JUSTIITS- JA DIGIMINISTEERIUM

Riigikohus
info@riigikohus.ee

Teie 09.10.2026 nr 5-26-39/3

Meie 03.11.2026 nr 10-3/7320

Vastus põhiseaduslikkuse järelevalve menetluses nr 5-26-39

Lugupeetud Riigikohtu esimees

Riigikohtu menetluses on haldusasjast nr 3-23-2107 võrsunud põhiseaduslikkuse järelevalve menetlus nr 5-26-39. Riigikohus palus hiljemalt 6.11.2026 esitada menetlusosalistel arvamus, kas põhiseadusega vastuolus olevaks tunnistatud regulatsioon oli haldusasja lahendamisel asjassepuutuv, milline on regulatsiooni seaduslik eesmärk ning kas see on proportsionaalne. Täiendavalt paluti Justiits- ja Digiministril ning Registrite ja Infosüsteemide Keskusel esitada vastused Riigikohtu küsimustele.

Leian, et vaidlusalused normid, s.o VangS § 31[1] esimene lause (alates 01.08.2019 kuni 31.03.2024 kehtinud redaktsioonis) ja VangS § 31[1] lõiked 1 ja 2 (alates 01.04.2024 kehtivas redaktsioonis) ning justiitsministri 30.11.2000 määruse nr 72 „Vangla sisekorraeeskiri“ § 52[1] lõike 1 (alates 17.08.2026 kehtivas redaktsioonis) on asjassepuutuvad ja konkreetne normikontroll lubatav.

Leian, et kinnipeetavate internetikasutusega seotud riskid, mida kirjeldasin viimati 24.04.2026 vastuses nr 10-3/2439 põhiseaduslikkuse järelevalve menetluses asjas nr 5-26-16, on asjakohased ka käesolevas asjas. Veebilehtede ringi järkjärguline laiendamine ei suurenda üksnes kinnipeetavate võimalusi oma põhiõigusi kasutada, vaid kasvatab paratamatult ka vangla julgeoleku, järelevalve ning vangistuse eesmärkide saavutamisega seotud riske. Mida ulatuslikum on lubatud veebikeskkondade ring, seda keerulisemaks muutub tagada, et internetti ei saaks kasutada vanglaväliste kontaktide loomiseks, õigusvastase tegevuse jätkamiseks või kuritegude ettevalmistamiseks ja koordineerimiseks. Riigikohtu 17.06.2026 otsusest nr 5-26-16 nähtub, et kinnipeetavale veebilehele juurdepääsu võimaldamise vajaduse hindamisel materiaalse põhiseaduspärasuse kontekstis on oluline arvestada nii veebilehe seost avaliku võimu tegevusega kui ka selle kaudu kättesaadava teabe sisu ja tähendust kinnipeetava põhiõiguste kasutamisel. Riigikohus on seejuures pidanud oluliseks eelkõige avaliku võimu tegevust ja riigi toimimist käsitleva teabe kättesaadavust ning selle tähtsust kinnipeetava taasühiskonnastamisel. Kuivõrd need põhjendused ei ole olemuslikult seotud üksnes avaliku sektori veebilehtedega, võib sama argumentatsioon teatud juhtudel olla kohaldatav ka eraõiguslike isikute hallatavatele veebikeskkondadele, mis vahendavad samalaadset teavet või täidavad võrreldavat funktsiooni. Seetõttu on veebilehtedele juurdepääsu võimaldamisel põhjendatud arvestada lisaks konkreetse veebilehe omadustele ka veebilehtede ringi laiendamise kumulatiivset mõju vangla julgeolekule ja kontrollimeetmete tõhususele.

Sellegipoolest tuleb arvestada, et Riigikohtu 17.06.2026 otsusega asjas nr 5-26-16 tunnistati VangS § 31[1] lg-d 1 ja 2 PSJKS § 15 lg 1 p 2 alusel põhiseadusega vastuolus olevaks ja kehtetuks.[1] Arvestades Riigikohtu 17.06.2026 otsuses sisalduvaid põhjendusi ja seda, et vaidlusalused sätted on alates tunnistatud 17.12.2026 kehtetuks, esitasin 21.09.2026 Riigikogule ettepaneku[2] muuta VangS § 31[1] sõnastust. Kuivõrd ettepaneku kohaselt võimaldataks kinnipeetavatele juurdepääs ka Eesti kohtute

[1] Vt otsuse resolutsiooni p 3. Tunnistada põhiseadusega vastuolus olevaks ja kehtetuks 1. aprillist 2024 kehtivad vangistusseaduse § 31[1] lg-d 1 ja 2. Lükata otsuse jõustumine selles osas edasi kuue kuu võrra.
[2] Kättesaadav: Eelnõud – Riigikogu

ametlikule veebilehele, kinnitab see hinnangut, et juurdepääsu võimaldamine sellele veebilehele on põhjendatud.

Arvestades esiteks, et asjassepuutuvad normid on tunnistatud põhiseadusega vastuolus olevaks ning Riigikohtu asjas nr 5-26-16 kujundatud loogikat, millistele tingimustele vastavatele veebilehtedele juurdepääsu keeldu ei ole peetud põhjendatuks, ja teiseks, et seadusandjale on tehtud ettepanek vaidlusalusele veebilehele juurdepääs lubada**, võivad asjassepuutuvad normid, milles need välistavad juurdepääsu kohtute veebilehele, osutuda põhiseadusega vastuolus olevaks ka käesolevas vaidluses.**

Järgnevalt esitan seisukohad (1) ja vastan Riigikohtu küsimustele (2).

1. Regulatsiooni asjassepuutuvus, seaduslik eesmärk ja proportsionaalsus

1.1. Normikontrolli lubatavus – vaidlustatud sätete asjassepuutuvas

Tallinna Ringkonnakohus arutas haldusasjas nr 3-23-2107 kaebaja apellatsioonkaebust Tallinna Halduskohtu otsusele, millega jäeti mh rahuldamata kaebaja taotlus saada juurdepääs maa-, haldus- ja ringkonnakohtute veebilehtedele ning taotlus tunnistada vangistusseaduse (VangS) § 31[1] põhiseadusega vastuolus olevaks. 2.10.2026. a otsusega tunnistas Tallinna Ringkonnakohus põhiseadusega vastuolus olevaks:

1. VangS § 31[1] esimese lause (alates 01.08.2019 kuni 31.03.2024 kehtinud redaktsioonis) osas, milles see välistas kinnises vanglas eelvangistust kandva vahistatu juurdepääsu maa-, haldus- ja ringkonnakohtute veebilehele;
2. VangS § 31[1] lõiked 1 ja 2 (alates 01.04.2024 kehtivas redaktsioonis) ning
3. justiitsministri 30.11.2000 määruse nr 72 „Vangla sisekorraeeskiri“ § 52[1] lõike 1 (alates 17.08.2026 kehtivas redaktsioonis) osas, milles need välistavad kinnises vanglas karistust kandva kinnipeetava juurdepääsu maa-, haldus- ja ringkonnakohtute veebilehele.

