 kohaselt peab makseteenuse pakkuja autoriseerimata maksetehingu puhul maksjale autoriseerimata maksetehingu summa viivitamata tagasi maksma. Erandina ei pea makseteenuse pakkuja raha tagastama, kui tal on mõistlik põhjus kahtlustada pettust ja ta sellest ka asjakohast riigiasutust teavitab. Seega autoriseerimata makse korral tuleb üldreeglina makseteenuse pakkujal rahasumma maksjale viivitamatult tagasi kanda.<sup>59</sup> Erandi eelnevast näeb ette direktiivi artikli 74 lõige 1, mis paneb maksjale vastutuse maksetehingu summa 50 eurot ulatuses, kui kahju tekkis kaotatud või varastatud makseinstrumendi kasutamisest või makseinstrumendi väärkasutamisest. Samas lõikes on ette nähtud veel täiendavad erandid, millal maksja siiski ka 50 euro ulatuses toimunud maksetehinguga tekkinud kahju eest ei vastuta. Edasi näeb sama säte ette, et maksja kannab kogu autoriseerimata maksetehinguga seotud kahju, kui see on tekkinud maksja poolt toime pandud pettuse tõttu või kui makseteenuse

<sup>55</sup> Saksamaa kohta vt nt D. Linardatos. The Transposition of the PSD2: The Role of EBA and of the National Legislator in Germany. – The Transposition of PSD2 and Open Banking. E. Bani, V. De Stasio, A. Sciarrone Alibrandi (eds.). Bergamo University Press 2021, lk 129; M. R. Guimaraes, R. Steennot (viide 53), lk 39.

<sup>56</sup> Võlaõigusseadus IV. Kommenteeritud väljaanne (viide 49), § 733<sup>4</sup> komm 3.2 (M. Ulp).

<sup>57</sup> Samas.

<sup>58</sup> M. R. Guimaraes, R. Steennot (viide 53), lk 39.

<sup>59</sup> Samas, lk 46.



kasutaja ei ole näiteks makseinstrumenti hoidnud hoolikalt või teavitanud makseteenuse pakkujat õigeaegselt makseinstrumendi kadumisest, varastamisest, väärkasutamisest või autoriseerimata kasutamisest kavatselt või hooletult. Seega lähtub makseteenuste direktiiv loogikast, et tehing võib olla autoriseerimata juhul, kui maksja ei ole andnud konkreetse tehingu tegemiseks teadvalt oma nõusolekut, kuid maksjapoolse vastutuse määr sõltub sellest, kuivõrd hoolikalt ta on oma makseinstrumendiga ümberkäimise kohustust täitnud.<sup>\*60</sup> Selle põhimõtte rõhutamiseks on ka Euroopa Parlament uut makseteenuste määrust ette valmistades teinud ettepaneku lisada määrusse põhjenduspunkt, mis selgitaks, et nõusolek maksetehingu tegemiseks peaks kajastama maksja teadlikku soovi teha konkreetne tehing konkreetsetel tingimustel ja eesmärgil.<sup>\*61</sup>

Kõike eelnevat arvestades tuleb asuda seisukohale, et ka Eesti õiguses tuleb lugeda autoriseerimata makseks makse, mis on küll tehniliselt veatult eID-d kasutades tehtud, kuid mille tegemiseks ei ole tulenevalt toimunud pettusest olnud maksja sisulist nõusolekut. Tõendamiskoormuse kandmine makseteenuse pakkuja puhul ei tohiks piirduda vaid näitamisega, et maksetehingu tegemiseks on korrektselt kasutatud maksja eID-d. Makseteenuse pakkujatel tuleks oma tõendamiskoormuse täitmiseks esile tuua täiendavaid asjaolusid, mis võimaldavad tõendada, et tehingu on teinud eID omaja ise vastavalt oma tegelikele veendumustele, mitte tegutsedes petturite loodud ekslikest asjaoludest lähtudes.

Kuna nii makseteenuste kasutamiseks kui ka krediitdilepingute sõlmimiseks kasutatakse eID-d ning tõendamiskoormuse kandmisega seonduvad küsimused on samad, ei tohiks erineda ka eID omaja sisuline tõendamiskoormus sõltuvalt sellest, kas eID-d kasutati pangaülekande tegemiseks või krediitdilepingu sõlmimiseks. Mõlemal juhul peaks põhjendatud kahtluse korral tahteavalduse andmise suhtes kehtiva tahteavalduse andmist eID omaja poolt tõendama kas krediidiandja või makseteenuse pakkuja.

