JUSTIITS- JA DIGIMINISTEERIUM

Riigikohus
info@riigikohus.ee

Teie 27.03.2026 nr 5-26-16/3
Meie 24.04.2026 nr 10-3/2439

Vastus põhiseaduslikkuse järelevalve menetluses nr 5-26-16

Lugupeetud Riigikohtu esimees

Riigikohtu põhiseaduslikkuse järelevalve kolleegiumi menetluses on asi nr 5-26-16 seoses kinnipeetavale neljale veebilehele (JDM, PPA, EMTA, eesti.ee) juurdepääsu keelamisega. Sellega seoses küsiti justiits- ja digiministri arvamust sätete asjassepuutuvuse, piirangu eesmärgi ja proportsionaalsuse kohta ning esitati täpsustavad küsimused seoses veebilehtedele juurdepääsuga kaasnevate riskide ja nende ärahoidmiseks tehtavate kulutustega. Käesolevaga esitan seisukohad[1] ja vastused Riigikohtu küsimustele.

Leian, et vaidlusalused normid, s.o (VangS) § 31[1] esimene lause (alates 01.08.2019 kuni 31.03.2024 kehtinud redaktsioonis) ning VangS § 31[1] lg 1 (alates 01.04.2024 kehtivas redaktsioonis) ja justiitsministri 30.11.2000. a määruse nr 72 „Vangla sisekorraeeskiri“ (VskE) § 52[1] lg 1 (alates 31.03.2024 kehtivas redaktsioonis), on asjassepuutuvad ja konkreetne normikontroll lubatav. Samuti leian, et normid osas, milles need välistavad juurdepääsu neljale vaidlusalusele veebilehele, on põhiseadusega kooskõlas. Järgnevalt esitan seisukohad (1) ja vastan Riigikohtu küsimustele (2).

1. Regulatsiooni asjassepuutuvus, seaduslik eesmärk ja proportsionaalsus

1.1. Normikontrolli lubatavus – vaidlustatud sätete asjassepuutuvus

Põhiseaduslikkuse järelevalve menetlus on võrsunud haldusasjast nr 3-23-187. Tartu Halduskohus arutas haldusasjas 3-23-187 kinnipeetavast kaebaja taotlust saada juurdepääs Justiits- ja Digiministeeriumi (JDM), Maksu- ja Tolliameti (MTA), Politsei- ja Piirivalveameti (PPA) ning Eesti teabevärava eesti.ee veebilehtedele ja e-toimiku rakendusele maksekäsu kiirmenetlust puudutavas osas. Tartu Halduskohus tunnistas 11.03.2026. a otsusega põhiseadusega vastuolus olevaks:
1) vangistusseaduse (VangS) § 31[1] esimese lause (alates 01.08.2019 kuni 31.03.2024 kehtinud redaktsioonis) osas, milles see välistas kinnises vanglas karistust kandva kinnipeetava ligipääsu MTA, JM, PPA ning Eesti teabevärava eesti.ee veebilehtedele, välja arvatud e-teenuseid puudutavas osas; 2) VangS § 31[1] lg 1 (alates 01.04.2024 kehtivas redaktsioonis) ning justiitsministri 30.11.2000. a määruse nr 72 „Vangla sisekorraeeskiri“ (VskE) § 52[1] lg 1 (alates 31.03.2024 kehtivas redaktsioonis) osas, milles need välistavad kinnises vanglas karistust kandva kinnipeetava ligipääsu MTA, JDM, PPA ning Eesti teabevärava eesti.ee veebilehtedele, välja arvatud e-teenuseid puudutavas osas.

[1] Võttes arvesse peaministri 27.03.2026. a resolutsiooni nr 7-7/26-00663, millega anti Justiits- ja Digiministeeriumile tulenevalt põhiseaduslikkuse järelevalve kohtumenetluse seaduse § 10 lõike 1 punktist 7 ülesanne täita kohtunõue ja tagada Vabariigi Valitsuse esindamine kohtus, Dokument: Küsimused menetlusosalistele ja menetlusse kaasatud isikutele

Vaidlusalused sätted:

1) 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.“.

2) Alates 1.04.2024. a kehtiva sõnastuse järgi sätestab VangS § 31[1] lg 1 järgmist: „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.“.