Vaidlusalused sätted:

4. VangS § 31[1] esimene lause kuni 31.03.2024 kehtinud redaktsioonis oli sõnastatud järgmiselt: *„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.“.*

5. Alates 1.04.2024. a kehtiva sõnastuse järgi sätestavad VangS § 31[1] lg-d 1 ja 2 järgmist:
   „(1) Kinnipeetaval ei ole lubatud kasutada internetti, välja arvatud turvalise tehnilise võimekuse olemasolu korral ja järelevalve all, vanglateenistuse poolt selleks kohandatud seadmetes lubatud veebilehele juurdepääsuks ning kinnipeetavale vajaliku teenuse või muu käesoleva seaduse eesmärkidega kooskõlas oleva internetilahenduse kasutamiseks.
   (2) Käesoleva paragrahvi lõikes 1 nimetatud veebilehtede loetelu ja interneti kaudu kinnipeetavale võimaldatavate vajalike teenuste ning internetilahenduste kasutamise tingimused, korra ja turvanõuded kehtestab valdkonna eest vastutav minister määrusega.“.

6. Justiitsministri 30.11.2000. a määruse nr 72 „Vangla sisekorraeeskiri“ (VskE) § 52[1] lg 1 (alates 17.08.2026 kehtivas redaktsioonis[3]) oli sõnastatud järgmiselt:
   „(1) Kinnipeetaval on õigus turvaliselt kohandatud vangla seadme (edaspidi käesolevas peatükis seade) kaudu juurde pääseda järgmistele veebilehtedele:
   1) Eesti ja Euroopa Liidu ametlike õigusaktide andmebaaside veebilehed;
   2) Eesti, Euroopa Inimõiguste Kohtu ja Euroopa Liidu kohtulahendite veebilehed;
   3) Riigikogu veebileht;
   4) Riigikohtu veebileht;
   5) õiguskantsleri veebileht;

[3] Alates 18.10.2026 on juurdepääs tagatud lisaks Justiits- ja Digiministeeriumi, Maksu- ja Tolliameti, Politsei- ja Piirivalveameti ja Eesti teabevärava veebilehtedele.

6) Ametlike Teadaannete veebileht;
7) tõlkerakenduse veebileht;
8) Eesti Rahvusringhäälingu uudisteportaali tekstiosa;
[---]
13) Rootsi avalik-õigusliku ringhäälingu Sveriges Television (SVT) uudisteportaal.“.

Sätete asjassepuutuvus

7. 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.[4] Norm peab seejuures olema kohtuasja lahendamisel otsustava tähtsusega.[5] Norm on otsustava tähtsusega siis, kui kohus peaks asja lahendades normi põhiseadusvastasuse korral otsustama teisiti kui normi põhiseaduspärasuse korral.[6]

8. Norm on asjassepuutuv, kui selle kehtetuse tõttu oleks võimalik teha teistsugune otsus. Vaidlusalused normid välistavad juurdepääsu veebilehtedele, millele kaebaja praeguses asjas ligipääsu soovib. Veebilehed, millele kaebaja juurdepääsu soovib, ei kuulu ka sätetes nimetatud erandi alla. Seega sõltub kohtuasja lahendamine sellest, kas VangS § 31^1 esimeses lauses (kuni 31.03.2024. a kehtinud redaktsioonis), VangS § 31^1 lg 1 esimeses lauses (alates 01.04.2024. a kehtivas redaktsioonis) ning VskE § 52^1 lg-s 1 (alates 17.08.2026-17.10.2026 kehtinud redaktsioonis) sätestatud interneti kasutamise keeld on (vaidlusaluses osas) põhiseadusega kooskõlas või mitte. Kaebuse saab rahuldada üksnes juhul, kui kõnealune keeld on põhiseadusega vastuolus ja seda sisaldav norm tunnistatakse kehtetuks, vastasel juhul tuleb kaebused jätta rahuldamata. Seetõttu on VangS § 31^1 esimene lause (kuni 31.03.2024 kehtinud redaktsioonis), VangS § 31^1 lg 1 esimene lause (alates 01.04.2024 kehtivas redaktsioonis) ja VskE § 52^1 lg 1 (17.08.2026-17.10.2026 kehtinud redaktsioonis) asjassepuutuvad normid ja seega on põhiseaduslikkuse järelevalve lubatav.

1.2. Piiratav põhiõigus ja selle riive

9. Nii VangS § 31^1 esimeses lauses (kuni 31.03.2024 kehtinud sõnastuses) sätestatud keeld, VangS § 31^1 lg 1 (alates 01.04.2024 kehtivas sõnastuses) ja VskE § 52^2 lõikes 1 sätestatud keeld piirasid või piiravad (interneti vahendusel) ligipääsu üldiseks kasutamiseks mõeldud teabele, millele ligipääsu õigus on tagatud põhiseaduses. Kuigi vaidlusalused sätted võivad oma sisult teataval määral erineda, viisid need konkreetsetes asjaoludes samasisulise piiranguni, s.t välistasid kaebaja taotletud veebilehele juurdepääsu, mistõttu puudub alus neid põhiõiguse riive analüüsimisel eristada. Seetõttu kohalduvad järgnevad põhjendused ühtviisi kõigi vaidlusaluste sätete suhtes.

10. Vaidlusalustes normides sätestatud keeld www.kohus.ee veebilehele juurdepääsuks piirab (interneti vahendusel) ligipääsu üldiseks kasutamiseks mõeldud teabele, millele ligipääsu õigus on tagatud põhiseaduses.

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

12. 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.

[4] RKPJKo 02.12.2002, 3-4-1-11-02, p 13
[5] RKÜKo 22.12.2000, 3-4-1-10-20, p 10
[6] RKPJKo 02.12.2002, 3-4-1-11-02, p 15

13. 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 vanglat jäävate isikute turvalisus) ja laiemalt põhiseadusliku väärtusena riigi sisemine rahu.[7] 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.

14. 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. 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. Kuigi praegu on vaidluse all kohtute veebileht, kehtiksid sarnased riskid ka teiste riigiasutuste veebilehtede puhul. Nt riigiasutuste puhul VVS § 38 tähenduses veel lisaks u 150 veebilehte), mis tähendaks 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.

15. Kinnipeetavate internetile ligipääsu laiendamise küsimuses, sh julgeoleku- ja turvariskidega seonduva osas jään Riigikohtule 24.04.2026 asjas nr 5-26-16 esitatud seisukohtade juurde. Kuivõrd nimetatud vastuses sisaldub nii teave piirangutega seotud ressursikulude kohta kui ka teave interneti kasutamisega seotud riskide kohta, siis on neis sisalduvaid põhjendused asjakohased ka praegu.

1.3. Kinnipeetavatele veebilehtede lubamisega seotud riskid

16. Õiguste riive põhiseaduspärasuse hindamisel, eelkõige hindamisel, kas piirang on mõõdukas, on asjakohane võtta arvesse riske, mis kaasneksid vaidlusalustele veebilehtedele juurdepääsu võimaldamisega. Seetõttu selgitan neid täpsemalt käesolevas vastuses.

