SISEMINISTEERIUM

Justiitsministeerium

Teie: 18.10.2023 nr 10-4/6884-1

Meie: 02.11.2023 nr 2-1/758-7

Avaliku teabe seaduse muudatuste kaardistus

Täname algatuse eest kaardistada avaliku teabe seaduse (edaspidi ka *AvTS*) kitsaskohti. Selle seaduse kitsakohad on üks valdkond, millele on Siseministeerium varemgi tähelepanu pööranud. Toome käesolevas kirjas esile teemad, mida peame olulisemaks.

1. Hinnata tuleks AvTS-i kooskõla sellega, et riik on üle läinud dokumendikeskselt haldus elt teabehalduse mudelile - dokument ~ teave selles ~ teabekandja. Samuti tuleks hinnata, kas avaliku sektori asutuste teabe avalikustamine avaliku dokumendiregistri lahendusena on tänases infoühiskonnas mõistlik, turvaline, kasutajamugav ja kaasaegne lahendus. Kas teabe avalikustamise eesmärk – avaliku võimu teostamise läbipaistvus ja võimalus kontrollida avalike ülesannete täitmist – tänasel viisil avalikus dokumendiregistris ning sellega kaasnev halduskoormus (avalikustamisele kuuluva teabe eel- ja järelkontroll), avaliku dokumendiregistri arendamine ja selle kulu, juurdepääsupiiranguga teabe osakaal ning võimalikud kaasnevad riskid, on omavahel mõistlikus tasakaalus. Näiteks Politsei- ja Piirivalveameti dokumendiregistris on juurdepääsupiiranguga teabe osakaal üle 90%.

2. Ülevaatamist vajavad teabenõude täitmisest keeldumise alused, eelkõige nö saripöördujatele vastamisest keeldumine. Oleme sellele tähelepanu juhtinud ka 06.09.2023 kirjas nr 1- 7/197- 5 „Vastus märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seaduse muutmise seaduse eelnõule“ punktis 7 – see puudutab küll märgukirjale või selgitustaotlusele vastamist, kuid sama probleem esineb ka teabenõuete puhul.

3. AvTS-is tuleks korrastada juurdepääsupiirangute kehtestamise või pikendamise pädevust ning hinnata, kas kõiki toiminguid peab tegema asutuse juht või võib seda delegeerida allapoole. Näiteks AvTS § 34, 38, 40 on vastav õigus ainult asutuse juhil, seevastu AvTS § 41 lg 1^1 kohaselt võib lisaks asutuse juhile otsustada konkreetsele dokumendile juurdepääsupiirangu kehtestada asutuse juhi määratud pädev töötaja.

4. Kõige suurem probleemistik on juurdepääsupiirangualuste piisavuse ja piirangute tähtaegade osas. Toetame igakülgselt aluste kataloogi avamist ja neist nii mõnegi sõnastuse täpsustamist õigusselguse huvides, kui ka põhjusel, et mõningatel juhtudel on üldisi andmekaitsepõhimõtteid arvestades igati põhjendatud teabe määratlemine juurdepääsupiiranguga teabeks, kuid samal ajal sobiva AvTS aluse leidmine pigem väljakutse, kui mitte võimatu. Juurdepääsupiirangu alused on sageli liialt dokumendi-kesksed, mistõttu ei pruugi ära katta kõikvõimalikke tänapäevaseid teabekandjaid. Samuti on probleemiks teabe hankimise kiirus ja lihtsus, mis teeb võimalikuks erineva teabe kiire omavahelise võrdlemise (vastukaaluks dokumendikeskne teabe hankimine,

selle kõrvutamise ja muud aeganõudvamad toimingud tegid selle kohmakaks). Selline kiirus ja teabe kõrvutamise võimalus võib olla ohuks julgeolekule.

