

Digi(taal)allkirjast talataristuni

Anto Veldre

Cybernetica AS infoturbeinsener ja tehniline toimetaja

Käsitletagu siinset kirjutist eelmise¹ jätkuna ning loetagu kindlasti veel kord üle ka sealses sissejuhatuses esitatud postulaadid.

Oma igapäevatöös puutun sageli kokku õigusaktidega, mis üritavad kirjeldada IT-maailma, infoturvet, andmekaitset ja küberit²it ning – üllatus? – ebaõnnestuvad. Sageli saab lõhe alguse kahe maailma(vaate) põrkumisest. Selline teemapüstitus pole sugugi uus – aastat 15 tagasi õnnestus mul käia ENISA³ konverentsil, kus juba siis käsitleti juristide ja tehnikute omavahelist suhestumist. Mulle tundub, et IT-spetsialist on kahe jalaga maa peal: kõik, mis ta teeb, allub loodusseadustele ja formaalloogikale. Juristi ülesanded on pisut teistsugused: tema teenindab valitsemis⁴mehhanismi ning seejuures pole ülearu oluline, kas ta tegevuse käigus loodud virtuaalsed konstruktsioonid on reaalses maailmas üldse võimalikud, loogilised või vettpidavad. Tõde selgub või(s)tluse hilisemas faasis – läbi tõlgendamise.

Moodsaks valitsemiseks on ühevõrra vaja nii kübergurusid kui ka juriste, isegi nende palgatase on mõnevõrra ühtlustumas. Kuid esimesi tavatsetakse ette kujutada patsi ja habemega ning asotsiaalsena, teisi ülikonformsena nii riietuselt kui käitumises. IT-spetsialistid ja juristid pole sotsiaalselt päris võrdsed. Nende maailmad paiknevad organisatsiooniskeemi eri tasemeil – vaid väga harva õnnestub IT-spetsialistil kõrgemalseisvatele ära tõestada, et jurist tegi vea. Siit erinev suhtumine ka vigade olemusse ja parandamise viisidesse.

Selgugu näiteks, et keemiatehase mingi tootmisprotsess on vääralt (ja inimesi ohustavalt) korraldatud. On kindel, et tõlgendusjuhiste üllitamise asemel muudetakse turvaliseks ikka protsess ise. Seevastu, kui seadus või määrus on otseselt eksitav, siis enamasti seda ei parandata, vaid asutakse tõlgendama. Tsitaat Vikipeediast⁵: „Õigusnormi looja võib⁶ eksida terminite valikus või kasutada formuleeringutes ebatäpseid termineid. Taoline olukord muudab õiguse tõlgendamise tema rakendamisel hädavajalikuks.“

Siinseks teemaks on selles tsitaadis kajastuv olemuslik konflikt, kus üks kahest suhtlevast poolest võib (s.t tohib) ja teine mitte niivõrd (s.t üksnes peab), mis läbi sünergia jääb saabumata. Siis ei toimi ühiskond enam tervikuna ega oma parimal võimalikul moel.

Olen analüüsinud, millised seadusetehtiste mured IT-spetsialiste kõige enam häirivad, ning jõudnud järgmise loeteluni.

¹ **A. Veldre**. [Oskussõnadest valdkondadevahelisel duelliplatsil](#). – Õiguskeel 2023, nr 1.

² *küber* – sellist sõna eesti keeles tegelikult pole, seda tüve tohib kasutada üksnes liitsõna esiosana, vt eelmist.

³ ENISA – European Network and Information Security Agency ehk Euroopa võrgu- ja infoturbe agentuur.

⁴ *valitsemine* – ingl *governance*.

⁵ Vikipeedia, [tõlgendamine](#).

⁶ *võib, saab, tohib* – vt „[Eesti keele põhisõnavara sõnastik](#)“.