17. Reeglina võib tõepoolest väita, et ühiskonna turvalisust ei kahjusta see, et kinnipeetavale on kättesaadav avalikuks kasutamiseks mõeldud teave, mida riigiasutused jagavad oma tegevuse kohta. Samas tuleb arvestada asjaoluga, et piirangu seadmisel ei ole lähtutud mitte konkreetse riigiasutuse poolt avaldatava infoga seonduvatest riskidest, vaid teistest kaalutlustest, eeskätt seoses sellega, millised on ohud veebilehtede mitteotstarbelisel kasutamisel. Samuti märgin, 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

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

täiendavalt ligikaudu 150 veebilehte, kuid lehti võib olla ka rohkem (nt juhul, kui ühelt veebilehelt avanevad teised alamlehed).

18. 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, Ettevõtluse ja Innovatsiooni 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 Justiits- ja digiministeeriumi 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[8], märgukirja või selgitustaotluse esitamise elektroonne vorm, mis sageli annab ka võimaluse saata suvalisele meiliaadressile pöördumise koopia[9]. 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 olemas Riigi Teataja veebilehe kohta. Justiits- ja Digiministeerium 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.

21. Sarnaseid näiteid on tuua ka hilisemast vanglate praktikast. Nt on Justiits- ja Digiministeerium kirjeldanud haldusasjas nr 3-23-187 esitatud vastuses nr 13-3/2861-3 (25.04.2025, p 38 jj) vangi portaaliga seotud väärkasutusi, st juhtumeid, kus kinnipeetavad hakkasid kasutama sisselogimiseks teiste kinnipeetavate nimesilte, kus peal on ka foto või teisi fotosid. See võimaldas teha teise kinnipeetava nimel erinevaid toiminguid, nt esitada kaebusi, samuti võimaldas see jätta teisele kinnipeetavale mustanddokumendi kaudu erinevaid teateid, st

[8] 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
[9] 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.

suhelda varjatud viisil. Kinnipeetavad kasutasid omavahel suhtlemiseks süsteemis loodavate dokumentide mustandeid (*draft*). Nt üks kinnipeetav koostas teksti kas pöördumise tegemiseks või vangla e-poe tagasiside funktsioonis, kuid ei saatnud seda ära. Pärast seda logis kaaskinnipeetav tema pildi, isikukoodi ja parooli abil VAPOsse sisse ja nägi teise kinnipeetava koostatud mustandeid.

22. Samuti on näiteid avaliku e-toiminu (AET-i) väärkasutusest. Eelmises punktis viidatud vastuses (p 40) kirjeldati AETi kasutamisega ilmnenud mitut probleemi. AETis on nimelt võimalik saada suhelda nii vanglaväliselt kui vanglasiseselt, sh näha erinevaid dokumente, lisatud audio või videofaile ja muud teavet, peamisel kahel viisil. Näiteks kui keegi esitab AET-is menetlusse uue asja nii, et tema ise on kinnipeetava esindaja ja kinnipeetav on taotleja rollis, saab kogu selle asja kaudu esitatud teave viimasele kättesaadavaks. Sama tulemus on võimalik saavutada ka teistpidi, st kui vabaduses olev isik on ise taotleja ja kinnipeetav on tema esindaja. Suhtluspiirangutega isikutel seda võimalust ei ole, nendele on kõik dokumendid automaatselt nähtamatuks tehtud, kuid nende kinnipeetavate puhul, kellel suhtluspiiranguid ei ole, seda piiratud ei ole.

23. 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.

24. 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 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.

25. 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.

26. 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 tegemise 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 Justiits- ja Digiministeeriumil, Registrite ja Infosüsteemide Keskusel (RIK) ega RIT-il. Osadel juhtudel on veebilehtede omanikud ka väljaspool Eestit, mis teeb selle info haldamise eriti keeruliseks.

27. 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 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 eesmärkidega.

28. 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.[10] 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).

29. 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 vangistust reguleerivatest õigusaktidest, 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 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

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

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[11] 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.

30. 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. Justiits- ja Digiministeeriumil 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.

31. Veebilehtedega seotud riskide hindamine võib oluliselt erineda sõltuvalt keskkonna keerukusest ja mahust. Kuigi mõnede veebikeskkondade puhul on teave muudatuste kohta selgelt hallatud ja hõlpsasti kättesaadav, esineb sageli ka olukordi, kus veebilehtede struktuur on mahukas ja killustunud. Sellistel juhtudel tuleb teostada põhjalik seire, sealhulgas kontrollida, millistes domeenides erinevad lehe osad paiknevad, hinnata kõiki suhtlusvõimalusi ning analüüsida kõiki linke, kuhu kasutajaid suunatakse. Lisaks tuleb üle vaadata lehtedele integreeritud multimeedia (nt videostriimid), hinnata nende sobivust ning otsustada, milline sisu on lubatav ja milline mitte. Sellele järgneb tehniliste piirangute rakendamine (nt blokeeringud) ning nende toimivuse kontrollimine. Kogu selline terviklik riskihindamise ja kontrolli protsess võib nõuda märkimisväärset ajakulu, ulatudes kokku mitme tööpäevani. 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 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.

32. Kuivõrd iga lisanduva veebilehe kulud kumuleeruvad, siis on Justiits- ja Digiministeerium toonud välja kuluarvestuse ka sellest lähtuvalt.[12] Justiits- ja Digiministeerium on hinnanud veebilehtede kontrollimiseks, mis võimaldaks tagada veebilehtede põhjalikumaks (kuid mitte täielikuks) kontrollimiseks vajalikud võimalused[13], ressursikulu järgmiselt: 1) kinnipeetavate tegevuse ja veebilehtede muudatuste jälgimisele kuluv monitoorimissüsteem 330 000 eurot arenduseks (s.o ühekordne kulu), millele lisandub vangla tööjõukulu 190 080 eurot aastas ning lisaks RIK-i tööjõukulu aastas 79 200 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) Kulud, mis kaasnevad iga uue veebilehe seadistamisega. Ühe veebilehega seotud järjepidevate tööde maksumus võib olla väga varieeruv, sõltuvalt veebilehe keerukusest kuid keskmiselt hinnatavalt u 3000–8000 eurot. 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.

33. Kuivõrd iga lisanduva veebilehe kulud kumuleeruvad, siis on Justiits- ja Digiministeerium toonud välja kuluarvestuse ka sellest lähtuvalt. 30.10.2022 vastuses nr 10-3/6915 selgitati, et

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

[12] Vt ka Justiitsministeeriumi 24.05.2022 vastus nr 13-3/3365-2.

[13] Haldamise ja kontrollikulud, kui kasutusvõimalus on tund aega nädalas, juurdepääs piiramatu, kuid seaduse alusel täielikult kontrollitav.

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. Mis puudutab seda, kui sageli praegu kontrollitakse, kas filter töötab nõuetekohaselt, ja seda, millised on selle ülesande täitmisega praegu kaasnevad kulud, märgin, et pole välistatud, et olemasolevate veebilehtede puhul on juba või tekivad tulevikus turvariskid, millest vanglateenistus ei ole teadlik. Igapäevast seiret selle üle teha ei ole mõistlik, kuivõrd see tähendaks pidevat halduskulu, mis saaks tulla üksnes arendustegevuste arvelt.

