

Riigikohus info@riigikohus.ee	Teie	27.03.2026	nr	5-26-16/3
	Meie	27.04.2026	nr	2-1-1/2026/2051

Arvamus põhiseaduslikkuse järelevalve asjas nr 5-26-16

Põhiseaduslikkuse järelevalve asjas nr 5-26-16 on Riigikohus esitanud Registrite ja Infosüsteemide Keskusele järgnevad küsimused:

- a) Kui vangistust kandev kinnipeetav saab juurdepääsu konkreetset teie hallata olevale veebilehele, siis milliseid reaalseid kuritarvitamise riske selline juurdepääs hõlmab, kui kinnipeetav sama veebilehe kaudu e-teenuseid kasutada ei saa?
Kas ja kuidas kontrollite samu veebilehti selleks, et ära hoida vabaduses olevate isikute poolseid kuritarvitusi (nt kolmandate isikute poolt lisatud suhtlusvõimalused)?
- b) Kas ja mida nimetatud asutused saavad teha selleks, et kuritarvitamise riske enda hallataval veebilehel vähendada või välistada? Milline oleks veebilehe haldaja selliste meetmete võtmise ühekordne ja seejärel regulaarne rahaline kulu ja milles see seisneks?

Registrite ja Infosüsteemide Keskus edastab küsimustele järgnevad vastused:

1. Registrite ja Infosüsteemide Keskus haldab menetlusega seotud veebilehtedest üksnes Justiits- ja Digiministeeriumi veebilehte¹. Nimetatud veebilehe puhul on tegemist klassikalise veebilehega, mis koondab kokku asutuse igapäevased uudised ja koondab teavet ministeeriumi vastutusalas olevatel teistel teemadel. Veebilehel on samuti lingid teistele veebilehtedele.
 - 1.1. Justiits- ja Digiministeeriumi veebileht koosneb mitmetest funktsionaalsustest, mille osas oleks vajalik otsus, kas ja millises osas on nendele juurdepääs Justiits- ja Digiministeeriumi veebilehelt võimaldatud. Nimetatud funktsionaalsused on näiteks:
 - 1.1.1. Hüperlingid sotsiaalmeedia platvormidele;
 - 1.1.2. Hüperlingid riigilikele töökeskkondadele, näiteks [Eelnõude infosüsteem](#);
 - 1.1.3. Hüperlingid andmekogudele, näiteks Justiits- ja Digiministeeriumi avalik dokumendiregister <https://adr.rik.ee/jm/>;
 - 1.1.4. Hüperlingid teistele riiklikele veebilehtedele, näiteks <https://minuraha.ee/et>, [Mis on korruptsioon? | Korruptsioon.ee](#), ;
 - 1.1.5. Hüperlingid statistika kohta eraettevõtete veebilehtedele, näiteks <https://public.tableau.com/app/profile/kriminaalpoliitika/viz/Narkoreoveeseire/Tarbitudannused>
 - 1.1.6. Hüperlingid avalik-õiguslike juriidiliste isikute veebilehtedele ning ministeeriumi haldusala asutuse veebilehtedele, näiteks [Notarite Koda](#), [Vanglateenistus](#), [Prokuratuur](#), [Kohtud](#), [Andmekaitse Inspeksioon](#), [Eesti Kohtuekspertiisi Instituut](#), [Registrite ja Infosüsteemide Keskus](#), [Patendiamet](#), [Konkurentsiamet](#), [Riigi Infosüsteemi Amet](#), [Riigi Info- ja Kommunikatsioonitehnoloogia Keskus](#), [Riigiside Sihtasutus](#), [Eesti Interneti Sihtasutus](#);
 - 1.1.7. Alamdomeenid <https://statistika.justdigi.ee/>, <https://rights.justdigi.ee/>.