## 4. Täiendavad argumendid, mida tõendamiskoormuse jagamisel krediidiandja ja eID omaja vahel arvestada

Digitaalalkkirja ehtsuse tõendamise koormuse asetamist krediidiandjale ei saa pidada liigselt koormavaks. Kui eID omajal on eespool märgitud põhjustel<sup>\*62</sup> keeruline hankida tõendeid, et ta on langenud petturite ohvriks, siis krediidiandja käsutuses on kahtlemata enam vahendeid, näitamaks, et lepingu on sõlminud ikkagi eID omaja. Nimetatud vahendid on mh rahalised, kuid krediidiandjate käsutuses on ka oskusteave, kuidas eID kasutamise puhul lepingu sõlmimiseks tõsta isikusamasuse kindlakstegemise taset senisest kõrgemale. Nii näiteks saab krediidiandja koguda infot, millisel IP-aadressilt on leping sõlmitud. Samuti ei ole välistatud, et tõendamiskoormuse kirjeldatud viisil jaotamise korral võtavad krediidiandjad kasutusele täiendavaid meetmeid, tegemaks kindlaks, kas lepingu allkirjastajaks on eID omaja. Näiteks saavad krediidiandjad saata täiendavaid SMS-e, e-kirju või helistada eID omanikule, kui laekub eID-d kasutades tema nimelt krediidi saamiseks taotlus<sup>\*63</sup> või kui soovitakse internetipangas muuta kontoomaniku kontaktandmeid või kui kontoomaniku tegevus seoses kontoga on märkimisväärselt erinev tavapärasest.<sup>\*64</sup> Tõendamiskoormuse krediidiandja kanda jätmisel tuleb mh silmas pidada, et krediidiandjad on ulatuslikust digitaliseerimisest märkimisväärselt kasu saanud (tööprotsessid on kiirenenud, personalivajadus teatud tööloikudes väheneb jne) ning täiendava tulu suunamine oma tööprotsesside turvalisuse suurendamiseks on põhjendatud. Tehingute tegemise digitaliseerimisest tulenevaid õiguslikke riske ei tohiks jätta üksnes tarbijate kanda.<sup>\*65</sup>

<sup>60</sup> Samamoodi on makseteenuste direktiivi mõistetud ka Saksa õiguses, vt M. Casper, B. Reich. Haftung bei einem qualifizierten Phishing mit weiteren Elementen des Social Engineering. – Zeitschrift für Bankrecht und Bankwirtschaft 2023 (35) 3, lk 141.

<sup>61</sup> Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse makseteenuseid siseturul ning millega muudetakse määrust (EL) nr 1093/2010. COM(2023) 367 – 2023/0210(COD), põhjenduspunkt 79a.

<sup>62</sup> Vt käesoleva artikli p 2.1.

<sup>63</sup> Niimoodi käituvad mitmed Eesti pangad, kui isiku maksekaarti on kasutatud ebatavalisel viisil (nt välismaal).

<sup>64</sup> Nii näiteks on Norras pankadele ette nähtud vastav hea tava, vt Bransjenorm. Finans Norge, p 6. Arvutivõrgus: <https://www.finansnorge.no/siteassets/dokumenter/avtaler/bransjenorm-bankid.pdf> (06.11.2024).

<sup>65</sup> Vt ka M. R. Guimaraes, R. Steenot (viide 53), lk 71; M. E. Kjørven. Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe. – European Business Law Review 2020 (31) 1, lk 109.

Seega peaks tõendamiskoormuse jaotamisel eID omaja ja krediidiandja vahel lähtuma TsMS § 277 lõikes 3 sätestatud reeglist ning mitte jätma eID omajale kogu tõendamiskoormust selle näitamiseks, et tema ei ole kõnealust krediidilepingut sõlminud.

Lisaks eespool kirjeldatud raskustele eID omajate jaoks seoses tõendite hankimise kohatise võimatusega ning ilmselgelt väiksema digikirjaoskusega kui krediidiandjatel esineb ka muid asjaolusid, mis sellist tõendamiskoormuse jaotust toetavad. Ennekõike ei ole eID kasutajad ise ennast sellisesse silmast silma suhtlusest riskantsemasse olukorda asetanud. On tõsi, et ei ID-kaardi, Mobiil-ID ega ka Smart-ID kasutamine ei ole kohustuslik, samas on paljude teenuste kättesaadavus nii avalikus kui ka erasfääris ilma seda veebi vahendusel tegemata vähene. Nii näiteks on Eesti suuremad pangad viimastel aastatel sulgenud oma kontoreid väiksemates asulates<sup>66</sup>, samuti on käitunud postiteenuse pakkuja<sup>67</sup> ja ka riik ise.<sup>68</sup> Mõnede krediidiandjate pakutavaid teenuseid ei ole üldse võimalik mujal kui veebis kasutada<sup>69</sup> ning näiteks ka arsti konsultatsiooni või selleks vastuvõtutaja saamiseks on sageli kiirem või ka ainuvõimalik tee võtta arstiga ühendust läbi vastava e-pöördumiste keskkonna.<sup>70</sup> Seega on nii riik kui ka erasfäär asetanud eID kasutajad olukorda, kus nad on sunnitud kasutama eID-d koos kõigi selle kasutamisest tulenevate riskidega, mh ohuga sattuda pettuse ohvriks, mille tulemusena eID omaja nimel sõlmitakse krediidileping või tühjendatakse tema pangakonto.

