JUSTIITSMINISTEERIUM

Riigikohus
info@riigikohus.ee

Teie 30.09.2022 nr r 3-18-477/62
Meie 30.10.2022 nr 10-3/6915

Arvamuse esitamine

Austatud Riigikohtu esimees

Riigikohus küsis justiitsministri arvamust vangistusseaduse § 31[1] esimese lause põhiseaduspärasuse kohta. Lisaks paluti vastajal avada, millised riskid võivad kaasneda vangidele täiendava ligipääsu võimaldamisega riigiasutuste (eeskätt vaidlusalustele) veebilehtedele ning millised võivad olla kulud (sh riskide maandamiseks).

VangS § 31[1] esimese lause kohaselt ei ole kinnipeetaval lubatud kasutada internetti, välja arvatud vanglateenistuse poolt selleks kohandatud arvutites, mille kaudu on vanglateenistuse järelevalve all võimaldatud juurdepääs ametlikele õigusaktide andmebaasidele, kohtulahendite registrile, Riigikogu veebilehele ja õiguskantsleri veebilehele.

Olen seisukohal, et VangS § 31[1] esimene lause on põhiseadusega kooskõlas. Sätte osa, mis lubab juurdepääsu üksnes kindlatele veebilehtedele, kujutab endast samaaegselt juurdepääsupiirangut sättes nimetamata veebilehtedele. Interneti vahendusel teabele juurdepääsu piiramist muudele kui sättes nimetatud veebilehtedele õigustavad kaalukad hüved: ühiskonna turvalisus, sh eesmärk tagada, et kinnipeetav ei paneks vangistuses viibimise ajal toime ega organiseeriks uusi kuritegusid. Piirangu puhul on seega kaalul oluline avalik huvi.

Oluline on arvesse võtta, et kinnipeetavale ei ole keelatud juurdepääs avalikuks kasutamiseks mõeldud teabele. Piirang puudutab üksnes juurdepääsu teabele interneti vahendusel, kuivõrd selle lubamisel ei ole võimalik alati tagada, et kinnipeetav ei saaks samal ajal juurdepääsu veebilehe osale, mille kaudu on võimalik elektrooniline suhtlemine. Nimetatud piirangu on seadusandja kehtestanud VangS § 31[1] teises lauses. Veebilehe sisu ja muudatusi ei ole mõistlikult (sh optimaalsete kuludega) võimalik igal ajahetkel kontrollida, seire ei ole järjepidev ja arvutiprogrammiga teostatav, mistõttu kontrollimiseks on vajalik inimtööjõud. Veebilehtede monitoorimise ja lubamatule osale juurdepääsupiirangute seadmisega seotud kulud ning riskid kasvavad järjest igale täiendavale veebilehele juurdepääsu võimaldamisega. Seadusandja on sätestanud, et vanglateenistus kontrollib, kellega kinnipeetav telefoni teel suhtleb või kirjavahetust peab (VangS § 29 lõige 2[1]). Vanglateenistusel on kohustus tõhusalt kontrollida, et kinnipeetav ei jätkaks vangistuses viibimise ajal kuritegude toimepanemist. Juurdepääsu võimaldamine rohkematele veebilehtedele (nt riigiasutuste puhul VVS § 38 tähenduses lisanduks ca 150 veebilehte) tähendab praktikas seda, et VangS § 29 lõikes 2[1] sätestatud kontroll toimuks tagantjärele ning varjatud suhtlusvõimaluse avastamise tõenäosus väheneks igale järgnevale veebilehele juurdepääsu võimaldamisega. Kui kinnipeetav on saanud veebilehe kaudu keelatud viisil suhelda, on kahju juba tekitatud.

Kinnipeetavate internetile ligipääsu laiendamise küsimuses, sh julgeoleku- ja turvariskidega seonduva osas, jään Riigikohtu üldkogule asja nr 3-3-2-1-16 menetlemisel esitatud seisukohtade juurde (justiitsministri 31.03.2017. a vastus nr 10-4/1972-2 „Arvamuse andmine Riigikohtu üldkogu asjas nr 3-3-2-1-16“). Julgeoleku- ja turvariskide ning nende maandamiseks vajalike ressursikulude kohta on Justiitsministeerium vastanud Tartu Halduskohtule 20.11.2017. a vastuses nr 13-3/6706-7, 27.04.2018. a vastuses; 11.05.2018. a vastuses nr 13-3/2319-5, 06.12.2019. a vastuses nr 13-3/6830-1 ja Riigikohtule 24.05.2022. a vastuses nr 13-3/3365-2. Kuivõrd neis vastustes sisaldub nii teave piirangutega seotud ressursikulude kohta kui ka põhjendused, mis toetavad seisukohta, et piirang on põhiseaduspärane, siis palume neis sisalduvaid põhjendussi arvesse võtta lisaks käesolevas vastuses kajastatule. Täiendavate veebilehtede lubamisega seotud riskid ja vajalikud kulutused on kirjeldatud käesoleva vastuse punktides 19–33.

I Asjaolud ja menetluse käik

1. Riigikohtu menetluses on Romeo Kalda kaebus juurdepääsu saamiseks Riigikohtu veebilehele, selle alamlehekülgedele ja Ametlike Teadaannete veebilehele. Varasem menetluse käik on üksikasjalikult kirjeldatud Riigikohtu halduskolleegiumi 17. augusti 2022. a määruses asjas nr 3-18-477.[1]
2. Riigikohtu halduskolleegium andis kohtuasja 17. augusti 2022. a määrusega lahendamiseks Riigikohtu üldkogule, kuna kohtuasja lahendamisel on vaja hinnata VangS § 31[1] esimese lause põhiseadusele vastavust.