34. Nagu eelnevalt selgitatud, eeldab veebilehtede turvaline kasutamine vanglakeskkonnas pidevat tehnilist seiret ning märkimisväärset tööjõu- ja rahalist ressurssi. Iga lisanduv veebileht suurendab püsivalt kontrolli- ja halduskoormust, mistõttu võib veebilehtede arvu ja tehnilise keerukuse kasvades osutuda võimatuks nõutava turvalisuse taseme tagamine. Vanglateenistus peab kasutama oma piiratud ressursse eesmärgipäraselt, seadmata ohtu põhiülesannete täitmist. Seetõttu ei saa pidada põhjendatuks veebilehtedele juurdepääsu piiramatut laiendamist, kui sellega kaasnev ressursikulu muutub ebaproportsionaalseks. Veebilehtedele juurdepääsu võimaldamise ulatuse määramisel tuleb seega arvestada nii julgeolekuriskide kui ka vanglateenistuse tegeliku võimekusega tagada nende üle tõhus kontroll.

1.4. Riive põhiseaduspärasus

35. VangS § 31[1] kuni 31.03.2024 kehtinud redaktsiooni esimese lause põhiseaduspärasuse kohta on justiitsminister varem esitanud arvamused Riigikohtule 30.10.2022 vastuses nr 10-3/6915 (kättesaadav dokumendiregistris: Justiits- ja Digiministeeriumi avalik dokumendiregister) ja 24.04.2026 vastuses nr 10-3/2439: Justiits- ja Digiministeeriumi avalik dokumendiregister. Kinnipeetavate interneti kasutamisega seotud riskide osas jään ka käesolevas menetluses samade põhjenduste juurde ja palun neid käsitleda justiits- ja digiministri seisukohtadena käesolevas menetluses. Kuigi nimetatud asjades oli vaidluse all juurdepääsu võimaldamine Riigikohtu, Ametlike Teadaannete, Justiits- ja Digiministeeriumi, Maksu- ja Tolliameti, Politsei- ja Piirivalveameti ja eesti.ee veebilehele, ei erine piirangu sobivust ja vajalikkust puudutavad põhjendused olemuslikult praegu lahendamisel oleva veebilehe piirangu põhjendustest. Nimetatud vastustes selgitati, 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. 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.

36. Riigikohus on asjas nt 3-18-477 vaidlusaluse sätte osas hinnanud piiranguid sobivaks ja vajalikuks (otsuse p 78). Samuti on Riigikohus pidanud sobivaks ja vajalikuks meetmeks juurdepääsu piiramist neljale veebilehele, mis olid vaidluse all asjas 5-26-16. Nimetatud otsuses (p 74) leidis Riigikohus, et piirang on sobiv ja vajalik ühiskondliku turvalisuse - nii vangla julgeoleku kui ka väljaspoole vanglat jäävate isikute turvalisuse - ja riigi sisemise rahu tagamiseks. Välistades ligipääsu vaidlusalustele veebilehtedele, välistab see ühtlasi vanglateenistuse kontrolli alt välja jääva vanglavälise suhtluse. Veebilehel suhtlusvõimaluste piiramine (veebilehe esmane audit ja seadistamine ning hilisem järelevalve) oleks kulukam, kui seda on veebilehele ligipääsu täielik keelamine. Seda isegi juhul, kui sama teabe muul viisil küsimisega kaasneksid samuti tööjõu- ja materjalikulud jms. Kulud kaasneksid ka sellega, kui kinnipeetav peaks soovitud veebilehele ligipääsuks esitama taotluse ning vanglateenistus otsustab ligipääsu üle kaalutlusõiguse alusel. Kuigi Rahvusarhiivi DIGAR-i teenuse kasutamine võib olla tasuta, ei pruugi selle teenuse kasutamine olla iga veebilehe puhul sobiv lahendus. Põhiõigust vähem riivates ei ole ilmselt võimalik saavutada eespool nimetatud legitiimset eesmärki sama efektiivselt kui juurdepääsu keelamisega (vt ka viidatud 3-18-477, p 78). Praeguses asjas vaidluse all oleva veebilehe puhul on võimalikud realiseeruvad riskid samad, millele Justiitsministeerium tugines 30.10.2022. a haldusasja 3-18-477 raames Riigikohtule esitatud seisukohades ja mille toon välja ka käesolevas vastuses. Seetõttu leian, et ka praegusel juhul on vaidlusaluse veebilehe osas piirang materiaalses mõttes sobiv ja vajalik.

37. 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.[14] Asjas nr 5-26-16 on Riigikohus leidnud, et VangS § 31¹ lg-d 1 ja 2 ei vasta volitusnormilt nõutavale määratuse ega seadusereservatsiooni tingimusele. Volitusnormi piirid, mõte ja eesmärk on praegusel juhul sõnastatud vaid riigi huvidest lähtudes, arvestamata põhiõiguste kaitse vajadust. VangS § 31¹ lg 1 näeb ette interneti kasutamise keelu, v.a „turvalise tehnilise võimekuse olemasolu korral ja järelevalve all, vanglateenistuse poolt selleks kohandatud seadmetes lubatud veebilehele juurdepääsuks [---]". VangS § 31¹ lg 2 annab justiits- ja digiministrile õiguse kehtestada määrusega muu hulgas lg-s 1 nimetatud veebilehtede loetelu, samuti internetilahenduste kasutamise tingimused, korra ja turvanõuded. Nii on ministril „turvalise tehnilise suutlikkuse puudumisel" ja muude VangS § 31¹ lg-s 1 nimetatud tingimuste puudumise korral - mille ta on ise enne kehtestanud - võimalik keelata internetile juurdepääs täielikult. Kuigi seadus ei pea sätestama konkreetsete veebilehtede loetelu, ei saa seadusandja delegeerida täitevvõimule täielikku õigust otsustada selle üle, kas üldse ja mil määral põhiõigused tagatakse (vt ka RKÜKo 03.12.2007, 3-3-1-41-06, p 22; RKPJKo 17.12.2019, 5-19-40, p 50). Täielik keeld oleks vastuolus Riigikohtu lahenditega, kus on juba peetud teatud veebilehtedele juurdepääsu puudumist põhiseadusega vastuolus olevaks (RKHKo 31.05.2007, 3-3-1-20-07; RKÜKo 15.02.2023, 3-18-477). Absoluutne keeld võib olla vastuolus ka EIK praktikaga (vt p-d 51-52). Asjaolu, et kehtiva VSkE § 52¹ lg 1 loetelu sisaldab veebilehti, mis olid nimetatud VangS § 31¹ v.r. esimeses lauses, ega halvenda seega kinnipeetavate olukorda võrreldes 1. aprillile 2024 eelnenud ajaga, ei muuda põhiseadusvastast volitusnormi põhiseaduspäraseks. Neile põhjendustele tuginedes tunnistas kolleegium VangS § 31¹ lg-d 1 ja 2 PSJKS § 15 lg 1 p 2 alusel põhiseadusega vastuolus olevaks ja kehtetuks. Seega, arvestades, et veebilehele juurdepääsu piiramist võimaldanud normid on tunnistatud kehtetuks ning samad normid on asjassepuutuvad ka käesolevas menetluses, on sama Riigikohtu otsuses kirjeldatud põhjendused asjakohased ka praegu.