- **Terminoloogia** – termineid loovad isikud, kes oma ettevalmistuselt ja teadmistelt seda teha ei tohiks, ning teevad nad seda normaalset protseduuri⁷ eirates. Sageli näib, et õigusaktide koostajail pole aimugi käsitletava valdkonna ISO standarditest ega sealsest ühtsest terminoloogiast. Suhtlus välispartneriga, kes toetub ingliskeelsetele ISO definitsioonidele, osutub selles kontekstis üpris vaevaliseks. Nii näiteks muutus pilvemääruse⁸ tagasiside töötlemisel *teabevaldaja* hetkega *teabepidajaks*. Kabinetivaikuses tekkis uus termin, mil pole ei definitsiooni, liiderkeelset vastet ega pädevat tehnilist sisu.
- **Defektsed definitsioonid**, näiteks aetakse segamini eelnevalt defineeritu ja parasjagu defineeritav. Mis pole ka ime, sest Backus-Nauri⁹ esitusviisi tunneb vaid IT-spetsialist. Või siis üritatakse defineerida sõna, kuigi keeleteadlane teab, et defineerimist vajab hoopis mõiste. Üldiselt peaks mõiste definitsioon olema esitatud kujul „selline soomõiste, mille liigitunnused on järgmised...“. Kontranäide „Orav on see, kui on saba ja ronib puu otsa“¹⁰ osutab murele värvikalt.
- Kirjelduse aluseks oleva **skeema mittemõistmine**. Vikipeedia eeltoodud tsitaat märgib olukorda realistlikult – rakendaja peab, samas kui seaduseteksti andja ei pea, üksnes võib ja tohib. IT-sündmused on mitmetahulised ja detailirikkad, küberturvasündmused veel enamgi. On täiesti mõistetav, miks muu eriala inimesed ei suuda esitatud faktipundart pädevaks skeemaks laiali lapata. Seda tüüpi viga võib sisse juhtuda ka tõlkes – eIDAS 2 tekstis tõlgiti fraas *and the management of remote¹¹ electronic signature and seal creation devices* sedasi: *vahemaa tagant e-allkirjade ja e-templite andmise vahendite haldamine, ehkki pidanuks olema digiallkirju ja e-templid loovate kaugvahendite haldus*. Asjasse pühendatud tehnik suudab seda skeemat endale piisava täpsusega ette kujutada küll. Äkki siis kaasakski selle tehnika kohe alguses ning kuulaks *inter pares* ka tema arvamust?
- Lõpuks aga lihtsalt **hooletusvead**. Tulenevad need mitte niivõrd hooletusest, kui eesti keele lausestuspõhimõtete mittetundmisest – pean sealhulgas silmas omastavade defekti¹² ja loetelu „skoobi“ viga¹³. Keeletoimetaja kaasamine on tore ja armas, kuid pärast seda ei tohiks seaduse sõnastust enam koosolekul omavoliliselt ringi teha – selle käigus võib juhtuda paljutki!

Nüüd, mil taustsüsteem on defineeritud, vaatleme konkreetseid seadusi ja määrusi, kus sisalduvad lapsused murravad e-tiigri kõik neli jalga korraga ning tühistavad e-Eesti üpris seaduseväliseks nähtuseks.

⁷ Oskussõnaloo normaalse protseduuri tehnikas eeldab eelkõige ühtsuse saavutamist senise mõistesüsteemiga.

⁸ Eelnõude infosüsteem, toimik nr 23-0863, seletuskiri, lk 49–50, pööratagu tähelepanu ka sealse dokumendiplangi pealkirjale: „PPA laevastiku ületoomise seletuskirja kavand“.

⁹ Backus-Naur esitusviis kujul: <tähis> ::= __väljend__

¹⁰ Definitsioon, mille väidetavalt Mati Hint sai ühelt oma tudengilt.

¹¹ *remote* on siin adjektiiv *device*’i juurde, mitte määrus *management*’i juurde.

¹² Omastavade defekti näide: Linnavalitsuse altkäemaksu likvideerimise komisjon.

¹³ Näide: sinised jänesed ja rebased – mis värvi olid rebased?

Avaliku teabe seaduse juhtum

AKIT¹⁴ annab aimu, et ingliskeelne *information* lõheneb IT-oskuskeeles kaheks: *informatsioon* esitatakse masinatele ja *teave* inimestele jõukohases vormis. *Infot* muul kujul kui kõnekeeles ja liitsõnaprefiksina ei eksisteeri. Seega tuleb dihhotoomne vahe sisse juba avalikul informatsioonil ja avalikul teabel, avalikest andmetest rääkimata. Tuleb välja, et avalikud andmed¹⁵ ongi see, mida avatasemel mõeldakse – ent avalik teave pole seda teps mitte. Avaliku teabe seaduse (AvTS)¹⁶ definitsiooni kohaselt on avalik teave hoopis kõik see, mida avaliku sektori asutus oma töö käigus toodab (vt täpset sõnastust AvTS § 3) ning mis võib osutada ülimalt mitteavalikuks. Naiivsel lugejal tõmmatakse definitsioonide vahetamisega vaip korralikult alt.