3) Justiitsministri 30.11.2000. a määruse nr 72 „Vangla sisekorraeeskiri“ (VskE) § 52[1] lg 1 on sõnastatud järgmiselt:
„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;
6) Ametlike Teadaannete veebileht;
7) tõlkerakenduse veebileht.“.

Sätete 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 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. Vaidlusalused normid välistavad kinnipeetavate juurdepääsu veebilehtedele, millele kinnises vanglas kinnipeetavana viibiv 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 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 asjassepuutuvad normid ja seega on põhiseaduslikkuse järelevalve lubatav.

1.2. <u>Piiratav põhiõigus ja selle riive</u>

1) 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. Kuivõrd vaidlusalustest sätetest

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

tulenev piirang avaldus isiku jaoks sisuliselt samaväärse tulemusena, ei ole nende erinev sõnastus või regulatiivne ülesehitus käesolevas kontekstis määrava tähtsusega. Seetõttu on piiratava põhiõiguse olemuse ning selle riive hindamisel asjakohane lähtuda ühtsetest põhjendustest. Kuigi vaidlusalused sätted võivad oma sisult teataval määral erineda, viisid need konkreetsetes asjaoludes samasisulise piiranguni, s.t välistasid kaebaja taotletud neljale veebilehele juurdepääsu, mistõttu puudub alus neid põhiõiguse riive analüüsimisel eristada. Seetõttu kohalduvad järgnevad põhjendused ühtviisi kõigi vaidlusaluste sätete suhtes.

2) Vaidlusalustes normides sätestatud keeld JDM, EMTA, PPA ja eesti.ee veebilehtedele juutdepääsuks piirab (interneti vahendusel) ligipääsu üldiseks kasutamiseks mõeldud teabele, millele ligipääsu õigus on tagatud põhiseaduses.

3) 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 ja kohtulahendite registrile. Kõnealune säte riivab PS § 44 lõikes 1 sätestatud põhiõigust teabe saamise viisi kaudu.

4) 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.

5) 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.[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.

6) 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

[5] 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

viibimise ajal kuritegude toimepanemist. Juurdepääsu võimaldamine rohkematele veebilehtedele. Kuigi praegu on vaidluse all neli veebilehte, kehtiksid sarnased riskid ka teiste riigiasutuste veebilehtede puhul. Nt riigiasutuste puhul VVS § 38 tähenduses lisanduks ca 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.

7) 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.

1.3. Kinnipeetavatele veebilehtede lubamisega seotud riskid

8) 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.

9) 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 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).

10) 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.

11) 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.

12) Tavapäraselt on veebilehtedel suhtlust võimaldavaks osaks teabenõude[6], märgukirja või selgitustaotluse esitamise elektroonne vorm, mis sageli annab ka võimaluse saata suvalisele meiliaadressile pöördumise koopia[7]. 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. 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 paroolivälјale trükkida sõnum 6-16 tähemärki. Seejärel sai paroolivälјale 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.

13) 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 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.

14) 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.

15) 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.

16) Lisaks veebilehtedele ligipääsu tagamisele tuleb iga lehe lubamisel teha pidevat seiret, et avastada võimalikke puudujääke ja turvariske. Kuna kulud ja risk kumuleerivad iga veebilehe

[6] 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

[7] 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.

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.

17) 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.

18) 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.

19) 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.

20) 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.[8] 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).

21) 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 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[9] 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.

22) 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.

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

[9] 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 ennekõike serverist info hankimiseks, seevastu POST päringut serverisse info edastamiseks.

23) 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.

24) Kuivõrd iga lisanduva veebilehe kulud kumuleeruvad, siis on Justiits- ja Digiministeerium toonud välja kuluarvestuse ka sellest lähtuvalt.[10] Justiits- ja Digiministeerium on hinnanud veebilehtede kontrollimiseks, mis võimaldaks tagada veebilehtede põhjalikumaks (kuid mitte täielikuks) kontrollimiseks vajalikud võimalused[11], 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.

25) 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 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, märgime, 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.