II Vaidlusalune säte

3. Vangistusseaduse vaidlusalune säte (vaidlustatud osas allajoonitud) on sõnastatud järgnevalt:

„§ 31[1]. Interneti kasutamine
Kinnipeetaval ei ole lubatud kasutada internetti, välja arvatud vanglateenistuse poolt selleks kohandatud arvutites, mille kaudu on vanglateenistuse järelevalve all võimaldatud juurdepääs ametlikele õigusaktide andmebaasidele, kohtulahendite registrile, Riigikogu veebilehele ja õiguskantsleri veebilehele. Kinnipeetaval on keelatud juurdepääs veebilehe osale, mis võimaldab elektroonilist suhtlemist.“

III Justiitsministri seisukoht

Normikontrolli lubatavus – vaidlustatud sätte asjassepuutuvus

4. PS § 15 lg 1 ja põhiseaduslikkuse järelevalve kohtumenetluse seaduse (PSJKS) § 9 lg 1 kohaselt on konkreetse normikontrolli taotlus lubatav juhul, kui norm, mille põhiseaduspärasuse kontrolli põhiseaduslikkuse järelevalve kohtult taotletakse, on kohtuasja lahendamisel asjassepuutuv. Normi asjassepuutuvuse hindamisel peab lähtuma sellest, kas see kuulub kohtuasjas kohaldamisele või mitte.[2] Norm peab seejuures olema kohtuasja lahendamisel otsustava tähtsusega.[3] Norm on otsustava

[1] Arvutivõrgus: https://www.riigikohus.ee/et/lahendid?asjaNr=3-18-477/61
[2] RKPJKo 02.12.2002, 3-4-1-11-02, p 13
[3] RKÜKo 22.12.2000, 3-4-1-10-20, p 10

tähtsusega siis, kui kohus peaks asja lahendades normi põhiseadusvastasuse korral otsustama teisiti kui normi põhiseaduspärasuse korral.[4]

5. Norm on asjassepuutuv, kui selle kehtetuse tõttu oleks võimalik teha teistsugune otsus. Kuivõrd VangS § 31[1] esimene lause (täpsemalt lauseosa „kinnipeetaval ei ole lubatud kasutada internetti“) välistab kinnipeetavate juurdepääsu veebilehtedele, millele kinnises vanglas kinnipeetavana viibiv kaebaja praeguses asjas ligipääsu soovib, ning Riigikohtu veebileht ja Ametlike Teadaannete võrguväljaanne ei kuulu ka VangS § 31[1] esimeses lauses sätestatud erandi alla, siis sõltub kohtuasja lahendamine sellest, kas VangS § 31[1] esimeses lauses sätestatud interneti kasutamise keeld on (vaidlusaluses osas) põhiseadusega kooskõlas või mitte. Kaebused saab rahuldada üksnes juhul, kui kõnealune keeld on põhiseadusega vastuolus ja seda sisaldav norm tunnistatakse kehtetuks, vastasel juhul tuleb kaebused jätta rahuldamata, mistõttu on VangS § 31[1] esimene lause asjassepuutuv norm ja seega on põhiseaduslikkuse järelevalve lubatav.

Piiratav põhiõigus ja selle riive

6. VangS § 31[1] esimeses lauses sätestatud keeld piirab (interneti vahendusel) ligipääsu üldiseks kasutamiseks mõeldud teabele, millele ligipääsu õigus on tagatud põhiseaduses. Riigikohtu kolleegiumi hinnangul ei ole nimetatud keelu eesmärk antud juhul väga kaalukas, mistõttu võib kolleegiumi hinnangul säärane regulatsioon olla vastuolus PS § 44 lõigetega 1 ja 2.

7. Põhiseaduse § 44 lg 1 esemeline kaitseala on üldiseks kasutamiseks levitatav informatsioon. Tegu on kõigi ja igaühe õigusega. Vangistusseaduse § 31[1] keelab kinnipeetaval interneti kasutamise, välja arvatud vanglateenistuse poolt selleks kohandatud arvutites, mille kaudu on vanglateenistuse järelevalve all võimaldatud juurdepääs ametlikele õigusaktide andmebaasidele ja kohtulahendite registrile. Kõnealune säte riivab PS § 44 lõikes 1 sätestatud põhiõigust teabe saamise viisi kaudu.

8. PS § 44 lg 1 võib mõista teatud mõttes piirava sättena, sest see sätestab õiguse saada üksnes sellist informatsiooni, mis on „üldiseks kasutamiseks levitatav“. Seega ei taga säte juurdepääsu mitte igasugusele informatsioonile, vaid üksnes teatud kvaliteeditunnustele vastavale informatsioonile. Kui aga võtta arvesse Eestile siduvaid rahvusvahelisi õigusakte, kus informatsiooniõigusele üldjuhul selliseid piiranguid sätestatud ei ole, ning silmas pidades ka seda, et § 44 lg 1 on reservatsioonita põhiõigus, on võimalik § 44 lg 1 piisavalt avar sisustamine.

9. PS § 44 lg-s 1 sätestatud põhiõigus on reservatsioonita põhiõigus ja seega peavad selle põhiõiguse piirangud olema õigustatavad teiste põhiseaduslike väärtustega või teiste põhiõigustega (vt eesmärgi konkreetsusega seoses RKÜKo 30.06.2017, 3-3-2-1-16, p-d 22–24; RKHKo 15.12.2017, 3-13-2425/53, p-d 21–22). Selline põhiseaduslik väärtus on ühiskonna turvalisuse tagamine, sh vangla julgeolek ning kinnipeetava turvalisuse tagamine, mis on tihedalt seotud vangistuse eesmärkide saavutamisega. Ühtlasi seostub see õiguskorra kaitsmise vajadusega. Õiguskorra kaitsmine karistuse täideviimise eesmärgina tähendab eelkõige selle tagamist, et süüdimõistetu ei paneks karistuse kandmise ajal toime uut kuritegu. Selliselt realiseeritakse vangistusega muu hulgas eesmärk tagada ühiskonna turvalisus (nii vangla julgeolek kui ka väljapoole

[4] RKPJKo 02.12.2002, 3-4-1-11-02, p 15

vanglat jäävate isikute turvalisus) ja laiemalt põhiseadusliku väärtusena riigi sisemine rahu.[5] Vangistuses viibimise perioodil piiratakse ka isiku muid põhiõigusi (nt omandiõigust, õigust era- ja perekonnaelu puutumatusele), kuivõrd vastasel juhul ei oleks vangistuse täideviimise eesmärk saavutatav. Põhiõigus, mis annab isikule õiguse kasutada vabaks kasutuseks olevat teavet, ei ole samuti piiramatu õigus. Interneti kasutamise keeld on sobiv vahend vanglavälise keelatud suhtluse takistamiseks (julgeoleku tagamiseks) või kriminaalmenetluse lubamatu mõjutamise vältimise eesmärgi saavutamiseks, kui seda eesmärki on selle meetmega põhimõtteliselt võimalik saavutada. Ühtlasi on piirangu eesmärk välistada internetist sellise teabe hankimist, mis võib ohustada vangla julgeolekut ja ühiskonna turvalisust väljaspool vanglat.