Kuidas tähenduse asendamine toimub? Kuulus vene kinorežissöör Lev Kulešov¹⁷ teab! Sõnumi või kujundi tähendus jadas sõltub mitte üksnes elemendi enda tähendusest, vaid ka talle eelnevate ja järgnevate elementide tähendusest. Soojenduseks kasutatakse väljendit *avalik teave* AvTSis juba enne selle defineerimist, selle võttega kinnistatakse fraas tema üldtähenduses. Siis aga, §-s 3, esitatakse selle fraasi eritähendus, mis erineb üldtähendusest totaalselt, kuid definitsiooni keerukuse tõttu ei pääse paraku mõjule. Samas paragrahvis defineeritakse *avalik teave* igaks juhuks veel kord ümber – „edaspidi *teave*“ – ehk kuna edaspidi epiteeti *avalik* ei lisata, tundub naiivsele lugejale, et kõike järgnevat sooritataksegi igasuguse teabega ning et *avalikule teabele* jäi tema üldtähendus. Ei jäänud. Saite petta.

Üks kaabutrikk tehakse veel – seletuskirjas kirjeldatakse pikalt ja laialt, kuidas kogu avaliku sektori töö tulemus on põhimõtteliselt avalik ning kuidas seda tohib piirata üksnes erijuhtudel. Seaduse sisu ise aga täieneb samal ajal üha uute piirangute ja lahtiütlustega. AvTS § 3 definitsioonile viitavad nüansse selgitamata üha uued õigusaktid, sealhulgas nn pilvemäärus¹⁸.

Retooriline küsimus: kas saanuks hakkama tähenduse arvukate transformatsioonideta?

Pilvemäärus

Pilvemääruse § 1 defineerib AvTS-i §-s 3 määratletud *avaliku teabe* veel kord ümber – ja üllatus – seekord iseendaks, *avalikuks teabeks*. Tõenäosus, et lugeja pärast seda läheb *avaliku teabe* definitsiooni mujalt otsima, muutub seeläbi nullilähedaseks. Lugeja usub nüüdsest siiralt, et tegu on selle fraasi üldtähendusega (kuid vt eelmine jaotis).

Ent pilvemääruse kvaliteet jääb latist allapoole muudeski aspektides. Pealkiri on täiesti eksitav – mingeid võrgu- ega infosüsteemi nõudeid seal ei esitata, jutt käib ikka pilvest ja selle

¹⁴ AKIT.

¹⁵ NB! *Avaandmed* on ebaõnnestunud lühendus, tõenäoliselt on need avause (aiaaugu) vahetus läheduses asuvad andmed. Vt ka veebileht avaeksperdid.ee ja diskussioon eelmises artiklis (märkus 1).

¹⁶ RT I, 07.03.2023, 11.

¹⁷ Vt <https://dzen.ru/a/YSPKiPJilmj3-1Sw> ja <https://dzen.ru/a/ZWrO2Z1uGWLnqsMd>. Ettevaatust, need lingid viivad vaenulikku välisriiki!

¹⁸ Nn pilvemäärus, täispealkirjaga „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“, RT I, 09.01.2024, 25.

kasutuselevõttust. Kuid edasi läheb veel hullemaks. Määrus on kirjutatud sedasi, et tehnikule poleks arusaadavad ei regulatsiooni objektid ega subjektid.

Pilve puudutavad standardid (ISO 19940, 17788, 17799) jagavad pilvvõimed kolmeks: rakendusevõime, taristuvõime ja platvormivõime. Määruse seletuskirjas neid sõnu ei kasutata, ka mitte ehedat eestikeelset *pilveltrakendust*, *pilveltaristut* ega *pilvelplatvormi*, vaid turustatakse jätkuvalt võõramaist SaaS, PaaS ja IaaS. Sellest järeldub otseselt, et määruse loojate maailmas ISO standardeid ei eksisteeri. Siit ka vead. Kus ISO pilvestandardid eristavad täiesti selgelt **klienti** (*customer* – CSC) **lõppkasutajast** (*user* – CSU), seal räägib pilvemäärus kasutamisest hoopis kliendi kontekstis.