26) Eelnevalt selgitasime veebilehtede monitoorimisega seotud kulusid. Iga lisanduva veebilehega need kulud kasvavad ja riigil ei pruugi olla mingil hetkel enam võimekust kontrolli tagada. Eeltoodud analüüsist nähtub, et veebilehtede turvaline võimaldamine vanglate keskkonnas eeldab püsivat ja märkimisväärset ressursipanust, mis hõlmab nii spetsialiseeritud tööjõudu kui ka tehnilisi lahendusi. Samas tuleb arvestada, et avaliku sektori

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

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

asutus tegutseb piiratud eelarve raames ning on kohustatud kasutama ressursse eesmärgipäraselt ja proportsionaalselt oma põhifunktsioonide täitmiseks. Vanglateenistuse esmaseks ülesandeks ei ole veebikeskkondade haldamine ega nende pidev tehniline monitoorimine, vaid kinnipidamistingimuste tagamine ja julgeoleku hoidmine. Sellest tulenevalt ei ole põhjendatud suunata ebaproportsionaalselt suurt osa ressurssidest tegevusse, mis ei ole asutuse põhitegevus, eriti olukorras, kus sama eesmärgi – kontrollimatu suhtluse välistamise – saab saavutada ka veebilehtede ligipääsu piiramise kaudu. Lisaks tuleb arvestada, et veebikeskkondade arv ja tehniline keerukus on ajas kasvavad. Iga täiendav veebileht ei lisa üksnes ühekordset kontrollikohustust, vaid suurendab püsivalt seire- ja halduskoormust. See tähendab, et isegi kui teatud hetkel on võimalik olemasolevaid veebilehti kontrollida, muutub see aja jooksul järjest ressursimahukamaks ning võib ületada asutuse võimekuse tagada nõutav turvalisuse tase. Selline areng ei ole jätkusuutlik. Seetõttu ei ole asutusel mitte üksnes praktiline, vaid ka sisuliselt õiguslik kohustus vältida olukorda, kus ressursside kasutamine muutub ebaproportsionaalseks. Kui veebilehtede turvaline haldamine eeldaks ülemäärast rahalist ja tööjõukulutust, mis kahjustab teiste ülesannete täitmist, ei ole selline lähenemine põhjendatud. Sellisel juhul tuleb eelistada lahendusi, mis on hallatavad olemasolevate ressursside piires, sealhulgas piirata lubatud veebilehtede hulka. Seega, kuigi teatud veebisisule ligipääsu võimaldamine võib olla soovitav, seab ressursside piiratus objektiivse piiri sellele, millises ulatuses seda teha saab. Veebilehtede arvu ja keerukuse kasvades ei ole võimalik tagada kõigi nende turvalist haldamist ilma ebaproportsionaalse ressursikuluta, mistõttu ei ole vanglateenistusel võimalik ega põhjendatud sellesse tegevusse piiramatus mahus panustada.

1.4. Riive põhiseaduspärasus

27) VangS § 31^1 kuni 31.03.2024 kehtinud redaktsiooni esimese lause põhiseaduspärasuse kohta on justiitsminister esitanud arvamuse Riigikohtule 30.10.2022 vastuses nr 10-3/6915 (kättesaadav dokumendiregistris: Justiits- ja Digiministeeriumi avalik dokumendiregister). Jään ka käesolevas menetluses samade põhjenduste juurde ja palun neid käsitleda justiits- ja digiministri seisukohtadena käesolevas menetluses. Kuigi nimetatud asjas oli vaidluse all juurdepääsu võimaldamine Riigikohtu veebilehele ja Ametlike Teadaannete veebilehele, ei erine piirangu põhjendused olemuslikult praegu lahendamisel oleva kaebuse kohta esitatavatest põhjendustest. Nimetatud vastuses asuti seisukohale, et VangS § 31^1 esimene lause on põhiseadusega kooskõlas. Samuti 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. Nimetatud piirang sisaldus 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.