Riive põhiseaduspärasus

10. Kaebaja õiguste riive põhiseaduspärasuse kontrollimiseks on vaja hinnata, kas VangS § 31[1] sätestatud interneti kasutamise keeld on põhiseaduspärane. Põhiõigusi piirav õigustloov akt on formaalselt põhiseaduspärane, kui ta vastab pädevus-, menetlus- ja vorminõuetele ning määratuse ja seadusereservatsiooni põhimõtetele.[6] Vaidlusalune säte vastab formaalse põhiseaduspärasuse nõuetele.

11. Riigikohtul puudub alus seaduse või muu põhiseadusest alamal seisva õigusakti põhiseadusvastaseks tunnistamiseks, kui normi on võimalik tõlgendada põhiseaduskonformselt. Teisisõnu, erinevate tõlgendusvõimaluste korral tuleb eelistada põhiseadusega kooskõlas olevat tõlgendust neile tõlgendustele, mis põhiseadusega kooskõlas ei ole. Samuti tuleks eelistada tõlgendust, millega oleks tagatud erinevate põhiseaduslike väärtuste kõige suurem kaitse.[7] Materiaalset põhiseaduspärasust hinnates tuleb käsitleda põhiõigust piirava normi proportsionaalsust. Põhiõigusi riivav õigustloov norm on materiaalselt põhiseaduspärane, kui riivel on legitiimne eesmärk ja riive on proportsionaalne (sobiv, vajalik ja mõõdukas), st kaalub üles riive ebasoodsa mõju.

12. Esmalt tuleb tuvastada, mis on põhiõiguste piiramise legitiimne eesmärk. VangS § 31[1] lõike 1 esimeses lauses sätestatud sisulise piirangu laiem eesmärk on tagada ühiskonna turvalisus (sh vangla julgeolek) ning õiguskorra kaitse. Kitsamas mõttes on piirangu eesmärk tagada, et süüdimõistetu ei paneks karistuse kandmise ajal toime uut kuritegu. Seda eesmärki teenib ka sama sätte teine lause, mille eesmärk on välistada kinnipeetava elektrooniline suhtlemine, mis väljub vanglateenistuse kontrolli alt ja mis oleks vastuolus VangS § 28 lõikes 3 sätestatuga.

13. Veebilehtedele juurdepääsu võimaldamisel lähtutakse VangS § 31[1] teise lause alusel põhimõttest, et kinnipeetavale ei tohi olla juurdepääsu veebilehe osale, mille kaudu on kinnipeetaval võimalik saata või saada kirju, teateid või teha või võtta vastu kõnesid. Elektroonilise suhtluse all peetakse silmas mistahes vormis suhtlust, mille abil on võimalik kirjavahetuse pidamine või kõnede tegemine. Kuivõrd VangS § 29 lõike 2[1] järgi kontrollib vanglateenistus, kellega kinnipeetav telefoni teel suhtleb või

---

[5] Vt Riigikohtu Üldkogu 07.12.2009 otsus asjas nr 3-3-1-5-09, p 31. Arvutivõrgus kättesaadav: https://www.riigikohus.ee/et/lahendid?asjaNr=3-3-1-5-09

[6] RKPJK 13.06.2005.a otsus asjas 3-4-1-5-05, p 8. Arvutivõrgus kättesaadav: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-5-05

[7] 3-2-1-73-04, p 36.

kirjavahetust peab, siis peetakse ka VangS § 31[1] lõike 1 teises lauses silmas suhtlusvorme, mille kaudu on võimalik teha kõnesid või pidada kirjavahetust. See nähtub muu hulgas 2019. a VangS muutmise seaduse eelnõu[8] seletuskirjast, mille kohaselt peeti elektroonilist suhtlust võimaldava osana silmas muu hulgas teabenõude vormi, avalduse ja tagasiside vormi, foorumit jms. Veebilehtedel võivad nendeks veel olla nt reaalajas kasutatav klienditeenindustugi, teisele veebilehele suunavad lingid, mis võimaldavad suhtlust teise veebilehe kaudu (nt erinevad sotsiaalmeedia rakendused) jms. Näiteks võimaldas ka õiguskantsleri veebileht teabenõude ja avalduse saatmist ning Riigikogu veebileht teabenõude ja tagasiside saatmist. Seletuskirjas põhjendati, et hüperlinkide kasutamine kinnipeetavatel välistatakse, sest vastasel korral puuduks vanglateenistusel selge ülevaade kinnipeetava vanglavälise suhtluse ulatusest (muudatusega lisatud veebilehed sisaldasid hüperlinki sotsiaalmeedia kanali veebilehele). Seega lähtub ülesande täitja otseselt VangS § 31[1] teises lauses nimetatud tingimusest – mistahes veebilehe osa, mille kaudu on võimalik kirjalik või suuline suhtlemine, peab olema kinnipeetavale välistatud. Kui kinnipeetavad saaksid kirjavahetust pidada ka veebilehe kaudu, eeldaks selle kontrollimine ulatuslikumaid infotehnoloogilisi arendusi ja investeeringuid. Samas ei pruugi ka alati olla tagantjärgi tuvastatav, kellega on kinnipeetav elektroonilisel teel suhelnud. VangS § 29 lg 2[1] kohaselt peab vanglateenistusel olema võimalik seda kontrollida. Seaduses sätestatud kohustust ei ole võimalik tagada, kui kinnipeetaval on võimalik kasutada internetis veebilehtede osi, mis võimaldavad elektroonilist suhtlust.