Määrus reguleerib kolme objekti kasutuselevõttu teatud subjektide lõikes. Need objektid on

- 1) pilvteenus;
- 2) pilvandmetöötlusteenus;
- 3) andmetöötlusressursside kogum, mis on paindlikult jagatav ja laiendatav võrgu- ja infosüsteemi ennast muutmata.

Tehnik saab aru vaid kõige esimesest terminist – **pilvteenus** (ISO standardi *cloud service* – CS). Kahe järgmise olemust pole võimalik mõista. Sest kui hakata eristama andmete töötlemise teenust nende mittetöötlemise, näiteks lihtsalt kogumis- või talletusteenusest (vt eespool oleva loetelu p 2 vs. p 3), siis tekivad probleemid tähendusega. Pole vast suur saladus, et isikuandmete kaitse üldmääruse¹⁹ arusaam töötlemisest on vastuolus normaalse IT-arusaamaga (neist esimene sisaldab ka andmete talletamist ja säilitamist ehk siis andmetega mitte midagi tegemist). Teiseks aga, kui need kaks (pos 1 ja 2) on samased, siis miks on vaja neid alul eristada ja siis § 2 lg 1 tekstis ikkagi ühe **pilvteenuse** alla kokku panna: „edaspidi koos *pilvteenus*“?

Mis varjub kole mõiste nr 3 taha, jääb selgusetuks. Võimalik, et siia on tahetud peita kas X-teen, ummistusründe eest kaitsvat teenust (näiteks firmalt Cloudfare) või riigipilve. Sest tehnik ju teab, et riigipilv pole tegelikult üldse mitte täisväärtuslik pilv, vaid pigem klubiline majutusriiul – riigiasutuste „ühispilv“²⁰ – *community cloud*, kuid pilvele omase mastabeeruvuse ja geograafilise ulatuseta.

Segadus valitseb ka teenuse kasutusviisi puhul. Tehnik näeb kaht võimalikku skeemi: a) asutus võtab välismaist pilvteenust otse välismaa firmalt; b) ta võtab omamaist teenust riigipilvest. Esimene käitumismall on kordades turvaohlikum, kuid § 2 pealkiri „Avaliku sektori osutatava pilvteenuse ja pilvandmetöötlusteenuse kasutusele võtmise eeldused“ ja sisu jätavad mulje, justkui põhiline turvamist vajav kasutusjuhtum oleks hoopis omamaine pilv, kuivõrd turvanõuded esitatakse just siin ja sellele. Tulemus: välismaalt pärit pilvteenusele eraldi paragrahvi pole ning sellele turvanõudeid üldse ei esitatagi. Sellega karjuvas vastuolus on aga

¹⁹ Euroopa Parlamendi ja nõukogu [määrus \(EL\) 2016/679](#) füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

²⁰ Vt AKIT, [community cloud](#).

§ 2 lg 2 p 4 sõnastus, mis kohustab hindama „osutaja“ ja „importija“ (!!!) usaldusväärsust (kas tõesti Eesti riigiasutus peabki hindama Eesti riigiasutuse usaldusväärsust?).

Pilvemääruse § 2 vastuolulisusele on vaid üks võimalik selgitus: kirjutajatel mõlkus salamisi meeles hoopis kolmas pilvetarvitamise skeem, kus kohalik tegija, näiteks riigipilv, võtab välismaa pilvefirmadelt teenust, peseb selle turvaliseks ja puhtaks ning jaotab arvukate avaliku sektori asutuste vahel laiali. Kui nii, siis tuleks vahendajat kaasav skeem selmet seda kõrglingvistiliste passaažide vahele peita, läbipaistvalt lahti kirjutada koos vahendaja kõigi kohustustega. Verdikt: pilvemäärus tegelikult ei täida oma eesmärki, selle mõistmiseks on vaja avalikus käibes puuduvat lisateavet. Tegelikult polnuks pilvemäärust üldse vajagi, sest ülisarnase kohaldamisalaga Eesti infoturbestandard (EITS)²¹ määratleb samad eesmärgid oma moodulites OPS2.3, OPS2.2 ja OPS3.2.