28) Kinnipeetavate internetile ligipääsu laiendamise küsimuses, sh julgeoleku- ja turvariskidega seonduva osas viidati Riigikohtu üldkogule asja nr 3-3-2-1-16 menetlemisel esitatud seisukohtadele (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 toetasid seisukohta, et piirang on põhiseaduspärane, paluti neis sisalduvaid põhjendussi arvesse võtta lisaks 30.10.2022 vastuses nr 10-3/6915 kajastatule. Nimetatud dokumentides sisalduvad põhjendused turvariskide ja nende maandamiseks vajalike kulude kohta on asjakohased ka praegu. Järgnevalt esitame põhjendused piirangu sobivuse, vajalikkuse ja mõõdukuse kohta. Riigikohus on asjas nt 3-18-477 vaidlusaluse sätte osas hinnanud piiranguid sobivaks ja vajalikuks (otsuse p 78). Praeguses asjas vaidluse all olevate veebilehtede 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. Täiendavalt esitan põhjendused piirangu mõõdukuse kohta (proportsionaalsus kitsamas mõttes).

29) 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.[12] Vaidlust ei ole, et vaidlusalused sätted vastavad formaalse põhiseaduspärasuse nõuetele.

30) 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.[13] 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.

31) 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.

32) 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.

33) 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 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[14] 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

[12] RKPJKo nr 3-4-1-5-05, p 8, https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-5-05
[13] 3-2-1-73-04, p 36.
[14] Vangistusseaduse muutmise seadus 680 SE, eelnõu ja seletuskiri arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8f08bcf8-2b6b-4017-b64c-6eea9c00a98c

sätestatud kohustust ei ole võimalik tagada, kui kinnipeetaval on võimalik kasutada internetis veebilehtede osi, mis võimaldavad elektroonilist suhtlust.

34) 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.[15] 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.[16] 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.[17] Eeltoodut arvestades on piirangu eesmärk legitiimne.

35) Sobiv on abinõu, mis soodustab eesmärgi saavutamist. Sobivuse seisukohalt on vaieldamatult ebaproportsionaalne abinõu, mis ühelgi juhul ei soodusta piirangu eesmärgi saavutamist.[18] 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.

36) 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.

37) Nagu eespool öeldud, on Riigikohus on hinnanud[19] 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

[15] Vt ka Vangistusseadus. Kommenteeritud väljaanne, Sootak. J., Juura, 2014, § 2^1 kommentaar, p 1,2, lk 94.
[16] 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
[17] https://rikos.rik.ee/LahendiOtsingEriVaade?asjaNr=3-3-1-5-09 p 34
[18] PS kommenteeritud väljaanne; § 11, komm 10.
[19] Vt otsuse p 78, 3-18-477/73

saavutamiseks sobiv ja vajalik. 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.

38) Abinõu mõõdukuse üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusesse sekkumise ulatust ja intensiivsust, teiselt poolt aga riive eesmärgi tähtsust.[20] Kaalumine eeldab kokkuvõttes võimalikult kõigi poolt- ja vastuargumentide nimetamist ja kohtu seisukohavõttu.[21] Olukorras, kus kinnipeetavatel ei ole juurdepääsu Maksu- ja Tolliameti (EMTA), Politsei- ja Piirivalveameti (PPA), Justiits- ja Digiministeeriumi (JDM) ja riigiportaali eesti.ee veebilehtedele, saab kirjeldada üksnes nende veebilehtedega 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.[22] Toome välja täiendavate veebilehtede lubamisega seotud riskid, mis kehtivad üldiselt iga täiendava veebilehe puhul, ja kulutused, mida tuleb kanda järjest lisanduvate veebilehtede puhul. Samuti tõime näited, kus kinnipeetavad on kuritarvitanud neile lubatud juurdepääsusid seoses vangi portaali ja e-toimiku kasutamisega (vt vastuse p 14). Vaidlusaluste veebilehtedega seotud riskid on välja toodud vastuse p-s 2, küsimuste a) ja d) vastuste juures.

39) 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.

40) 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 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. Seetõttu saab järeldada, et abinõu on mõõdukas (proportsionaalne).

41) 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 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[23] 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

[20] RKÜKo 3-4-1-7-01, p 21.
[21] PS kommenteeritud väljaanne; § 11 komm 17.
[22] Vt nt Õhtulehes 18.02.2025 avaldatud artiklid: VIDEO | Bardakk vanglate e-süsteemis: vangid vahivad pornot ja peavad keelatud suhtlust, JUHTKIRI | Virtuaalselt vangist väljas.
[23] Vangistusseaduse muutmise seadus 680 SE, eelnõu ja seletuskiri arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8f08bcf8-2b6b-4017-b64c-6eea9c00a98c

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.