14. Kirjavahetuse ja telefonikõnede kontrollimine kujutab endast PS §-ga 11 kooskõlas olevat põhiõiguse proportsionaalset riivet. Ka on Euroopa Inimõiguste Kohus seisukohal, et kontroll kinnipeetavate kirjavahetuse või telefonikõnede üle ei ole konventsiooniga vastuolus, kui meetmel on legitiimne eesmärk ning seaduslik alus. See eesmärk on seotud põhiseadusliku väärtusega kindlustada riigi sisemine rahu.[9] Euroopa Inimõiguste Kohus on oma praktikas möönnud, et riigi ametiasutuste viidatud turva- ja majanduslikke kaalutlusi võib pidada piirangu vajalikkuse põhistusena asjakohasteks. Seega on turva- ja majanduslikud kaalutlused EIKi praktika järgi legitiimsed. Turvalisuskaalutlused on EIKi väljakujunenud praktika kohaselt põhjuseks, miks kinnipeetavate õigusi võib piirata. Euroopa Inimõiguste Kohtu asjas nr 17429/10 tehtud otsuse eriarvamuses on väljendatud, et ei ole õige riiki sanktsioneerida selle eest, et ta on võimaldanud kinnipeetavatele juurdepääsu teatud internetilehekülgedele, ning et EIKi otsus heidutab teisi riike üldse sellist võimalust kinnipeetavatele pakkumast. Samuti, kuigi EIK on viidanud interneti tähtsust rõhutavatele rahvusvahelistele instrumentidele, ei näe ükski nendest instrumentidest ette kinnipeetavate õigust internetile. Kuigi tegemist oli EIKi esimese otsusega selles küsimuses, puudub otsuses Euroopa Nõukogu riikide praktikate võrdlev ülevaade. Kuna sellise õiguse tunnustamiseks ei olnud eriarvamuse kohaselt piisavalt alust, siis aluste puudumise tõttu peaks tegelikult riikidel olema hoopis ulatuslik kaalutlusõigus kõnealuses küsimuses.[10] Ka Eesti kohtupraktikas on leitud, et riivet õigustasid põhiseaduse preambulis väljendatud väärtused, nagu sisemise rahu kaitse. Keelu

[8] Vangistusseaduse muutmise seadus 680 SE, eelnõu ja seletuskiri arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8f08bcf8-2b6b-4017-b64c-6eea9c00a98c

[9] Vt ka Vangistusseadus. Kommenteeritud väljaanne, Sootak. J., Juura, 2014, § 2[1] kommentaar, p 1,2, lk 94.

[10] EIK aktsepteeris lahendis Kalda vs. Eesti EIÕK artikli 10 riive legitiimse alusena teiste isikute õiguste kaitsmise ning kuritegude ja korratuste ärahoidmise eesmärki. Lahend ja eriarvamus kättesaadav: http://hudoc.echr.coe.int/eng?i=001-160270

eesmärgina nägi Riigikohtu üldkogu vajadust kaitsta ühiskonna turvalisust - nii julgeolekut vanglas kui ka ühiskonna turvalisust väljaspool vanglat, mh karistuse eesmärkide täitmise soodustamise teel.[11] Eeltoodut arvestades on piirangu eesmärk legitiimne.

15. Sobiv on abinõu, mis soodustab eesmärgi saavutamist. Sobivuse seisukohalt on vaieldamatult ebaproportsionaalne abinõu, mis ühelgi juhul ei soodusta piirangu eesmärgi saavutamist.[12] VangS §-ga 31[1] välistatakse juurdepääs Riigikohtu veebilehe alamlehekülgedele ja veebilehele Ametlikud Teadaanded. Seetõttu on välistatud, et kinnipeetavatel oleks võimalik vaidlusaluste lehekülgede kaudu kasutada internetti viisil, mis võiks ohustada vangistuse täideviimise eesmärke või ühiskonna julgeolekut ning välistab vanglavälise elektroonilise suhtlemise võimaluse nende veebilehtede kaudu. VangS §-s 31[1] sätestatud meede on seega sobiv abinõu soovitava eesmärgi saavutamiseks.

16. Abinõu on vajalik, kui eesmärki ei ole võimalik saavutada mõne teise, kuid isikut vähem koormava abinõuga, mis on vähemalt sama efektiivne kui esimene. Antud juhul on meede vajalik, sest isikut vähem koormava abinõuga ei ole sama efektiivne tulemus saavutatav. Kinnipeetavatele järjest täiendavatele veebilehtedele ligipääsu võimaldamisega tekiks olukord, kus vanglal ei ole ühel hetkel enam võimalik täita seadusandja poolt vanglateenistusele VangS § 66 lg 1 ja VangS § 29 lg 2[1] sätestatud kohustust. VangS § 66 lg 1 kohaselt korraldatakse kinnipeetavate järelevalve viisil, mis tagab vangistusseaduse ja vangla sisekorraeeskirjade täitmise ja üldise julgeoleku vanglas. VangS § 29 lg 2[1] kohaselt kontrollib vanglateenistus, kellega kinnipeetav telefoni teel suhtleb või kirjavahetust peab. Olukorras, kus kinnipeetaval on võimalik saada juurdepääs väga paljudele veebilehtedele, sh veebilehtedele, mida ei halda riigiasutused, ei pruugi olla võimalik suhtlust eesmärgile vastavalt kontrollida. Sel juhul ei ole vanglateenistusel enam võimalik täita VangS § 66 lg-st 1 ja § 29 lg-st 2[1] tulenevaid kohustusi. Puudub meede, mis tagaks eesmärgi saavutamise VangS §-s 31[1] sätestatud piiranguga sama efektiivselt, kuid põhiõigusi vähem riivaval viisil.

17. Abinõu mõõdukuse üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusesse sekkumise ulatust ja intensiivsust, teiselt poolt aga riive eesmärgi tähtsust.[13] Kaalumine eeldab kokkuvõttes võimalikult kõigi poolt- ja vastuargumentide nimetamist ja kohtu seisukohavõttu.[14] Käesoleva kohtuasja puhul on oluline arvestada, et kinnipeetavad saavad ligi Riigikohtu poolt avaldatud kohtulahenditele. Seega on tagatud juurdepääs Riigikohtu poolt avaldatud kohtulahenditele kui teabele, millele juurdepääsu saab pidada isiku õiguste kaitseks vältimatult vajalikuks. Veebilehel olev muu informatsioon ei ole kinnipeetava õiguste kontekstis sama kaaluga. Ametlike Teadaannetega (AT) seonduvalt on esmalt tähtis, et AT võrguväljaandena on esmajärjekorras mõeldud teadete avaldamiseks olukorras, kus isiku asukoht ei ole teada (nö kättetoimetamise fiktsiooni rakendamise tarbeks). Kinnipeetava asukoht on riigile teada. Muude AT-s avaldatud andmetega seonduvalt on kaheldav, et kinnipeetaval oleks nendega tutvumise korral võimalik asuda teadetest tulenevaid õigusi realiseerima – nt osaleda ameti- ja kutsekonkurssidel, kasvava metsa raieõiguse või pankrotivara enampakkumistel. Samuti on riive mõõdukuse hindamisel oluline, et

[11] https://rikos.rik.ee/LahendiOtsingEriVaade?asjaNr=3-3-1-5-09 p 34
[12] PS kommenteeritud väljaanne; § 11, komm 10.
[13] RKÜKo 3-4-1-7-01, p 21.
[14] PS kommenteeritud väljaanne; § 11 komm 17.