Segadus ulatub ka terminoloogiasse. Tagasiside arutamise käigus (vt märkus 7) avastas ametnik, et termin *teabevaldaja* põhjustab talle probleeme. Keegi ei märganud, et sisuliselt käis jutt hoopis andmetest. Tekitati uus termin *teabepidaja* (vrd *pean kassi* ja *pean teavet*). Koosolekul ei viibinud teadaolevalt ühtki terminoloogi, võib-olla oleks õnnestunud omavahel ortogonaalsesse vastavusse panna vastutav töötleja andmevaldajaga ning volitatud töötleja andmepidajaga. Olnuks loogiline.

Eestikeelsest sõnast „usaldusväärsus“ on pilvemääruses ootamatult saanud termin. Ei märganud, et sel sõnal on ingliskeelseid vasteid vähemalt kolm: *reliability*, *credibility* ja *trustworthiness*, mistõttu termini alusmõiste ISO standardite tähenduses jääbki tuvastamatuks.

Toimet (*pro* talitlust) ja osutamist (*pro* teenustamist²²) käsitlesin eelmises kirjutises (vt märkus 1), raske on leida seadust, mis tarvitaks neid tehnilisi termineid õigesti.

Kuigi pilvemääruse lisa esitatakse fakultatiivsena, leidub segadusi ka seal. Vaevalt suudaks infoturbeinimene või andmekaitseametnik analüüsida mõne suurfirma rahaallikaid, peakorterit asukohta ja kohtusüsteemi läbipaistvust – kuigi seda kõike eeldatakse ilmsi.

DAS²³ ja EUTS²⁴

Digi(taal)allkirja defineerimatus juhtumil on kaks lapsevanemat: 2016. aasta sügisel DASi EUTSiga asendamisel tehtud hooletusviga ning EL-i õigusaktid, kus digiallkirjade asemel räägitakse hoopis elektroonilistest ehk e-allkirjadest. Veel üks lisamure tuleneb inglise ja eesti keelte semantilisest erinevusest, sest *digital signature* saab meil vaheldumisi olla kas *digitaalsignatuur* – seda juhul, kui tegu on tehnilise vahendiga, või *digitaalallkiri*, kui jutt käib signatuurile seadusega garanteeritud rakendusviisist. Tõlkides tuleb alati eristada, kumb on kumb, kusjuures vahel tuleb eristada veel kolmandat varianti: et autor neid kaht ei eristanud ja käsitles ingliskeelses tähenduses koos. Probleem algab just nimelt viimasest, kuivõrd keegi ei

²¹ EITS – Eesti infoturbestandard, vt <https://eits.ria.ee/>.

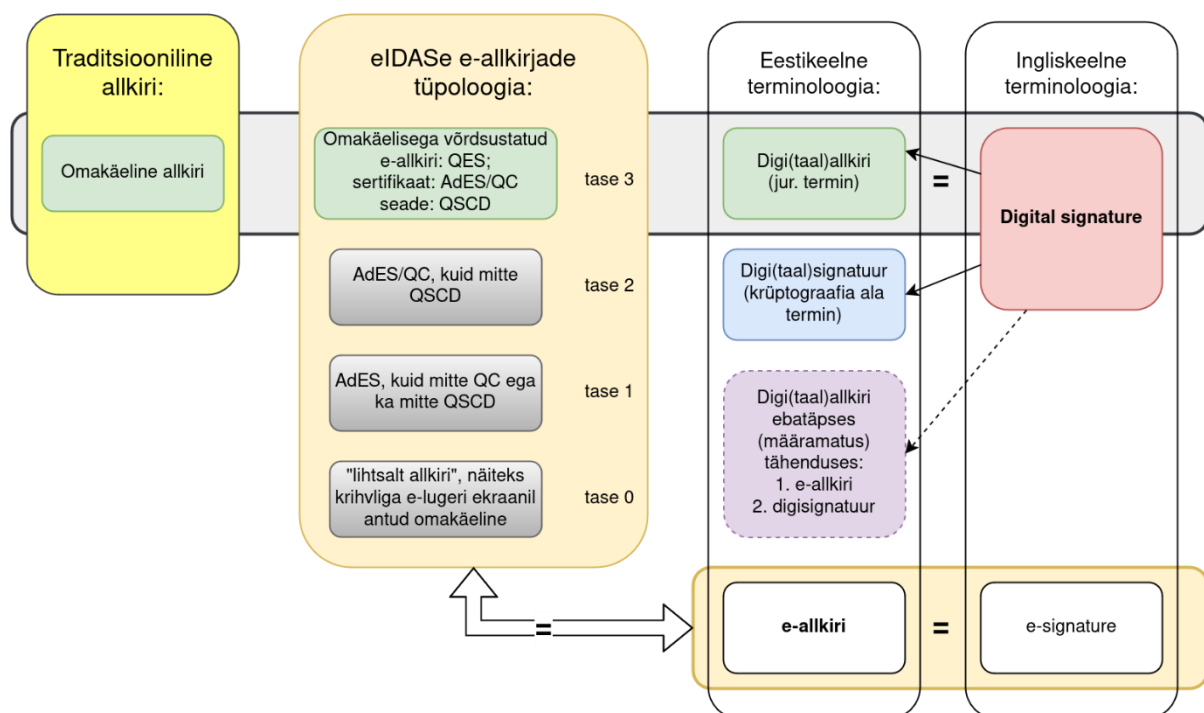
²² AKIT, [teenustamine](#).