Leiame, et kindlasti tuleks üle vaadata AvTS § 40 lõikest 1 tulenev 10-aastane maksimaalne juurdepääsupiirangu tähtaeg. Oleme aastaid juhtinud tähelepanu nimetatud tähtajaga seonduvale probleemistikule (erinevate pöördumiste loetelu on leitav kirja lõpus). Samuti oleme teinud ettepaneku täiendada riigisaladuse ja salastatud välisteabe seaduse (edaspidi *RSVS*) täiendamist § 11 lg-ga 4, mis võimaldaks RSVS § 11 lg-s 3 nimetatud teabe puhul AK juurdepääsupiirangut pikendada senikaua kuni juurdepääsupiirangu kehtestamise põhjus püsib, kuid mitte üle samadele tunnustele vastava riigisaladuse salastamise tähtaja. Viimati tegime RSVS muutmise ettepaneku Justiitsministeeriumi algatatud vangistusseaduse, karistusseadustiku ja kriminaalhooldusseaduse muutmise seaduse eelnõule 22.05.2023 kirjas nr 1-7/74-3.

5. Nii kuritegevuse kui ka riikliku julgeoleku seisukohast on murekoht ka autentimata juurdepääs igasugustele avaandmetele ja registritele. Varasemalt on olnud kaasuseid, kus tulenevalt AvTS kehtivast sõnastusest on alla laetud erinevaid andmestikke, mida hiljem kuritarvitatakse ning riigil puudub võimalus isikustada, kes need andmed alla laadis. Probleemi lahendamiseks peaks AvTS-is ette nägema isikustatud juurdepääsu kõigi riigi poolt üleslaetud andmestikele ning registritele, eelkõige neile, kus leidub mingeidki isikuandmeid. See tõstab märgatavalt pahatahtliku tegutseja lävendit nende andmete omandamisel ja võimaldab hiljem kuriteotunnuste tuvastamisel välja selgitada, kes võis olla andmete omandamise taga.

6. Leiame ka, et üle tuleks vaadata andmekogude peatükk. Üheselt peaks olema selge, mis alustel või eeldustel tekib/muutub miski riigi infosüsteemi kindlustavaks süsteemiks ning selgelt võiks AvTS-is olla ka toodud, kes teeb kindlustavate süsteemide kasutuselevõtu üle järelevalvet ning mis ulatuses.

   Samuti peaks seaduse tasandil olema selgelt toodud, mis peab olema andmekogude puhul reguleeritud seaduse tasandil ning mis peab olema põhimääruses, lähtudes nii Eesti Vabariigi põhiseaduse kui ka isikuandmete kaitse üldmääruse nõuetest. Praegu on andmekogude regulatsioonid väga erinevad. Ka isikuandmete ja andmekogu vastutava töötleja mõiste vajab selgitamist, alati ei pruugi need kattuda ja on andmekogusid, milles isikuandmeid ei ole.

   Aeg-ajalt on tõusetunud vaidlused andmekogude ja andmeladude või -aitade mõistete ja neile kehtivate nõuete kohta. Majandus- ja Kommunikatsiooniministeeriumi eestvedamisel valmis 14.04.2023 selgitav juhis „Andmeladude olemus ja selle funktsioonid“, kus tuuakse välja, et andmelao defineerimiseks seaduses puudub vajadus. Ühtlasi selgitatakse, et olemuslikult on andmeladu andmekogu osa. Õigusselguse huvides oleks mõistlik täiendada AvTS sätetega, millal andmeladu tuleb asutada seaduse tasandil ja millal andmeladu on andmekogu osa.

7. Nõustume, et tähelepanuta ei saa jätta teabe väljastamise pädevust (ühe ukse põhimõte). Õigusselguse huvides tuleks teabe väljastamise loogika selgelt seaduse tasandil reguleerida, lõpetamaks olukorra, kus teabenõudjad ja adressaadid võivad tõlgendada nii väljastamiseks kohustatud isikut kui ka väljastamisele kuuluvat teavet erikujul. Samas tuleb seda väga täpselt reguleerida, kuna on teada juhtumeid, kus ühe asutuse juurdepääsupiiranguga teavet väljastab teine asutus ning see jõuab osapooleni, kes ei tohiks seda teavet mitte mingil juhul näha. Ka tuleb siin arvestada välisriigilt saadud juurdepääsupiirangut sisaldava teabega.