kinnipeetaval on võimalik saada üldiseks kasutamiseks mõeldud informatsiooni teabenõudega. Õigusaktidele ja kohtulahenditele, s.o teabele, mis on vajalik otseselt kaebaja õiguste kaitseks, on kaebajal vangla arvutis interneti vahendusel ligipääs olemas ja seega on isikul võimalik oma õigusi (nt kohtumenetluses) efektiivselt kaitsta. Samuti on seadusandja võimaldanud kinnipeetavatele juurdepääsu Riigikogu ja õiguskantsleri veebilehtedele. Riigil on kohustus tagada kinnipeetud isikutele juurdepääs üldiseks kasutamiseks mõeldud teabele, kuid see ei tähenda, et kinnipeetavale peab olema tagatud kiire ja vahetu juurdepääs kõigi riigiasutuste veebilehtedele. Avalikuks kasutamiseks mõeldud teabele interneti teel juurdepääsu mittevõimaldamise proportsionaalsuse hindamisel tuleb arvestada isiku huvide ja vajaduste kõrval riigi kohustusega kindlustada olulise avaliku huvi kaitse – tagada, et kinnipeetav ei jätka vangistuse ajal kuritegude toimepanemist.

Riskid ja kulud täiendava ligipääsu võimaldamisel

Arvamuse andmisel käsitlen järgnevalt riske, mis võivad kaasneda kinnipeetavatele täiendava ligipääsu võimaldamisega riigiasutuste veebilehtedele, samuti juurdepääsuga seonduvaid kulusid.

18. Halduskolleegium märkis (määruse punkt 42), et kolleegiumi hinnangul ei kahjusta ühiskonna turvalisust see, et kinnipeetavale on kättesaadav avalikuks kasutamiseks mõeldud teave, mida riigiasutused jagavad oma tegevuse kohta. Selle seisukohaga saab sisuliselt nõustuda, kuid arvestada tuleb asjaoluga, et piirangu seadmisel ei ole lähtutud mitte konkreetse riigiasutuse poolt avaldatava infoga seonduvatest riskidest, vaid punktides 12-17 viidatud kaalutlustest. Samuti märgime, et mõiste „riigiasutus“ hõlmab väga laia ringi erinevate ülesannetega asutusi. Arvesse tuleb võtta, et ühe asutuse hallata võib olla mitu erinevat teemapõhist veebilehte. See tähendaks täiendavalt ligikaudu 150 veebilehte, kuid lehti võib olla ka rohkem (nt juhul, kui ühelt veebilehelt avanevad teised alamlehed). Riigi ametiasutus avaliku teenistuse seaduse § 6 lõike 1 tähenduses on: 1) valitsusasutus VVS tähenduses; 2) Riigikogu Kantselei; 3) Vabariigi Presidendi Kantselei; 4) Riigikontroll; 5) Õiguskantsleri Kantselei; 6) kohus; 7) soolise võrdõiguslikkuse ja võrdse kohtlemise voliniku kantselei. Täidesaatva riigivõimu asutused Vabariigi Valitsuse seaduse (VVS) tähenduses on: 1) valitsusasutused; 2) valitsusasutuste hallatavad riigiasutused (nt muuseumid, haridusasutused, Eesti Kohtuekspertiisi Instituut, Eesti Keele Instituut, Keskkonnaagentuur, Tervise Arengu Instituut jpt). Valitsusasutused on ministeeriumid, kaitsevägi ja Riigikantselei, samuti ametid ja inspektsioonid ning nende kohalikud täidesaatva riigivõimu volitusi omavad asutused. Seadusega võib ette näha ka teisi valitsusasutusi (VVS § 39 lg 3). Lisaks on riigil rida sihtasutusi, näiteks Haigekassa, Töötukassa, KredEX, Ettevõtluse Arendamise Sihtasutus. Täiendavalt tuleb arvestada, et ka kohalikud omavalitsused avaldavad oma veebilehtedel teavet, mis võib olla isiku vaates kasulik ja avalikkusele suunatud samadel põhjendustel, mis riigiasutuste veebilehtede puhul.

19. Konkreetsetest riskidest rääkides viitame, et paljude asutuste veebilehtedel on alamleheküljed, mille kaudu avanevad täiendavad lisalehed, millest vanglateenistusel ei pruugi teavet olla. Seda tuleks iga kord käsitsi üle kontrollida. Näiteks, ka Justiitsministeeriumi veebilehelt on võimalik edasi liikuda veebilehele, www.kriminaalpoliitika.ee, www.korruptsioon.ee, https://kpkoda.ee/,

www.juristaitab.ee jt. Seega tuleks leida igalt veebilehelt üles lingid, kust omakorda võib avaneda mõni elektroonset suhtlust võimaldav kanal.