²³ [Digitaalallkirja seadus](#), praeguseks juba kehtetu.

²⁴ E-identimise ja e-tehingute usaldusteenuste seadus, [RT I, 03.03.2023, 3](#).

saa väita, justkui oleks eesti keeles sõna *digitaalallkiri* tähendus automaatselt selge. Ei ta ole ühti, järelkult vajab igal juhul defineerimist.

Kuivõrd Eesti on osa oma digisuveräänsusest nüüdseks loovutanud EL-ile, siis pärinevad ka vastavad seadusesätted sealt ja nende kõrval osutuvad meie endi seadused/määrused suhteliselt sekundaarseks. eIDAS²⁵-e kohaselt on e-allkirju nelja sorti: – alates „lihtsalt allkirjast“ (näiteks krihvliga Telia tahvlile käsitsi antavast) kuni nn QES-allkirjani (kõige turvalisem ja parem, omakäelisega võrdsustatud). Eesti- ja ingliskeelsete terminite vastavust on kujutatud joonisel 1. Probleem seisneb selles, kuidas suhestada omavahel 11 kastikest, aga eelkõige, kuidas vastendada eIDASes määratud kastikest „QES e-allkiri“ ning eesti mütoloogias pidevalt esilekerkivat kastikest „dig(itaal)allkiri“. Käsitleme seda teemat üksnes seetõttu, et praktikas pole vastendamine õnnestunud.



Joonis. Digiallkirja puudutavad terminid ja nende omavaheline suhestumine

Kõigepealt tuleb selgeks teha, mida *digi(taal)allkiri* üldse tähendab. Ükski tehnik ega jurist ei kahtle, et see on eIDAS-e kõrgeimale, kõige toredamale tasemele vastav e-allkiri. Paraku, kui see asjaolu mõnes Eesti seaduses kinnitust ei leia, taandub ihaldatud vastavus hajusluuluks.

Kuni aastani 2016 oli olukord lilleline. Eesti omatermin *digitaalallkiri* defineeriti DASi § 2 lõikes 1: „Digitaalallkiri on tehniliste ja organisatsiooniliste vahendite süsteemi abil moodustatud andmete kogum, mida allkirja andja kasutab, märkimaks oma seost dokumendiga.“ Kuigi definitsioon oli puudustega (ei vastanud mallile soomõiste/liigimõiste), see vähemasti eksisteeris.

²⁵ Euroopa parlamendi ja nõukogu [määrus \(EL\) nr 910/2014](#) e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.

EUTS asendas DASi ning jõustus 25. novembril 2016. EUTSi arutamise ajal oli veel kõik korras, sest digitaalallkirja definitsioon sisaldus alles kehtivas DASis. Kuid keegi ei märganud, et EUTSis endas definitsiooni enam pole. Seega hetkel, kui kolksatas Riigikogu esimehe haamer, kadus ka digitaalallkirja definitsioon. Puhas hooletus.