42) Seega on vaidlusaluste normidega sätestatud interneti kasutamise keeld eesmärkide saavutamiseks sobiv ja vajalik. Normid välistavad ligipääsu vaidlusalustele veebilehtedele, välistades seeläbi ühtlasi vanglateenistuse kontrolli alt välja jääva vanglavälise suhtluse. Veebilehel suhtlusvõimaluste piiramise efektiivsus sõltub selleks valitud tehnilistest lahendustest ja kontrollist, mis võivad kaasa tuua erinevas suuruses kulusid. Veebilehel suhtlusvõimaluste piiramine on üldjuhul kulukam, kui oleks veebilehele ligipääsu täielik keelamine. Kulud kaasneksid ka sellega, kui kinnipeetav peaks soovitud veebilehele ligipääsuks esitama taotluse ning vanglateenistus otsustaks ligipääsu üle kaalutlusõiguse alusel. Seetõttu on raske näha abinõu, mis võimaldaks põhiõigust vähem riivates saavutada mõlemat legitiimset eesmärki sama efektiivselt - piirata veebilehel vanglavälist suhtlust kolmandate isikutega sama tõhusalt, toomata seejuures kaasa suuremaid kulusid. Sellega, et tegu on sobiva ja vajaliku meetmega, on Riigikohus nõustunud analoogses vaidluses asjas nr 3-18-477[24] (otsuse p 78).

2. Täpsustavad vastused Riigikohtu küsimustele

Järgnevalt vastan Riigikohtu täpsustavatele küsimustele.

a) Justiits- ja digiminister, RIK, RIA, MTA, PPA: ***kui vangistust kandev kinnipeetav saab juurdepääsu konkreetselt 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)?***

Küsimusele vastamisel tuleb lähtuda nii kehtivast õiguslikust raamistikust kui ka kaasaegsete veebirakenduste tehnilisest olemusest, millest tulenevad reaalsed riskid ei piirdu üksnes e-teenuste kasutamise võimalikkusega.

Järeldus, et e-teenuste ligipääsu puudumisel on veebilehe kasutamine riskivaba, ei ole põhjendatud. Ka nn avalik või informatiivne veebikiht kujutab endast tehniliselt täisfunktsionaalset veebirakendust, mille kaudu toimub lehitseja ja erinevate serverite vaheline andmeside. Selline andmeside realiseerub muu hulgas HTTP(S) päringute, JavaScripti kaudu tehtavate API-kutsete (XHR, fetch), redirect-mehhanismide (ümbersuunamised) ning väliste ressursside laadimise kaudu. Iga nimetatud mehhanism võib võimaldada andmete edastamist väliskeskkonda kas otseselt (nt sisendvormid, mailto-lingid) või kaudselt (nt taustapäringud kolmandate osapoolte teenustesse).

Arvestada tuleb, et veebilehtede funktsionaalsus ei ole staatiline. Ka juhul, kui konkreetsel ajahetkel ei ole tuvastatav otsest suhtlusmehhanismi, võivad need tekkida dünaamiliselt kas veebilehe arendustegevuse käigus, kolmandate osapoolte komponentide (nt analüütika, lisatud lahendused) lisandumisel või JavaScripti käitumise muutumisel. Sellest tulenevalt ei ole võimalik üksnes ühekordse kontrolli alusel järeldada, et veebileht ei võimalda kontrollimatut suhtlust.

[24] 3-18-477/73

Risk hõlmab ka veebilehe kaudu toimuvat suunamist teistesse keskkondadesse. Ka ilma e-teenuste otsese kasutamiseta võib kasutaja jõuda ümbersuunamiste või linkide kaudu süsteemidesse, kus on võimalik autentimine või andmete sisestamine. Arvestades, et kaasaegsed veebirakendused kasutavad laialdaselt domeenidevahelist integratsiooni (sh SSO- mehhanismid, CORS- põhised päringud), ei ole selliste liikumiste täielik välistamine ilma ulatusliku tehnilise kontrollita tagatav.