20. Tavapäraselt on veebilehtedel suhtlust võimaldavaks osaks teabenõude[15], märgukirja või selgitustaotluse esitamise elektroonne vorm, mis sageli annab ka võimaluse saata suvalisele meiliaadressile pöördumise koopia[16]. Seda on võimalik üpris lihtsasti kasutada soovitud e-posti aadressile sõnumi saatmiseks. Juhul, kui selline suhtlusvõimalus on jäänud märkamata või on veebilehel tehtud muudatuste tõttu ekslikult avatuks jäänud ning kui turvariski ei avastata ega seda suleta õigeaegselt, ei ole võimalik kontrollida, kellega kinnipeetav on suhelnud. Juhul, kui piirang kõrvaldada, siis seda, kellega kinnipeetav suhtleb, sh nt eesmärgiga jätkata kuritegude toimepanemist vangistuse ajal, ei ole võimalik kontrollida. Kodeeritud sõnumeid või teavet ei pruugi keegi avastada. Kahtlemata võib öelda, et sellist suhtlust saab korraldada ka telefoni või kirja teel, kuid veebilehte (nt e-kirja teel) oleks kinnipeetaval ilmselt kõige mugavam ja kiirem kasutada, lisaks väheneb keelatud viisil suhtluse puhul vahele jäämise risk sedavõrd, mida rohkematele veebilehtedele on juurdepääs lubatud. Veebilehtede sisu on ajas sageli muutuv ja nendele võib lisanduda funktsioone, mis võimaldavad kontrollimatut keelatud vanglavälist suhtlust. Vastav näide on vanglate praktikas juba olemas Riigi Teataja veebilehe kohta. Justiitsministeerium on varem kirjeldanud „minu RT“ juhtumit haldusasjas nr 3-18-477 27.04.2018. a vastuse nr 13-3/2319-2 punktis 3.9. Nimelt sisaldub Riigi Teataja veebilehel www.riigiteataja.ee „Minu RT“ lahendus, mis võimaldab kasutajal registreerida konto ning tellida akte, kohtukokkuvõtteid ja õigusuudiseid e-postile. Sellele rakendusele kui veebilehe ühele osale oli ka kinnipeetavatel lühikest aega ligipääs, kuni turvaaugu avastamiseni. Probleem oli Riigi Teataja lehekülje osas, mis võimaldas end registreerida lehe kasutajaks. Kasutajaks registreerimisel oli kinnipeetaval võimalik sisestada suvaline e-posti aadress ning paroolivälja trükkida sõnum 6-16 tähemärki. Seejärel sai paroolivälja trükitud sõnumi edastada eelnevalt sisestatud e-posti aadressile. Parooli muutmise teel sai hulgaliste sõnumite edastamist jätkata ning seeläbi tekkis vangidel võimalus saata piiramatult kõikvõimalike sisuga teateid. Seda võimalust ära kasutades sai edastada vanglast väljapoole teateid vanglateenistuse kontrolli alt väljuval viisil. Eeltoodu kinnitab, et kuigi veebileht ise võib olla turvaline, ei pruugi sellel olevad lisarakendused alati arvestada vangistuses viibivate isikute vanglavälise suhtluse piirangutega seonduvaga ning seda ka riigiasutuste endi hallatavate veebilehtede puhul.

21. Lisaks veebilehtedele ligipääsu tagamisele tuleb iga lehe lubamisel teha pidevat seiret, et avastada võimalikke puudujääke ja turvariske. Kuna kulud ja risk kumuleerivad iga veebilehe lisandumisega, siis ei ole õige vaadelda iga veebilehte eraldiseisvalt. See risk tõuseb iga veebilehe lisandumisega. See tähendab ühtlasi aktiivset pidevat koostööd vanglatega, sest infotehnoloogiliselt ei pruugi tehniliselt töötavas süsteemis turvaauke kohe leida. Viga süsteemis võib tähendada ka seda, et mingi funktsioon on kinnipeetavatele ekslikult kättesaadav. Selliseid turvaauke võib olla keerukas tuvastada ja ei ole ka otstarbekas, et veebilehti selliselt pidevalt kontrollitaks. Selleks, et kontrollida järjepidevalt kindlate ajavahemike tagant üle kõik veebilehed ja nende alamlehed, millelt avanevad võimalikud teabenõuete vormid või millele on lisatud

[15] Vt nt https://www.terviseamet.ee/et/teabenoue, https://www.sotsiaalkindlustusamet.ee/et/teabenoudevorm; https://www.rtk.ee/asutus-uudised-kontakt/kontaktid/esita-teabenoue-voi-paring

[16] Vt nt https://www.riigikohus.ee/et/form/teabenoude-esitamine; https://www.evs.ee/et/RequestForInformation; https://piksel.ee/dogre/lepitaja/index.php?module=240&op=&xid=&dok_id=3.

täiendavaid linke, mille hulgas võib olla ka suhtlusportaale või sotsiaalmeediakanaleid, on vajalik personaliressurss. Lehtede sisu tuleb järjepidevalt monitoorida, kontrollida ja vajadusel käsitsi eemaldada juurdepääsud veebilehe osale, mille kaudu on võimalik elektrooniline suhtlus. Samas ei tulene õigusaktidest veebilehe haldajale kohustust tagada ega võtta arvesse vajadust näiteks ka edasiste uuenduste ja arenduste puhul vajadusega keelatud suhtlus välistada.

22. Iga veebilehe seadistamise soov vajab Riigi Info- ja Kommunikatsioonitehnoloogia Keskuse (RIT) tehnoloogiaosakonna sekkumist. Selleks tuleb kontrollida serveris olemasolevaid reegleid, lisada uued reeglid ning teenus seadistada. Keerukus seisneb uute reeglite tekitamises ja lisamises teenuse konfiguratsiooni ilma, et olemasolev funktsionaalsus „katki“ läheks, st vajalik on personal, kes teemat valdab ja asjast aru saab. See on ajakulu teenuse osutajale ja samuti tellijale, kuna vajab tellija poolset testimist ja aru saamist, kuidas asi peaks toimima ja kuidas ei tohiks toimida. Mida rohkem erinevaid reegleid sama domeeni raames on, seda keerulisemaks läheb konfiguratsioon. Selle arvelt kulub rohkem töötunde ning teenuse hind kasvab.

23. Erandite lisandumisel suureneb risk, et lisatud erand ei täida enam oma esialgset eesmärki. See on tingitud sellest, et puudub kontroll selle üle, millist sisu või funktsionaalsust veebilehe omanik konkreetsel URL-il võimaldab. Näiteks kui proksiserveri kaudu on lubatud teostada POST-päringut https://midagi.ee/otsing.html aadressil otsingu teostamise eesmärgil, kuid sinna lehele peaks lisanduma näiteks tagasiside või kommentaari lisamise vorm, siis see reegel seda ei keela, ning seda funktsionaalsust on võimalik kasutada, kuigi lubava reegli esialgne eesmärk puudutas ainult otsingu teostamise võimalust. Iga lisatud erand suurendab seda riski. Erandi iseloomust sõltuvalt võib see eeldada ka veebilehe sisust ja nurgatagustest väga head ülevaadet. See teadmine on veebilehe omanikul ja veebilehtede arendajatel, kes tellivad arendusi veebilehtedele, mitte Justiitsministeeriumil, Registrite ja Infosüsteemide Keskusel (RIK) ega RIT-il. Osadel juhtudel on veebilehtede omanikud ka väljaspool Eestit, mis teeb selle info haldamise eriti keeruliseks.