Ei saa eitada, et EUTSis sisaldub üks kirjakoht, mis üritab miskit defineerida. Selleks on § 24 lg 1. Vaatame, mida seal räägitakse: „Digitaalallkirja loetakse e-allkirjaks, mis vastab Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 3 punktis 12 sätestatud kvalifitseeritud e-allkirja nõuetele.“ Paistab selgelt, et EUTSi kehtestamise hetkel olid juristid mures pigem selle üle, mis saab meie seni antud digiallkirjadest. EUTSi definitsiooni võib vaadelda nii- ja naapidi, kuid see eirab defineerimise reegleid totaalselt. Seal ei öelda, et „digiallkiri on“. Seal öeldakse, et „digitaalallkirja loetakse nii- ja naasuguseks e-allkirjaks“. Ent kusagilt ei selgu, mis on digiallkiri ise.

Olen Eesti õigusakte guugeldanud risti ja põiki ning võin öelda, et mall „B loetakse A-ks“ on erandlikult harv – kasutusel enamasti kontekstis, et mingi nõue A loetakse täidetuks ka erijuhul B (näiteks VÕS²⁶: „kohustus loetakse täidetuks“). Kuid kusagilt ei ilmne samasust: et kohustus B oleks iga A puhul automaatselt täidetud või veel enamgi, et kohustus B oleks samane oma täidetusega A. Otse öeldes: fraas „loetakse millekski“ osutab erijuhule. Definitsioon pidanuks kõlama umbes nii: „Digitaalallkiri on eIDASe kvalifitseeritud e-allkirja (QEC) nõuetele vastav e-allkiri.“ Lihtne?

On tehtud veel üks katse digi(taal)allkirja defineerida, sedakorda tsiviilseadustiku üldosa seaduses (TsÜS)²⁷. Selle §-s 80 tõdetakse, et „elektrooniliseks allkirjaks on ka digitaalallkiri“ (selle fraasi autoril on tuline õigus nüansis, et ka kümned muud asjad meie digiallkirja kõrval kvalifitseeruvad e-allkirjaks). Keelekorraldajad teavad²⁸, miks on väljend „Muri on koeraks“ paha. Tuleb aru saada, et saava käände puhul satuvad objektid A ja B (*a.k.a* defineeritav ja seniteatu) omavahel vahetusse. Grammatiliselt normaalne (kuigi sisult väär) lause kõlaks: „QEC e-allkiri loetakse digiallkirjaks“. Probleem on selles, et sugugi mitte iga QEC-allkiri (näiteks Läti oma) ei ole Eesti seaduste kohaselt digiallkiri.

Vähe sellest, et DASi definitsioon kaotas kehtivuse, see poleks tänastes oludes eIDASe kontekstis pädev enam isegi mitte pidepunktina – sest vahepeal on aeg edasi läinud ja eIDASe vastavusnõuded on juba oluliselt karmimad.

Kokkuvõtte on karm: Eesti seadustes täna digi(taal)allkirja definitsioon puudub. Juristidel pole õnnestunud joonise 1 kaht kõige olulisemat kastikest omavahel kvaliteetselt seostada. Mis on selle fakti võimalikud tagajärjed, mõistab igaüks isegi. Üksainuke keeleliselt vigane definitsioon põhjustab ulatuslikke tagajärgi kogu riigikorralduses. Ent sellega segadus ei piirdu.

²⁶ Võlaõigusseadus, [RT I, 04.07.2024, 17](#).

²⁷ [RT I, 06.07.2023, 98](#).

²⁸ Vt Eesti Keele Instituudi [keelenõuannete kogu](#).

Valimisseadused

Valimiste korraldus on Eestis reguleeritud Riigikogu valimise seaduse (RKVS), kohaliku omavalitsuse volikogu valimise seaduse ja Euroopa Parlamendi valimise seadusega. Neist sisulisim on RKVS²⁹, kus digitaalallkirja nimetavad päris mitmed sätted (§-d 48⁴, 48⁵, 48⁸ ja 60¹). Ülejäänud valimisseadused pelgalt viitavad RKVS sätetele.