Viimasena tuleb rõhutada, et vanglateenistusel lasub seadusest tulenev kohustus välistada kontrollimatu suhtlus väliskeskkonnaga. See kohustus ei piirdu üksnes ilmselgete suhtluskanalitega, vaid hõlmab ka kaudseid ja tehniliselt varjatud andmesidevorme. Seetõttu tuleb riskihindamisel lähtuda mitte üksnes tavapärasest kasutusstsenaariumist, vaid ka kõikidest mõistlikult ettenähtavatest tehnilistest kuritarvitamise võimalustest.

Mis puudutab küsimust, kuidas samu veebilehti kontrollitakse vabaduses olevate isikute puhul, siis tuleb rõhutada, et tegemist on õiguslikult ja tehniliselt erineva olukorraga. Vabaduses olevate isikute internetikasutusele ei kohaldu samasugune suhtluspiirang ning veebilehtede turvameetmed on suunatud eelkõige süsteemi tervikluse, kättesaadavuse ja andmete konfidentsiaalsuse tagamisele (nt haavatavuste testimine, sisuhaldus, ligipääsukontroll). Need meetmed ei ole kavandatud ega piisavad selleks, et välistada üksiku kasutaja poolt igasugune andmeedastus väliskeskkonda.

Vanglate kontekstis on nõutav oluliselt rangem standard – välistada tuleb ka sellised andmesidevõimalused, mis tavakasutuses ei ole käsitletavad turvariskina. Sellest tulenevalt ei ole võimalik tugineda tavapärastele veebiturbe meetmetele, vaid vajalik oleks eraldiseisev, pidev ja mitmekihiline tehniline kontroll (sh võrgu-, rakenduse- ja kliendipoolne piiramine), mille puudumisel ei ole võimalik tagada, et veebilehe kasutamine ei võimalda kontrollimatut suhtlust.

Seega ei saa riski hinnata üksnes selle põhjal, kas konkreetse veebilehe kaudu on võimalik kasutada e-teenuseid. Ka ilma e-teenusteta sisaldavad veebilehed tehnilisi mehhanisme, mille kaudu võib toimuda andmevahetus, ning nende mehhanismide täielik ja püsiv kontrollimine ei ole praktikas tagatav ilma märkimisväärse ressursikuluta. Sellest tulenevalt kaasnevad ka piiratud ligipääsuga reaalsed kuritarvitamise riskid, mida vanglateenistus on kohustatud ennetama.

d) Viru Vangla ning justiits- ja digiminister: ***kui vaidluse all olevate veebilehtede haldajad edastaksid vanglale regulaarselt teavet oma veebilehel tehtavate muudatuste kohta, siis mida konkreetselt peaks vangla veel tegema, et takistada kinnipeetavale keelatud elektroonilist suhtlust? Kui suured oleksid vangla esmased ühekordsed ja seejärel regulaarsed kulutused elektroonilise suhtluse takistamiseks konkreetsete veebilehtede puhul?***

Ka juhul, kui veebilehtede haldajad edastaksid vanglale regulaarselt teavet veebilehtedel tehtavate muudatuste kohta, ei oleks see iseenesest piisav meede kontrollimatu elektroonilise suhtluse välistamiseks. Selline teave oleks oma olemuselt deklaratiivne ega asendaks tehnilist verifitseerimist ega järelevalvet, mida vanglateenistus on kohustatud teostama.

Veebilehtede toimimine ei piirdu üksnes nähtavate muudatustega. Kaasaegsed veebirakendused sisaldavad märkimisväärses ulatuses kliendipoolset loogikat (*JavaScript*), dünaamilisi API-päringuid ning kolmandate osapoolte komponente, mille käitumine võib muutuda ka ilma selgelt dokumenteeritud või haldaja poolt kommunikeeritud muudatusteta. Seetõttu ei ole võimalik tugineda üksnes haldaja poolt edastatud teabele, vaid vajalik on iga muudatuse tehniline kontroll, sealhulgas võrguühenduste, otspunktide ja andmevoogude analüüs. Teiseks ei pruugi veebilehe haldaja poolt edastatav teave olla piisava detailsusega, et hinnata selle mõju vanglateenistuse seisukohalt. Näiteks võib uus funktsionaalsus või väline integratsioon (nt analüütika, *embed*-komponent või ümbersuunamised) luua täiendava andmesidekanali, mille risk realiseerub alles tehnilise testimise käigus. Samuti ei saa välistada olukorda, kus kolmandate osapoolte teenused (nt CDN-id, skriptiraamistikud) muudavad oma käitumist iseseisvalt. Sellest tulenevalt peaks vangla ka regulaarse teavituse olemasolul täiendavalt tegema vähemalt järgmisi toiminguid:

- iga muudatuse tehniline analüüs (sh koodi ja võrguühenduste kontroll)
- lubatud domeenide ja otspunktide nimekirja ajakohastamine
- vajadusel uute blokeeringute rakendamine (proxy, tulemüür, CSP jms)
- funktsionaalne testimine, et kontrollida, kas suhtluskanalid on tegelikult välistatud
- pidev seire, et tuvastada ka haldaja poolt mitteteavitatud või kaudseid muudatusi

Seega ei asenda haldaja teavitus vanglateenistuse enda kontrolli, vaid võib üksnes vähesel määral toetada riskide varasemat tuvastamist. Kulude osas tuleb eristada esmast seadistust ja püsivat tegevust. Esmane ühekordne kulu hõlmab: veebilehtede põhjalikku tehnilist auditit (funktsionaalsuste ja andmevoogude kaardistamine), filtreerimis- ja piirangumehhanismide (nt proxy, tulemüür, CSP reeglid) seadistamist ning testimist ja valideerimist.

Oluline on rõhutada, et haldaja poolne teavitamine ei vähenda seda kulu olemuslikult, kuna vanglateenistus ei saa delegeerida oma õiguslikku kohustust kontrollida ja välistada kontrollimatu suhtlus. Teavitus võib küll lihtsustada muudatuste tuvastamist, kuid ei välista vajadust nende iseseisvaks tehniliseks analüüsiks ja kontrollimiseks. Seega ei ole pelgalt muudatuste kohta teabe edastamine piisav meede keelatud elektroonilise suhtluse takistamiseks. Vanglal tuleb ka sellisel juhul rakendada mitmekihilist tehnilist kontrolli ning kanda sellega seotud püsivaid kulusid, mis on märkimisväärsed ning ajas kumuleeruvad.

Ametlike veebilehtede, sealhulgas Justiits- ja Digiministeeriumi veebikeskkonna kasutamise lubatavuse hindamine vanglate infosüsteemides eeldab detailset tehnilist analüüsi, mis käsitleb veebirakendust kui potentsiaalset andmesidekanalit, mitte pelgalt staatilise sisu allikat. Sellise hindamise keskmes on veebilehe kogu ründepinna (attack surface) kaardistamine, hõlmates nii kasutajaliidese kaudu nähtavaid funktsioone kui ka taustal toimuvaid andmevahetusmehhanisme.

Esmalt tuleb tuvastada kõik sisend-väljundmehhanismid, mille kaudu klientrakendus (lehitseja) saab serveriga andmeid vahetada. See hõlmab HTML-vorme (POST/GET päringud), JavaScripti kaudu tehtavaid asünkroonseid päringuid (XMLHttpRequest, fetch API), samuti URI-skeeme nagu mailto:, mis võivad käivitada väliseid suhtluskanaleid. Iga selline mehhanism kujutab endast potentsiaalset kanalit, mille kaudu vang võib edastada andmeid väljapoole kontrollitud keskkonda. Tehniliselt tuleb need funktsioonid kas eemaldada DOM-tasemel (nt sisendväljade ja vormide kuvamise blokeerimine) või katkestada võrgu tasemel, filtreerides vastavad HTTP-päringud proxy või rakendustulemüüri (WAF) abil.[25]

Veel tuleb analüüsida kogu väljaminevat liiklust (*outbound traffic*), mida veebileht genereerib. Kaasaegsed veebirakendused kasutavad sageli kolmandate osapoolte teenuseid, CDN-e, analüütikat ja API-sid, mille poole tehakse automaatseid päringuid. Selleks tuleb teostada võrguinspektsioon (nt lehitseja arendaja tööriistadega, proxy logid), et tuvastada kõik sihtdomeenid ja endpoint'id (otspunktid). Seejärel tuleb kehtestada rangelt piiratud lubatud domeenide nimekiri (whitelist) ning blokeerida kõik ülejäänud domeenide päringud ja HTTP/HTTPS ühendused. Eriti oluline on tuvastada edasisuunamise mehhanismid (HTTP 3xx vastused[26], *JavaScript* ümbersuunamised, mis võivad kasutaja suunata kontrollimata keskkonda.