38. 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.[15] 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.

39. VangS § 31¹ lõike 1 esimeses lauses sätestatud sisulise piirangu laiem eesmärk oli tagada ühiskonna turvalisus (sh vangla julgeolek) ning õiguskorra kaitse. Kitsamas mõttes oli piirangu eesmärk tagada, et süüdimõistetu ei paneks karistuse kandmise ajal toime uut kuritegu. Seda eesmärki teenis ka sama sätte teine lause, mille eesmärk oli välistada kinnipeetava elektrooniline suhtlemine, mis väljub vanglateenistuse kontrolli alt ja mis oleks vastuolus VangS § 28 lõikes 3 sätestatuga.

40. 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.

41. Veebilehtedele juurdepääsu võimaldamisel lähtuti VangS § 31[1] (kuni 31.03.2024 redaktsioonis) 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.[16] 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 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[17]

[14] RKPJKo nr 3-4-1-5-05, p 8, https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-5-05
[15] 3-2-1-73-04, p 36.
[16] n 01.08.2019 kuni 31.03.2024 kehtinud redaktsioon.
[17] Vangistusseaduse muutmise seadus 680 SE, eelnõu ja seletuskiri arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8f08bcf8-2b6b-4017-b64c-6eea9c00a98c

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 lähtuti 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.

42. Alates 1.04.2024 kehtima hakanud VangS § 31^1 lg 1 redaktsioonis on sätestatud, et kinnipeetaval ei ole lubatud kasutada internetti, välja arvatud turvalise tehnilise võimekuse olemasolu korral ja järelevalve all, vanglateenistuse poolt selleks kohandatud seadmetes lubatud veebilehele juurdepääsuks ning kinnipeetavale vajaliku teenuse või muu käesoleva seaduse eesmärkidega kooskõlas oleva internetilahenduse kasutamiseks. Lõike 2 kohaselt kehtestab lõikes 1 nimetatud veebilehtede loetelu ja interneti kaudu kinnipeetavale võimaldatavate vajalike teenuste ning internetilahenduste kasutamise tingimused, korra ja turvanõuded valdkonna eest vastutav minister määrusega.[18] Interneti kasutamisega seonduvad üksikasjad reguleeriti ministri määrusega, kuna määruse tasandil sätestatud regulatsioon võimaldab muutunud oludele operatiivselt reageerida ning interneti kasutamise võimalusi ja korda vastavalt vajadusele muuta. Justiitsministri 30.11.2000. a määruse nr 72 „Vangla sisekorraeeskiri“ 51^1 lõike 2 järgi on kinnipeetaval keelatud juurdepääs veebilehe osale, mis võimaldab elektroonilist suhtlemist.

43. 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.[19] EIK 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. EIK 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.[20] Ka Eesti kohtupraktikas on leitud, et riivet õigustasid põhiseaduse preambulis väljendatud väärtused, nagu sisemise rahu kaitse. Keelu eesmärgina nägi Riigikohtu üldkogu vajadust kaitsta ühiskonna turvalisust - nii julgeolekut vanglas kui ka ühiskonna turvalisust väljaspool vanglat, mh karistuse eesmärkide täitmise soodustamise teel.[21] Eeltoodut arvestades on piirangu eesmärk legitiimne.

[18] Vangistusseaduse ja teiste seaduste muutmise seadus (vangistusseaduse kaasajastamine ja digilahenduste kasutusele võtmine)-Riigi Teataja, RT I, 22.03.2024, 1.
[19] Vt ka Vangistusseadus. Kommenteeritud väljaanne, Sootak. J., Juura, 2014, § 2^1 kommentaar, p 1,2, lk 94.
[20] 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
[21] https://rikos.rik.ee/LahendiOtsingEriVaade?asjaNr=3-3-1-5-09 p 34

44. Sobiv on abinõu, mis soodustab eesmärgi saavutamist. Sobivuse seisukohalt on vaieldamatult ebaproportsionaalne abinõu, mis ühelgi juhul ei soodusta piirangu eesmärgi saavutamist.[22] Vaidlusaluste sätetega välistatakse juurdepääs kohtute veebilehele. Seetõttu on välistatud, et kinnipeetavatel oleks võimalik vaidlusaluse veebilehe 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.

45. 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.

46. Nagu eespool öeldud, on Riigikohus on hinnanud[23] asja nr 3-18-477 raames VangS § 31^1 lõike 1 põhiseaduspärasuse kontrolli käigus piirangu sobivust ja vajalikkust ning leidnud, et VangS § 31^1 (esimeses lauses) sätestatud interneti kasutamise keeld on eesmärkide saavutamiseks sobiv ja vajalik. Sama on Riigikohus leidnud vaidlusaluste sätete kontrollimisega 17.06.2026 otsuses asjas nr 5-26-16. See seisukoht on asjakohane ka praegu, kuivõrd VangS § 31^1 (esimene lause) välistas ligipääsu vaidlusalustele veebilehtedele, välistades seeläbi ühtlasi vanglateenistuse kontrolli alt välja jääva vanglavälise suhtluse.

47. Abinõu mõõdukuse üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusesse sekkumise ulatust ja intensiivsust, teiselt poolt aga riive eesmärgi tähtsust.[24] Kaalumine eeldab kokkuvõttes võimalikult kõigi poolt- ja vastuargumentide nimetamist ja kohtu seisukohavõttu.[25] Olukorras, kus kinnipeetavatel ei ole juurdepääsu kohtute veebilehele, saab kirjeldada veebilehega seotud võimalikke riske. Samas on asjakohane välja tuua kõik riskid, mis juba lubatud veebilehtede ja rakenduste kasutamisel on realiseerunud. Osa neist leidis kajastust ja on kirjeldatud ka meediaväljaannetes.[26] Tõin eelnevalt välja täiendavate veebilehtede lubamisega seotud riskid, mis kehtivad üldiselt iga täiendava veebilehe puhul, ja kulutused, mida tuleb kanda järjest lisanduvate veebilehtede puhul. Samuti tõin näited, kus kinnipeetavad on kuritarvitanud neile lubatud juurdepääsusid seoses vangi portaali ja e-toimiku kasutamisega.

48. Samuti on riive mõõdukuse hindamisel oluline, et kinnipeetaval on võimalik saada üldiseks kasutamiseks mõeldud informatsiooni teabenõudega. 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.