Mõistmaks, mis täpselt on valesti, tuleb süveneda eIDASe olemusse. eIDASele allub terve hulk rakendusmäärusi, mis määratlevad e-allkirja (sh QES-taseme e-allkirja) mitmesuguseid omadusi. Turvatasemest oli juba juttu, kuid rakendusmäärused³⁰ viitavad veel ka arvukatele tehnilistele standarditele³¹, millele e-allkiri peab vastama. Kui kasvõi üht neist arvukatest standarditest pole järgitud, siis ei ole enam tegemist e-allkirjaga ja ammugi ei saa siis tegemist olla digi(taal)allkirjaga.

Jätan siinkohal detailselt refereerimata Riigikohtust õilsal ettekäändel tagasi põrgatatud kaebekirjad, mis väitsid, et valimistel on e-allkirjaga miskit valesti. Igaüks leiab need ise, kuid tehnikuna kinnitan, et ongi valesti. Või täpsemini, tehniliselt on e-hääletusel kõik väga õige (ja turvaline), paraku see, mida häälte kogumise ja arvestamise käigus allkirjadega tehakse, väljub raamest, mida eIDAS juriidiliselt võimaldab.

Nimelt, eIDASe e-allkirja vääramatuks eelduseks on rangelt ettenähtud vorming. Ese, mille vorming ei vasta standardis EN 319 102-1 määratletud vormingule, ei ole eIDASe mõistes enam e-allkiri, ning ammugi mitte digiallkiri. See on lihtsalt kogus bitte, äärmisel juhul veel ka juppideks saetud signatuur. Sest just seda e-hääletuse käigus tehakse – puhttehnilistel põhjustel, heas usus lõhutakse signeeritud hääle algosakesteks, mida siis hoitakse erinevates kohtades. Parafraseerides kuulsat sententsi, peab asi mitte ainult näima seaduslik, vaid selline ka olema, mida praegune e-hääletus aga ülalkirjeldatud põhjusel olla ei saa. Põhjus on formaaljuriidiline – tuleks lihtsalt paika keerata digi(taal)allkirja definitsioon ja õige pisut kõpitseda valimisseadusi – et need ei väidaks eIDASe rakendusmäärusele risti vastu, justnagu häälte kogumise käigus käideldaks e- või digiallkirja. Küll juristid vajaliku sobitusfraasi välja mõtleavad, eriti nüüd, kus nad on aru saanud kurbmängu tehnilisest sisust.

Õnneliku lõpu asemel

10. augustil 2024 kuulutati Paide arvamusefestivalil välja NATO sõnause tulemused. Nüüdsest on julgeolekuarhitektuuri asemel vaja rääkida **turvatalastust**. Naiivse pilguga vaadates: inglise *security* väljakujunenud vastena käibis välis- ja kaitseministeeriumi haldusalas pikalt „julgeolek“, siseministeeriumi haldusalas aga „turvalisus“. Sellest 15 aastat kestnud vaikivast kokkuleppest nüüd taganeti.

²⁹ Riigikogu valimise seadus, [RT I, 24.05.2024, 10](#).

³⁰ Sh komisjoni [rakendusotsus \(EL\) 2015/1506](#), millega kehtestatakse täiustatud e-allkirja ja täiustatud e-templi vormingu kirjeldus vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 27 lõikele 5 ja artikli 37 lõikele 5.

³¹ Nt standard [EN 319 102-1](#).

Mis puudutab arhitektuuri taandamist talastuks, *tala* kui keskse arhitektuurielemendi tähendust (näiteks väljendis *panin (ettevõtmisele) tala*) ning võrdlusi *taristu vs. talastu*, siis see kõik võinuks olemata olla. Alammõiste ei tohiks üritada ümber defineerida põhimõistet. Arhitektuuri oluline erinevus struktuurist seisneb asjaolus, et arhitektuur on millegi väline vaade, struktuur aga selle sisemine korraldus. On (võib-olla liigagi) ilus, et talastu/taristu kui vastandpoolused on täiusliku *yin-yang*-paarina nüüdseks teineteist leidnud. Teisalt aga usuvad julgeolekuametnikud, et neil õnnestub uut väärisõna *turvatalastu* sedasi hillitseda, et selle kasutus toimuks vaid väga piiratud kontekstis – NATO strateegiadokumentides, mitte aga näiteks kunstiakadeemias ega ehituskoolis. Võtan seda lubadusena ja loodan, et minu salahirmud (*talataristu* küsimuses) eales ei realiseeru.