24. Kinnipeetavatele veebilehtedel keelatud osa (elektroonilist suhtlust võimaldava osa) piiramiseks on ehitatud filtrid, mis piiravad veebilehe funktsionaalsuse, mille sisu on postituse loomine, avatuks on jäetud vaid VangS § 31^1 nimetatud, lubatud lehed. Pidevat järelevalvet selle üle, et veebilehtedel ei oleks avatud mistahes suhtlusvõimalusi, ei ole sisuliselt võimalik teha. See eeldaks iga veebilehe järjepidevat kontrollimist, mis tähendaks tööprotsesside mõttes iga lubatud veebilehe igapäevast kontrollimist, sh tuleb arvestada, et veebilehtede sisu muutub ajas pidevalt, veebilehtedele laetakse uuendusi, lisatakse mooduleid ja rakendusi, muudetakse veebilehe koodi, ülesehitust ja ajakohastatakse veebilehel kajastuvat teavet. Sealjuures ei vastuta veebilehe muutmise eest üks isik, vaid veebilehe eri osadel võivad olla muutmisõigused eri inimestel. Pigem on tavapärane, et veebilehti haldavad väga paljud inimesed, kellel on õigus teha reaalajas muudatusi. Kasutusel ei ole ka programme, mis võimaldaksid võrrelda, kas veebilehel tehtud muudatustes on midagi sellist, millest nähtuks, kas kinnipeetavale võib olla muudatuse tulemusel tekkinud juurdepääs lehe osale, millele tal juurdepääsu olema ei peaks. Veebilehe sisu uuendajate või arendajate puhul ei pruugi kehtida ka taustakontrolli nõudeid, mis

tähendab, et eksisteerib ka oht teadlikult veebilehe sisu muutmiseks vangistuse täideviimise eesmärkide vastaselt. Vastav sisu ei pruugi olla veebilehe menüüst ka leitav. Piisab vaid sellest, kui vastava veebilehe alamleht seatakse üles mingil kindlal URL-il, mida vaid kinnipeetav teab ja sinna tekitatakse sisu, mis võib olla vastuolus vangistuse täideviimise eesmärkide ja VangS § 31[1] teise lausega.

25. Veebilehe kasutaja tehtud päringute filtreerimiseks vastavalt etteantud reeglitele (nt teatud veebilehtede või sisu blokeerimiseks) kasutatakse proksisid. Proksi ehk proksiserver on arvutivõrgus server (riistvara või tarkvara), mis vahendab infovahetust kliendi ehk päringut tegeva süsteemi ja serveri (päringule vastava süsteemi) vahel. Kui vahetu ühenduse korral saadab klient oma päringud otse serverile ning server vastused kliendile, siis proksi kasutamisel saadab klient päringud proksile, proksi edastab need serverile, server vastab proksile ning proksi edastab vastuse kliendile.[17] Veebilehe osale juurdepääsu takistamiseks luuakse filter (proksi), kuid juhul, kui nt veebilehe omanik lehel midagi muudab, on tõenäoline, et proksi ei tööta (suhtlus veebilehte majutava serveri ja kliendi vahel toimub edasi ilma filtrita), samas ei anna süsteem sellest vastutajale teada, piirang seda ei tuvasta (puudub automaatne teavitussüsteem). Veebilehtedel tehtavad uuendused on tavapärased (uuendamata tarkvarad on turvarisk), nt võib mõne kuu pärast peale lehe valmimist olla aegunud nii lehe sisuhaldustarkvara, selle pluginad kui serveri PHP versioon, neid on vaja uuendada, et vältida lehel tekkida võivaid turvaauke, lehe „katki minemist“ või mõne funktsiooni kaotamist. Kuna turvaauguga lehel on lihtsam veebilehele tungida, seda lõhkuda või kaaperdada, siis pigem teevad veebilehtede haldajad uuendusi, mis omakorda tingib vajaduse võimaliku keelatud osa lisandumise kontrolliks. Muudatusega aga ei pruugi olla lisandunud keelatud veebilehe osa, vaid lihtsalt lehe rakendamiseks vajalikud uuendused. Vajalik on piirata ka terminalseadme kasutamist selliselt, et kinnipeetavad ei saaks muuta süsteemi teiste kasutajate jaoks mittekasutatavaks või jätta üksteisele sõnumeid. Selliseid kontrolle tuleb teha sisuliselt igakuiselt, kuna keskseid tootjapoolseid uuendusi väljastatakse kindla regulaarsusega. Võimalikud ohukohad on ka igasugused lisandunud veebilehe funktsionaalsus (nt foorumid, kommentaarid, postituste loomine jms).

26. Reaalajas muudatuste tõttu veebilehe keelatud osale juurdepääsu kohta teavet ei ole seetõttu võimalik saada ning see teave selgub alles hiljem, nt kui vanglale on saanud info teatavaks kinnipeetavate endi või kolmanda isiku kaudu. Veebilehtedel, mida ei halda RIK/RIT, on sellise kontrolli võimalus pea olematu. Veebilehtede haldajatele ei tulene ühestki õigusaktist kohustust tagada oma veebilehtedel tingimusi, mis tulenevad VangS § 31[1], pidevalt luuakse uusi rakendusi, mis soodustaksid veebilehtede külastatavust, suhtlusroboteid jms võimalusi interaktiivselt kasutajakogemuse jagamiseks ja eri klienditeenindusrakenduste mugavalt kättesaadavaks tegemiseks. Veebilehe haldajal on õigus teha veebilehel erinevaid toiminguid, kajastada erinevat teavet ja võimaldada veebilehe külastajal teabega tutvumist, luua leheküljega seotud rakendusi ja lisavõimalusi ning sealjuures ei ole tal mingit kohustust oma tegevust eelnevalt kooskõlastada vanglateenistusega. Sellist kohustust ei tulene ühestki õigusaktist ning sellise kohustuse sätestamine ei ole ka

[17] https://et.wikipedia.org/wiki/Proksiserver

mõeldav. Kõik see tähendab, et vanglateenistusel tuleks ise pidevalt erinevaid veebilehti kontrollida ning nende rakendusi läbi katsetada, suhelda veebilehe haldajatega ja teavitada neid võimalikest probleemist, sulgeda ja avada kinnipeetavate poolt kasutatavaid alamlehekülgi, rakendusi jms. Selleks vajalikud ressursikulud suurenevad iga potentsiaalselt lubatava veebilehekülje lubamisega, olenemata sellest, kes veebilehte haldab. Samuti tuleb arvestada, et igal veebilehe alalehel võib olla mitmeid (kui mitte kümneid) sõltumatuid sisu uuendajaid või arendajaid (sh erinevatest asutustest ja eraettevõtetest), kes pidevalt ka vahetuvad ning kes ei arvesta arenduste tegemisel sellega, et kinnipeetavatele ei ole veebilehe elektroonilist suhtlust võimaldav osa lubatud. Kõik muudatused tuleb käsitsi lisada/eemaldada. Veebilehe kontrollimisel ja seadistamisel lähtutakse järgmistest põhimõtetest:

1) konfiguratsioonis on kirjeldatud domeenid, kuhu ligipääs on lubatud;
2) vaikimisi on igale poole POST-päringute[18] tegemine keelatud ja lubatud on ainult GET-päringud.
3) Erandite alusel on iga veebilehe osas lubatud teatud URL-idel POST-päringud, et veebis otsing toimiks ja teatud kohtades on keelatud GET-päringud.