## 5. Kokkuvõte

Kui krediidilepingu sõlmimiseks on kasutatud võõrast eID-d, lasub Riigikohtu praktika kohaselt tõendamiskoormus võõra eID kasutamise osas eID omajal. Seeläbi on pettuse ohvriks sattunud eID omajad asetatud olukorda, kus neil lasub ulatuslik tõendamiskoormus asjaolude suhtes, mille tõendamine ei pruugi olla nende võimuses. See omakorda vähendab eID omajate motivatsiooni oma õiguste kaitseks kohtusse pöörduda ning eID omajad võivad jääda vastutavateks tehingute tegemise eest, milleks nad oma taht väljendanud ei ole.

Kohasem oleks tõendamiskoormuse jaotamisele ka digiallkirja puhul kohaldada TsMS § 277 regulatsiooni ning sarnaselt omakäelise allkirja ehtsuse vaidlustamisega nõuda digitaalallkirja andnud isikult põhistamist, et tegemist ei ole tema antud allkirjaga. Seejuures peab Euroopa Kohtu otsuse kohaselt asjas C-466/22 digiallkirja ehtsuse vaidlustamise menetlus olema identne omakäelise allkirja vaidlustamise menetlusega. Eestis see praegu nii ei ole, sest omakäelise allkirja ehtsuse vaidlustamiseks piisab Riigikohtu praktika kohaselt vaid väidetavalt allkirja andnud isiku väitest, et tegemist ei ole tema allkirjaga. Seevastu digitaalse allkirja puhul peab eID omaja tõendama, et allkirja on andnud keegi teine. Ka TsMS § 277 lõikes 3 sisalduvate reeglite kohaldamine digiallkirja ehtsuse vaidlustamisele ei võimalda saavutada praegu olukorda, kus omakäelise ja digiallkirja ehtsuse vaidlustamine oleks võimalik täpselt samadel alustel. See on nii, sest TsMS § 277 lõike 3 kohaselt peab eID omaja oma väidet digiallkirja mitteehtsuse kohta põhjalikumalt põhistama kui omakäelise allkirja ehtsust vaidlustav isik vastavalt TsMS § 277 lõikele 1. Kõrvaldamaks Eesti õiguse vastuolu Euroopa õiguse põhimõtetega, oleks mõistlik TsMS § 277 lõiget 1 muuta nii, et ka omakäelise allkirjaga varustatud dokumendi ehtsust oleks võimalik vaidlustada üksnes selliste asjaolude põhistamisega, mille põhjal võib eeldada, et dokumendil olevat allkirja ei ole andnud selleks õigust omav isik.

Makseteenuste puhul on välja petetud eID-d kasutades tehtud tehingutega seoses keskse tähtsusega autoriseerimata makse mõiste ning tõendamiskoormuse jagunemise reeglid VÕS-s. Autoriseerimata

<sup>66</sup> Vt nt Eesti Panka pangakontorite sulgemine murelikuks ei muuda. – ERR, 08.02.2023. Arvutivõrgus: <https://www.err.ee/1608877910/eesti-panka-pangakontorite-sulgemine-murelikuks-ei-muuda> (04.10.2024).

<sup>67</sup> J. Voltri. Omniva vähendab postkontorite arvu veel viiendiku võrra. – ERR, 21.05.2024. Arvutivõrgus: <https://www.err.ee/1609357953/omniva-vahendab-postkontorite-arvu-veel-viiendiku-vorra> (04.10.2024).

<sup>68</sup> M. Hindre. Asutuste lahkumine Põlvast: mõtteviis riigi kohalolust on muutunud. – ERR, 04.10.2024. Arvutivõrgus: <https://www.err.ee/1609479293/asutuste-lahkumine-polvast-motteviis-riigi-kohalolust-on-muutunud> (04.10.2024).

<sup>69</sup> Credit24. Arvutivõrgus: <https://credit24.ee/ettevotest/> (04.10.2024); Bondora. Arvutivõrgus: <https://www.bondora.ee/bondorast/kuidas-kaib-laenu-taotlemine/> (04.10.2024); Smsraha. Arvutivõrgus: <https://smsraha.ee/abi-ja-kontakt> (04.10.2024).

<sup>70</sup> Nt Digiregistratuur. Arvutivõrgus: <https://digiregistratuur.ee/login> (04.10.2024); Perarst24. Arvutivõrgus: <https://www.perearst24.ee> (04.10.2024).

maksena tuleb käsitada makset, mille tegemiseks eID omaja oma nõusolekut andnud ei ole. Kuna maksetehingule nõusoleku andmise näol on tegemist tahteavalduse tegemisega, siis peab selles sisalduma eID omaja tahe konkreetne maksetehing teha. Olukorras, kus eID-d kasutab kolmas isik ilma eID omaja teadmata, ei sisaldu korrektset eID kasutamises eID omaja tahet vastav tehing teha ning seega ei saa rääkida eID omaja antud nõusolekust. Selline maksetehing tuleb lugeda autoriseerimata makseks. Tõendamiskoormuse kandmiseks peab makseteenuse pakkuja lisaks korrektsele eID kasutamisele esile tooma täiendavaid asjaolusid, mis võimaldavad tõendada, et eID omaja on tehingu teinud ise, väljendades oma tahet.

**Autorist:** Piia Kalamees on Tartu Ülikooli tsiviilõiguse kaasprofessor.