¹ <https://www.justdigi.ee/>

- 1.2. Eeltoodut näidetest tulenevalt on oluline, millises ulatuses juurdepääsu võimaldamiseks räägitakse.
 - 1.2.1. Kui juurdepääs tuleb võimaldada kogu alamdomeeni <https://rights.justdigi.ee/> sisule, siis seasel lehel kuvatakse kasutajale YouTube videod. Täna on sisu lubamisel ja keelamisel kasutusel nn filtersüsteem², mis ei võimaldaks kuvada üksnes lehele mõeldud video, vaid juurdepääs tekiks kogu YouTube sisule.
 - 1.2.2. Loetletud funktsionaalsused on üksnes olukorra näitlikustamiseks ning ei sisalda kindlasti kõiki võimalike funktsionaalsusi ega viiteid, kuhu on Justiits- ja Digiministeeriumi lehelt võimalik liikuda. Kui ulatuse määramisel tuleb otsus, et mingi funktsionaalsus või viide peaks olema juurdepääsetav, siis see laiendab skooopi, milliste veebilehtede sisu tuleb üle kontrollida.
 - 1.3. Veebilehtede kaitsmisel lähtutakse infoturbe³ põhikomponentidest – konfidentsiaalsus, terviklus, käideldavus. Iga süsteemi või veebilehe puhul hinnatakse selle sisu eraldiseisvalt ja määratakse igale komponendile vastav kaitsetarve. Lisaks kasutatakse erinevaid teenuseid, et kaitsta veebilehti küberünnakute eest. Hetkel ei ole Registrate ja Infosüsteemidele teadaolevalt kolmandad isikud lisanud veebilehtedele funktsionaalsusi, mis lisaksid veebilehele suhtlusvõimalusi. Selle ärahoidmiseks monitooritakse veebilehti pidevalt ning vaadatakse, et veebilehtedele ei lisataks kolmandate isikute poolt funktsionaalsusi. Halduskohtu menetluses nr 3-23-187 toimunud istungil rääkisid Registrate ja Infosüsteemide Keskuse eksperdid sellest, kuidas juba veebilehe pidaja poolt loodud funktsionaalsusi on võimalik ära kasutada suhtluseks. Vabaduses viibivate isikute puhul ei kohaldu suhtlusele samad piirangud, mis kinnipeetavatele, mistõttu ei kasutata vabaduses viibivad isikud üldjuhul riiklike veebilehti omavaheliseks suhtluseks, vaid eelistatakse erinevaid suhtlusplatvorme. Kui on olemas õiguslik alus, siis on ka sellist suhtlust võimalik kontrollida logidest.
2. Kinnipeetavatele interneti juurdepääsu võimaldamisel kasutatakse kahte lähenemist – filtersüsteem ning kasutajale veebilehe/infosüsteemi kohandamine.
 - 2.1. Filtersüsteemi tehniline lahendus on ülesse ehitatud teatud veebilehtede põhjal ning toimib üksnes teatud maale, näiteks on see lihtsasti seadistav asutuse veebilehtedele, mis omavad üksnes informatiivset sisu. Juhtudel, kus on tegemist suuremate veebilehtedega või infosüsteemidega, siis filtrite seadistamine võib osutuda väga keeruliseks ja juba täna sisaldab murekohti, kuna puudub vajalik ressurss teha pidevat seiret kinnipeetavatele võimaldatud veebilehtede üle. Lisaks on eriti keeruline kontrollida veebilehti, mille sisu muutub dünaamiliselt (näiteks uudistevoog), kuna filtritega on keeruline tuvastada, kas tehtud on ebasobivaid muudatusi.
 - 2.2. Veebilehe/infosüsteemi kohandamine tähendab, et veebileht/infosüsteem teab ise, et tegemist on kasutajaga, kellele ei ole teatud funktsionaalsuste kasutamine lubatud. Sellise lähenemise puhul arvestatakse juba veebilehe/infosüsteemi loomisel, et on eraldi kasutajagrupp, kellele võimaldatakse sisule teistsugune juurdepääs. Näiteks avaliku e-toimiku puhul on kasutusel selline lahendus. Uute funktsionaalsuste loomisel arvestatakse avaliku e-toimiku puhul kohe sellega, et kas kinnipeetavate osas tuleb funktsionaalsuse osas teha erisus. Lahenduse puhul on kinnipeetavate võrgus e-toimiku ainult üks reegel, et kinnipeetav saab tahvelarvutist e-toimikkuse minna ning süsteemi kuritarvitamine on välistatud e-toimiku infosüsteemi poolt.
 - 2.3. Kokkuvõtvalt ei ole võimalik välja tuua ühte „õiget“ lähenemist kuritarvitamise riskide vähendamisel või välistamisel. Otsustuse tegemisel tuleb arvestada iga konkreetse veebilehe/infosüsteemi puhul eraldi, kaaludes seejuures veebilehe/infosüsteemi keerukust ning selles olevat sisu ja funktsionaalsusi.
 - 2.4. Rahalist kulu on antud juhul väga keeruline välja tuua, kuna olenevalt infosüsteemi/veebilehe keerukust võib see olla väga erinev. Lisaks mõjutab rahalist kulu

² Filtersüsteem – süsteem, millega seatakse veebilehele võrgutasandi reeglid.

³ Infoturbe eesmärk on kaitsta andmeid ja süsteeme (sh veebilehti) volitamata juurdepääsu, hävitamise, kasutamise või muutmise eest.

see, millist lähenemist veebilehtede/infosüsteemide kohandamisel kinnipeetavatele kasutatakse. Justiits- ja Digiministeeriumi veebilehe puhul sõltub rahaline kuluks sellest, milline on ulatus, millele tuleb kinnipeetavale juurdepääs tagada.

Lugupidamisega

/allkirjastatud digitaalselt/

Rivo Reitmann

Direktor

Koostajad: Vanglate infosüsteemide tiimi tiimijuht Jaanus Kirmet, peaarhitekt Oliver Orav, õigusteenuse tiimi jurist Merle Sirje Tael-Ibrahimli