49. Mõõdukuse hindamisel on määrav, kas isikule jääb vaatamata piirangule alles tegelik võimalus oma põhiõigust mõistlikus ulatuses teostada. Käesoleval juhul ei ole kinnipeetav täielikult ilma jäetud informatsiooni saamise võimalusest, vaid tal on võimalik kasutada muid, kontrollitud teabeallikaid (nt trükimeedia, vangla kaudu vahendatud info, piiratud ligipääsuga keskkonnad). Seega ei kõrvalda piirang põhiõigust tervikuna, vaid piirab selle teostamise viisi. Samal ajal

[22] PS kommenteeritud väljaanne; § 11, komm 10.
[23] Vt otsuse p 78, 3-18-477/73
[24] RKÜKo 3-4-1-7-01, p 21.
[25] PS kommenteeritud väljaanne; § 11 komm 17.
[26] Vt nt Õhtulehes 18.02.2025 avaldatud artiklid: VIDEO | Bardakk vanglate e-süsteemis: vangid vahivad pornot ja peavad keelatud suhtlust, JUHTKIRI | Virtuaalselt vangist väljas.

oleks vähem piiravate meetmete rakendamine (nt üksikute veebilehtede osaline lubamine või selektiivne filtreerimine) seotud märkimisväärse tehnilise ja ressursilise koormusega ning ei võimaldaks piisava kindlusega välistada kontrollimatut andmesidet, arvestades veebikeskkondade dünaamilist ja muutuvat iseloomu. Selline lahendus ei tagaks vanglateenistusele pandud kohustuse täitmist ning jätaks püsiva turvariski. Eeltoodut arvestades kaalub vangla julgeoleku ja kontrollimatu suhtluse välistamise eesmärk antud juhul üles informatsioonile ligipääsu piirangu, sest piirang ei välista informatsiooni saamist tervikuna, samas ei ole alternatiivsed vähem riivavad meetmed ei ole piisavalt tõhusad ning turvariskide realiseerumine kahjustaks oluliselt kaitstavaid õigushüvesid.

50. Sellegipoolest, arvestades Riigikohtu asjas nr 5-26-16 väljendatud seisukohti ning asjaolu, et Riigikogule on tehtud ettepanek võimaldada kinnipeetavatele juurdepääs ka Eesti kohtute ametlikule veebilehele, ei saa välistada, et vaidlusalusele veebilehele juurdepääsu jätkuv piiramine ei pruugi enam olla mõõdukas. Selline järeldus tugineb eelkõige Riigikohtu viidatud lahendis esitatud põhjendustele, kuivõrd sarnased kaalutlused võivad olla asjakohased ka Eesti kohtute veebilehele juurdepääsu piiramise õiguspärasuse hindamisel.

2. Vastused Riigikohtu küsimustele

a) Kui võimaldada kinnipeetavale juurdepääs kohtute veebilehele, siis milliseid kuritarvitamise riske selline juurdepääs endas kätkeb?

IT-turbe ja vangla julgeoleku seisukohast ei saa veebilehele juurdepääsu hindamisel lähtuda üksnes sellest, kas veebileht sisaldab otseseid suhtlusfunktsioone. Riskianalüüs peab hõlmama ka veebilehe tehnilist arhitektuuri, selle kaudu kättesaadavaid seotud infosüsteeme ning võimalust, et veebikeskkonna funktsionaalsus aja jooksul muutub. Arvestada tuleb nn kaudse sidekanali riskiga. Kuigi veebileht ise ei ole mõeldud kasutajate vaheliseks suhtluseks, sisaldab see kontaktandmeid, tagasisidevorme ning viiteid teistele e-teenustele. Selliste funktsioonide olemasolu võib võimaldada teabe edastamist väljapoole vanglat või luua alternatiivseid suhtlusvõimalusi. IT-turbe vaates ei ole määrav üksnes see, kas veebilehel on olemas erinevaid sõnumivahetuse vorme või ka nt e-posti kasutuse võimalus, vaid laiem küsimus, kas kasutaja saab veebikeskkonna kaudu algatada kontrollivälist infovahetust.

Risk kaasneb ka veebilehe kaudu teiste infosüsteemideni jõudmisega. Veebileht toimib väravana mitmetesse riigi infosüsteemidesse ning sisaldab arvukalt väljuvaid linke. Isegi juhul, kui konkreetne veebileht on staatilise sisuga, tuleb tehniliselt tagada, et kasutaja ei saaks selle kaudu liikuda keskkondadesse, kus on võimalik andmeid sisestada, dokumente üles laadida, teha päringuid või kasutada autentimist nõudvaid teenuseid. Praktikas tähendab see vajadust rakendada veebiliikluse filtreerimist, URL-põhiseid piiranguid ning pidevat seiret, kuna veebilehtede struktuur ja lingid võivad ajas muutuda.

Lisaks tuleb arvestada dünaamilise veebisisu riskiga. Kaasaegsed veebilehed ei koosne üksnes staatilistest HTML-lehtedest, vaid kasutavad sageli väliseid skripte, sisuhaldusplatvorme, manustatud rakendusi ja kolmandate osapoolte teenuseid. Seetõttu ei pruugi veebilehe tegelik funktsionaalsus piirduda esmapilgul nähtava sisuga. Iga täiendav tehniline komponent suurendab vajadust kontrollida, milliseid andmeid veebileht laadib, milliste serveritega ühendust võtab ning kas veebikeskkonnas võivad tulevikus tekkida täiendavad interaktiivsed funktsioonid.

Kaasaegsete veebikeskkondade funktsionaalsus muutub pidevalt ning vanglal puudub võimalus tagada, et veebilehele ei lisandu tulevikus uusi funktsioone, väliseid teenuseid või muid lahendusi, mis võimaldavad kasutajapoolset sisestust, dokumentide edastamist või suhtlust. Seetõttu eeldab iga veebilehe lubamine selle pidevat tehnilist seiret ja ümberhindamist, et tagada veebikeskkonna vastavus vangla julgeolekunõuetele. Vastasel juhul võib algselt lubatud veebileht omandada omadusi, mille tõttu ei oleks sellele juurdepääsu võimaldamine enam kooskõlas nende julgeolekukaalutlustega, millele tuginedes ligipääs algselt anti.

Nagu ka eespool kirjeldasin, tuleb arvestada kumulatiivse riskiga. Ühe veebilehe eraldiseisev risk võib olla väike, kuid olukorras, kus kinnipeetavatele tehakse järjest suurem hulk veebilehti kättesaadavaks, suureneb veebikeskkondade kogumahust tulenev ründe- ja kuritarvituspind. Iga täiendav veebileht eeldab eraldi tehnilist analüüsi, pidevat monitooringut ning kontrolli selle üle, et veebikeskkond ei võimaldaks mööduda vangla internetikasutuse piirangutest. Seetõttu ei pruugi küsimus seisneda üksnes vaidlusaluses veebilehes, vaid laiemalt selles, millised tagajärjed kaasnevad põhimõttega, et

juurdepääs tuleb võimaldada kõigile veebilehtedele, mis sisaldavad põhiõiguste teostamiseks vajalikku teavet. Sellest tulenevalt võib järeldada, et veebilehele www.kohus.ee ligipääsu hindamisel ei ole keskne üksnes selle sisuline eesmärk või seal avaldatava teabe laad. Sama oluline on hinnata veebilehe tehnilisi omadusi, selle seoseid teiste infosüsteemidega, võimalikke tulevikuarendusi ning veebipääsu laiendamise kumulatiivset mõju vangla küberturvalisusele, järelevalve tõhususele ja vangistuse täideviimise eesmärkide saavutamisele.

b) Kas ja mida saate teha selleks, et neid kuritarvitamise riske kohtute veebilehel vähendada või välistada?