27. Kuivõrd keelatud suhtlusvõimaluste veebilehelt avastamine on keeruline ja eeldab iga veebilehe osa käsitsi üle kontrollimist ning seda iga päev, siis ei pruugi seda avastatud olla. Näiteks „Minu RT“ juhtum sai samuti teatavaks mitte veebilehe kontrollimise, vaid kolmanda isiku kaudu. Justiitsministeeriumil ei ole teavet selle kohta, kui hästi kolmanda osapoole veebilehti IT-tehniliselt kaitstakse või kui usaldusväärsed on nende lehtede sisu uuendajad ja arendajad. Lehti on võimalik rünnata ja nende osi üle võtta (häkkida). Iga lisanduva lehega see risk kasvab ja riski täielikult maandada ei ole võimalik.

28. Ametlike teadaannete veebilehte haldab RIK ning teave erinevate muudatuste kohta on vajadustel kergesti kättesaadav. Seevastu on nt Riigikohtu veebileht üpris mahukas ning selle põhjalik kontrollimine hõlmab seiret, mis domeenides lehed asuvad (nt https://praktikariigikohtus.mobirisesite.com/praktikariigikohtus.html on teises domeenis), lisaks tuleb kontrollida üle kõik suhtlusvõimalused, vaadata üle kõik lingid, kuhu veebileht külastaja suunab (nt üks suunav link veebilehelt on: https://www.ejtn.eu/Catalogue/EJTNs-searchable-database/), lisaks kontrollida üle videostriimid, mis on lehtedele lisatud, otsustada, mida võib vangile lubada ja mida mitte, realiseerida need reeglid, st lisada veebilehtedele vajalikud IT-tehnilised blokeeringud ning kontrollida üle, kas seatud reeglid toimivad. Kõik see võib võtta personali tööaega summaarselt mitu päeva. Lisaks peab veebilehe pidaja teavitama vanglateenistust igast muudatusest, mida ta lehel on teinud. Kuivõrd sellist kohustust ei tulene veebilehe haldajale õigusaktidest, siis on vaja selleks sõlmida eraldi koostöökokkulepe. Muudatuste teavitussüsteemi on vaja, et vanglateenistusel oleks võimalik üle kontrollida, kas konkreetne muudatus võis kinnipeetavale juurdepääsu veebivaates midagi „katki“ teha. See võib tähendada seda, et mingi osa veebilehest on kinnipeetavale muudatuse tulemusel kättesaadav, kuigi see ei peaks nii olema (nt teabenõude vorm, juurdepääs mingile veebilehele, kuhu muidu ei peaks juurdepääsu

[18] Kasutaja arvuti brauser suhtleb mh nende päringute abil serveriga - kogu info vahetatakse arvuti ja serveri vahel kõige sagedamini POST ja GET päringute abil. GET päringut kasutatakse ennekõike serverist info hankimiseks, seevastu POST päringut serverisse info edastamiseks.

olema). Kui sellist teavet vanglateenistuseni ei jõua, tuleb igakordselt hakata veebilehti ise üle kontrollima. Selline ressursikasutus ei pruugi olla otstarbekas, ühtlasi ei ole RIT-i andmetel selliseks monitooringuks olemas ka automaatset lahendust, mis võiks inimressurssi vajadust vähendada.

29. Kuivõrd iga lisanduva veebilehe kulud kumuleeruvad, siis on Justiitsministeerium toonud välja kuluarvestuse ka sellest lähtuvalt.[19] Justiitsministeerium on hinnanud veebilehtede kontrollimiseks, mis võimaldaks tagada veebilehtede põhjalikumaks (kuid mitte täielikuks) kontrollimiseks vajalikud võimalused[1], ressursikulu järgmiselt: 1) monitoorimissüsteem 300 000 eurot arenduseks (s.o ühekordne kulu), millele lisandub vangla tööjõukulu 172 800 eurot aastas ning lisaks RIK-i tööjõukulu aastas 72 000 eurot. Tegu ei ole ennetava meetmega, kuivõrd monitoorimissüsteem aitab tuvastada võimalikke väärkasutusi hiljem, st rikkumine on juba toimunud. Selline ressursikulu võib olla ebaproportsionaalselt kulukas, kui kontrolli teha järjepidevalt. 2) Ühe veebilehega seotud järjepidevad monitoorimistööde ja piirangute lisamisega seotud tööde maksumus võib olla sõltuvalt veebilehe keerukusest üle 1000 euro. Iga lisanduva asutuse veebilehe lisandumine tähendab vanglateenistuse jaoks samasugust kulu. Tõenäoline on, et kui neid asutusi on palju, siis see kulu ka suureneb, kuna vajalike piirangute ülesleidmine (mida vaja kontrollida) läheb keerukamaks. Ka perioodiline täiendav kontroll oleks maksumuselt sama kulukas, sest selle automatiseerimiseks lahendusi ei ole.

Eeltoodud põhjendustele tuginevalt leian, et **VangS § 31[1] esimene lause**, mis sätestab, et kinnipeetaval ei ole lubatud kasutada internetti, välja arvatud vanglateenistuse poolt selleks kohandatud arvutites, mille kaudu on vanglateenistuse järelevalve all võimaldatud juurdepääs ametlikele õigusaktide andmebaasidele, kohtulahendite registrile, Riigikogu veebilehele ja õiguskantsleri veebilehele, **on põhiseadusega kooskõlas.**

Lugupidamisega

(allkirjastatud digitaalselt)

Lea Danilson-Järg
Minister

Signe Reinsalu
Signe.reinsalu@just.ee
Laura Glaase
Laura.Glaase@just.ee

[19] Vt Justiitsministeeriumi 24.05.2022 vastus nr 13-3/3365-2.
[1] Haldamise ja kontrollikulud, kui kasutusvõimalus on tund aega nädalas, juurdepääs piiramatu, kuid seaduse alusel täielikult kontrollitav.