8 Nõustume, et kiirelt areneva tehnoloogia ning andmete kiirema ja mugavama käitlemise vaates võib olla vajalik juurdepääsupiirangu määramise mõningane automatiseerimine. Sellise lahenduse olemasolu võib mugavdada andmete jagamist ja piiramist. Küll aga kätkeb see juba eos teatavaid riske ning tehniliselt ei ole seda lihtne lahendada. Näiteks kinnitas seda TEXTA projekt, mille

raames oli eesmärk treenida piisavalt täpsed mudelid juurdepääsupiiranguid vajavate dokumentide tuvastamiseks dokumendihaldussüsteemis DELTA. See tähendab igal juhul lisaarendusi tänastesse dokumendihaldussüsteemidesse. Leiame, et uute tehnoloogiliste arenduste puhul peaks lõplik otsustus jääma teabevaldajale, sh kas ja kuidas ta neid rakendab.

9. Toome esile ka, et kõik asutused ei kasuta juurdepääsupiirangu klassifikaatoreid. Eeldatavasti on dokumendihalduse süsteemides kasutusel vabateksti väli, mistõttu kasutajad sisestavad juurdepääsupiirangu aluseid erineval viisil. Tagamaks süsteemide omavahelise toimimise juurdepääsupiiranguga teabe kaitsel tuleks nõuda klassifikaatorite kasutamist, eriti DHX kaudu saatmisel. Samuti on juhtumeid, kus asutused, kes peaksid oma teavet kaitsma ei märgista dokumenti ja eeldavad, et teine osapool (saaja) kaitseb teavet avalikuks tuleku eest.

Täiendavalt märgime, et erinevaid probleemikäsitlusi, eelkõige liiga lühikese juurdepääsupiirangu tähtaja kohta, oleme pikemalt selgitanud oma erinevates kirjades, eelkõige 2016. aasta kirjades, edaspidi on pigem viidatud juba esitatud probleemidele:
- 24.03.2016 kirjaga nr 2-1/116-1;
- 19.05.2016 kirjaga nr 1-6/1210-1;
- 21.12.2017 kirjaga nr 2-1/246-3;
- 11.05.2018 kirjas nr 1-7/88-5;
- 22.04.2021 nr 1-7/92-5 ning
- 22.05.2023 nr 1-7/74-3.

Lisaks on teema olnud arutusel erinevat formaati koosolekutel, näiteks 2016. aasta augustis Siseministeeriumi ja Justiitsministeeriumi kohtumisel (protokollitud), 2019. aasta septembris Justiitsiministeeriumi korraldatud koosolekul avaliku teabe läbipaistvamaks muutmise kohta ning 2020. aasta jaanuaris Andmekaitse Inspektsioonis toimunud avaliku teabe nõukogu koosolekul (protokollitud). Samuti on juurdepääsupiirangute tähtaja lühiduse probleemi kirjeldatud ühes eelnõus, mida küll Justiitsministeerium ei kooskõlastanud, kuid probleemid on jätkuvalt üleval - https://eelnoud.valitsus.ee/main/mount/docList/427d1494-5abe-4d30-a1cf-b61cf3785183.

Oleme valmis oma probleemkohti täpsemalt selgitama ning ootame Siseministeeriumi kaasamist edaspidistesse tegevustesse. Ehk on õigem kaardistada probleeme ka valdkonnapõhiselt, sest näiteks sisejulgeoleku/turvalisuse valdkonna või sotsiaalvaldkonna sfääri kuuluvad küsimused võivad erineda üsna suurel määral.

Lugupidamisega

(allkirjastatud digitaalselt)

Krista Aas
varade asekantsler

Kertu Nurmsalu 6125084
kertu.nurmsalu@siseministeerium.ee