Veebilehe kasutamisega seotud riske on võimalik vähendada erinevate tehniliste ja korralduslike meetmete rakendamise kaudu. Eelkõige saab vanglateenistus piirata juurdepääsu üksnes veebilehe kindlaksmääratud alamlehtedele, blokeerida väliseid linke ja ümbersuunamisi, keelata failide allalaadimise ning takistada ligipääsu veebilehe interaktiivsetele funktsioonidele. Samuti on võimalik kasutada veebiliikluse filtreerimist, logimist ja järelevalvemeetmeid, mis võimaldavad tuvastada kõrvalekaldeid lubatud kasutusviisidest. Kuigi veebilehe kasutamisega seotud riske on võimalik tehniliste ja korralduslike meetmetega olulisel määral vähendada, ei ole neid võimalik täielikult kõrvaldada. Samas eeldab selline lähenemine pidevat haldus- ja tehnilist kontrolli, et tagada veebilehe vastavus vangla julgeolekunõuetele.

Veebilehe edasise arendamise ja haldamise käigus tuleb arvestada asjaoluga, et veebikeskkond võib olla kättesaadav ka kinnipeetavatele vanglate kontrollitud internetikasutuse lahenduse kaudu. Sellest tulenevalt peavad veebilahenduse arhitektuur, funktsionaalsus ja tehnilised komponendid olema kavandatud viisil, mis ei võimalda kinnipeetavatel luua kontrollimatuid sidekanaleid, algatada interaktiivset suhtlust väliste isikute või infosüsteemidega ega omandada juurdepääsu sellistele veebikeskkondadele, mille kasutamine ei ole vangla julgeolekukaalutlustest lähtuvalt lubatud.

Küberturvalisuse ja internetikasutuse kontrollitavuse tagamiseks on põhjendatud eelistada lahendust, kus kogu veebilehe sisu, ressursid ja funktsionaalsused paiknevad sama domeeni ja hallatava infrastruktuuri piires. Võimaluse korral tuleks vältida kolmandate osapoolte teenuste, väliste skriptide, sisujagamiskeskkondade, API-de, iframe-lahenduste ning muude manustatud komponentide kasutamist, kuna need võivad luua täiendavaid võrguühendusi väliste süsteemidega ning raskendada veebiliikluse filtreerimist, logimist ja turvajärelevalvet. Eelkõige ei ole soovitatav kasutada väliseid multimeediateenuseid, sealhulgas YouTube'i või muid videoplatvorme, mille kaudu võib tekkida juurdepääs sisule või funktsionaalsusele, mida ei ole võimalik vangla kontrollikeskkonnas piisava kindlusega piirata.

Samuti tuleb välistada selliste funktsioonide rakendamine, mis võimaldavad kasutajapoolset andmesisestust või kahesuunalist andmevahetust väliste süsteemidega. See hõlmab muu hulgas tagasisidevorme, kommentaariume, jututubasid, vestlusaknaid, tehisintellektil põhinevaid suhtluslahendusi, dokumentide üleslaadimise võimalusi ning muid funktsionaalsusi, mille kaudu on võimalik edastada teavet väljapoole vangla kontrollitavat sidekeskkonda.

Arvestades, et isegi näiliselt piiratud ulatusega tehnilised muudatused võivad mõjutada veebilehe turvaprofiili ning vanglate internetikasutuse kontrollimeetmete toimivust, tuleb vanglateenistusele tagada võimalus hinnata kavandatavaid arendusi enne nende kasutuselevõttu tootmiskeskkonnas. Selleks on põhjendatud võimaldada juurdepääs arendus- või testkeskkonnale piisava ajavaruga enne muudatuste avalikustamist, soovitatavalt vähemalt 3 – 4 nädalat enne nende tootmiskeskkonda rakendamist. Selline eelkontroll võimaldab hinnata muudatuste mõju võrguliiklusele, ligipääsukontrollidele, veebisisu filtreerimisele ning vangla infosüsteemide ja julgeolekumeetmete toimimisele.

Seejuures tuleb arvestada, et vanglateenistusel peab säilima õigus anda kavandatavatele muudatustele julgeoleku- ja küberturvalisuse hinnang ning vajaduse korral seada veebilahenduse kasutamisele täiendavaid tehnilisi või organisatsioonilisi tingimusi. Kui selliste tingimuste rakendamine ei ole võimalik või kui kavandatavad muudatused suurendavad ebaproportsionaalselt vangla julgeoleku-, küberturvalisuse või järelevalveriske, võib osutuda vajalikuks veebilehe konkreetsete funktsioonide, alamlehtede või tehniliste komponentide blokeerimine või nende kättesaadavuse piiramine vanglate kontrollitud internetikeskkonnas.

c) Kui suured on selliste meetmete rakendamisega seotud esmased ühekordsed ning edasised püsikulud? Palun esitada iga võimaliku meetme kohta eraldi kuluarvestus.

Nagu eelpool välja toodud, siis praegu ei kontrollita igapäevaselt kinnipeetavate tegevust arvuti kasutamisel. Seetõttu ei ole võimalik tuua välja kulutusi eelarverea põhiselt.

Justiits- ja Digiministeerium on hinnanud veebilehtede kontrollimiseks, mis võimaldaks tagada veebilehtede põhjalikumaks (kuid mitte täielikuks) kontrollimiseks vajalikud võimalused[27], ressursikulu järgmiselt:
1) kinnipeetavate tegevuse ja veebilehtede muudatuste jälgimisele kuluv monitoorimissüsteem 330 000 eurot arenduseks (s.o ühekordne kulu), millele lisandub vangla tööjõukulu 190 080 eurot aastas ning lisaks RIK-i tööjõukulu aastas 79 200 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) Kulud, mis kaasnevad iga uue veebilehe seadistamisega. Ühe veebilehega seotud järjepidevate tööde maksumus võib olla väga varieeruv, sõltuvalt veebilehe keerukusest kuid keskmiselt hinnatavalt u 5000 – 10 000 eurot. Iga lisanduva asutuse veebilehe lisandumine tähendab vanglateenistuse jaoks samasugust kulu.

Suures osas tehakse eespool nimetatud kontrollitegevusi ka juba lubatud veebilehtede puhul, kuid igapäevast ulatuslikku monitoorimist ega pidevat asutustevahelist infovahetust selleks ei toimu. Kui vanglateenistus saab teavet võimaliku probleemi või turvariski kohta, kontrollitakse olukorda ning vajaduse korral tehakse vastavad seadistuste muudatused. Veebilehtede igapäevane ja põhjalik kontrollimine eeldaks märkimisväärseid lisavahendeid, mistõttu moodustaks see vanglateenistuse sisutegevuste eelarvest ebaproportsionaalselt suure osa. Sellist lähenemist ei saaks pidada riigi ressursside otstarbekaks ja mõistlikuks kasutamiseks. Seetõttu on otsustatud suunata ressursid eelkõige kinnipeetavate taasühiskonnastamisele ja selleks vajalike teenuste arendamisele. Näiteks on loodud kinnipeetava ja vangla vaheline suhtlusportaal (VAPO), mis võimaldab kinnipeetaval osaleda igapäevases asjaajamises vanglaga.

Riskide kuritarvitamise võimaluste vähendamise kontekstis pean oluliseks välja tuua, et ka Euroopa vanglate digitaliseerimise käsitlustes on rõhutatud, et uute IKT-lahenduste kasutuselevõtt toob lisaks eelistele kaasa ka julgeoleku- ja kommunikatsiooniriske. Eelkõige on peetud oluliseks tagada kontroll digitaalse suhtluse üle ning vältida olukordi, kus tehnoloogilised lahendused võimaldavad kinnipeetavatel luua kontrollimatuid sidekanaleid või kasutada vangla väliskeskkonnaga suhtlemiseks funktsioone, mida esialgses riskihinnangus ei ole arvesse võetud. Seetõttu on EuroPrisi analüüsides rõhutatud, et mida ulatuslikumalt digilahendusi vanglates kasutatakse, seda suuremaks muutub vajadus pideva turvahindamise ja järelevalve järele. See tähendab, et digitaalsete lahenduste laiendamisega kasvab ka järelevalveks vajaminev personali ja rahaline ressurss.

d) Kas ja kui aegsasti on võimalik anda vanglatele eelteavitus kohtute veebilehel tehtavatest muudatustest, mille tagajärjel võib rakendatud meetmetele vaatamata osutuda võimalikuks elektrooniline suhtlus kinnipeetava poolt? Kas ja kui suur lisakulu sellega kaasneks ning milles see seisneks?

Uue funktsionaalsuse kasutuselevõtu ettevalmistamisel tuleks vanglateenistusele võimaldada juurdepääs arenduskeskkonnale vähemalt 3 – 4 nädalat enne lahenduse tootmiskeskkonda (*Live*) juurutamist. Selle aja jooksul viiakse läbi funktsionaalsuse ja sisu kontroll vanglate infosüsteemide ning turvanõuete vaatest, määratletakse vajadusel täiendavad tehnilised või sisulised piirangud ning tehakse ettepanekud nende rakendamiseks. Samuti hinnatakse, kas mõne funktsionaalsuse või sisuelemendi kuvamine kinnipeetavatele tuleb turva- või õiguskaitselistel põhjustel piirata või välistada.

Arvestada tuleb, et veebilehe kohus.ee kättesaadavaks tegemine kinnipeetavatele ei piirdu üksnes olemasoleva veebisisu avamisega. Vajalik on veebikeskkonna turvalisuse, funktsionaalsuste ja välisliideste pidev hindamine ning testimine vanglate infosüsteemide vaatest. Samuti eeldab see Vanglateenistuse kaasamist veebilehe muudatuste ja uute funktsionaalsuste eelkontrolli. Selleks vajalik täiendav töömaht võib esialgsel hinnangul ulatuda 20 – 40 tööpäevani veebilehe kasutuselevõtmisel ning 10 – 30 tööpäevani aastas veebilehe edasiste arenduste ja muudatuste kontrollimisel.

4) Tallinna Vanglalt palub Riigikohus järgmist täiendavat teavet: kui vanglat teavitataks kohtute veebilehel tehtavatest muudatustest ette, siis mida peaks vangla omalt poolt tegema, et takistada

[27] Haldamise ja kontrollikulud, kui kasutusvõimalus on tund aega nädalas, juurdepääs piiramatu, kuid seaduse alusel täielikult kontrollitav.

kinnipeetavale keelatud elektroonilist suhtlust? Kui suur oleks vangla esmane ühekordne ja sellele järgnev püsikulu, et takistada kohtute veebilehel elektroonilist suhtlust?

Riigikohus on adresseerinud küsimuse Tallinna Vanglale, kuid arvestades, et vanglate IT valdkonda juhitakse vanglateülese keskse üksuse kaudu[28], kes on neid kulusid hinnanud ja Justiits- ja Digiministeeriumile on nende kulude summa ja kujunemine teada, vastan ka kuluarvestuse osas.

Ka juhul, kui vanglateenistust teavitatakse kohus.ee veebilehel kavandatavatest muudatustest ette, ei kõrvalda see vajadust hinnata iga muudatuse vastavust vangistuse täideviimise turvanõuetele. Vanglal tuleb kontrollida, kas uus funktsionaalsus, väline liidestus, interaktiivne element või kolmanda osapoole komponent võib võimaldada kinnipeetaval pidada keelatud elektroonilist suhtlust või luua selleks täiendavaid võimalusi. kohus.ee sisaldab muu hulgas viiteid teistele infosüsteemidele ja elektroonilistele teenustele, mistõttu tuleb muudatuste mõju hinnata ka tehnilisest vaatest. Selleks tuleb vanglateenistusel läbi viia muudatuste eelkontroll, testida nende toimimist vanglate kasutuskeskkonnas, analüüsida võimalikke kuritarvitamise stsenaariume ning vajaduse korral rakendada täiendavaid tehnilisi piiranguid või blokeerimisreegleid. Tegemist ei ole ühekordse tegevusega, vaid pideva kontrolliprotsessiga, mida tuleb korrata iga olulisema veebiarenduse korral.

Esialgsel hinnangul kaasneks sellise kontrollimehhanismi loomisega ligikaudu 20 – 40 tööpäeva suurune ühekordne töömaht, mille maksumus oleks suurusjärgus 5 000 – 10 000 eurot. Edaspidi tuleks kohtute veebilehel tehtavaid muudatusi regulaarselt hinnata ja testida, mistõttu kaasneks püsiv töökoormus ligikaudu 10 – 30 tööpäeva aastas ning hinnanguline iga-aastane kulu suurusjärgus 3000 – 8000 eurot. Seega eeldab keelatud elektroonilise suhtluse tõkestamine kohtute veebilehe kaudu pidevat tehnilist ja organisatsioonilist kontrolli ega piirdu üksnes veebilehe esmakordse avamisega kinnipeetavatele. Seega eeldab keelatud elektroonilise suhtluse riski maandamine nii täiendavat personaliressurssi kui ka püsivat tehnilist järelevalvet.

Lugupidamisega

(allkirjastatud digitaalselt)
Liisa-Ly Pakosta
justiits- ja digiminister

Laura Glaase 51916910
Laura.Glaase@justdigi.ee

[28] Vanglateenistuse IT ja andmehalduse valdkonna teenistujate põhiülesanne on vangistusseaduse § 5[1] lõikes 1 nimetatud andmekogu ja muude vanglateenistuse andmekogude, infotehnoloogiliste lahenduste arendamine ja haldamine koostöös registrite ja infosüsteemide keskusega ning Riigi Kinnisvara AS-ga ning andmehaldus, justiitsministri 6.12.2001. a määruse nr 87 „Tartu Vangla põhimäärus“ § 13[11] lg 1.