Lisaks tuleb hinnata kliendipoolse koodi käitumist. JavaScript võib dünaamiliselt luua suhtluskanaleid, näiteks kliendi ja serveri vahelisi kahepoolseid ühendusi (*websocket*) või lisada väliseid ressursse *iframe'i* kaudu. Seetõttu tuleb rakendada sisuturbe poliitikaid (*Content Security Policy*), mis piiravad lubatud skriptide, *iframe'ide* ja ühenduste allikaid. Samuti võib olla vajalik skriptide täielik keelamine või selektiivne isoleerimine (*sandboximine*), et välistada varjatud andmeedastusmehhanismid.

Multimeedia komponentide puhul, mida väga paljud veebilehed ka kasutavad, tuleb arvestada, et lisatud videopleierid (nt *iframe* YouTube'ist) ei ole pelgalt staatilised objektid, vaid sisaldavad sageli täiendavat funktsionaalsust, sealhulgas linke, soovitusi ja mõnel juhul ka suhtlusvõimalusi. Tehniliselt tähendab see, et sellised lisad tuleb kas eemaldada või piirata nii, et lubatud on üksnes staatiline sisu ilma interaktiivsete elementideta, näiteks läbi meediateenuse või rangete CSP reeglite.

Lisaks nähtavale funktsionaalsusele tuleb hinnata ka varjatud andmevooge, sealhulgas küpsiste kasutust, localStorage/sessionStorage mehhanisme ning võimalikke andmete eksfiltratsiooni kanaleid. Kuigi need ei pruugi otseselt võimaldada kahepoolset suhtlust klassikalises mõttes, võivad need toetada oleku säilitamist või andmete kogumist.

[25] Viimast saab teha veebilehe/rakenduse majutaja/haldaja. See tähendab, et kui nt JDM lehe puhul on võimalik seda teha, siis teiste vaidlusaluste lehtede puhul tuleks paluda seda teha veebilehe omanikul.
[26] serverilt saadav http/https staatuskood 300-308.

Õiguslikust vaatest tuleb kõik need tehnilised aspektid taandada küsimusele, kas veebirakendus võimaldab kontrollimatut andmesidet vangla infosüsteemi ja välismaailma vahel. Kui selline võimalus esineb, tuleb see elimineerida kas rakenduse tasemel (nt DOM manipulatsioon, skriptide eemaldamine), transpordikihi tasemel (nt TLS kontroll, proxyserveriga piiramine) või võrgu tasemel (tulemüür, domeenide lubamine/keelamine).

See kõik eeldab nii funktsionaalset testimist kui ka võrguanalüüsi, et kinnitada, et ükski keelatud andmeedastuskanal ei ole kasutatav. See tähendab praktiliselt kontrolli, et kasutaja ei saa genereerida väljaminevaid päringuid lubamata sihtkohtadesse, ei saa sisestada ja edastada andmeid läbi veebilehe ning ei saa kasutada varjatud või dünaamiliselt loodud suhtlusmehhanisme. Selline mitmekihiline tehniline kontroll on vältimatu, et tagada vastavus VangS-ist tulenevale nõudele välistada kontrollimata suhtluskanalid.

Riigiportaali eesti.ee puhul tuleb tehniline analüüs viia detailsele tasemele, arvestades, et tegemist ei ole pelgalt informatiivse veebilehega, vaid mitmekihilise infosüsteemide integratsiooniplatvormiga, mille keskseks funktsionaalsuseks on kasutaja autentimine ja sellele järgnev isikustatud teenuste osutamine. Vanglateenistuse vaates on seetõttu määrava tähtsusega just nende funktsionaalsuste tuvastamine ja välistamine, mis võimaldavad kasutajal end tuvastada ning algatada isiklikku andmevahetust väliste süsteemidega, samuti üldisemalt kõik mehhanismid, mille kaudu võib tekkida kontrollimatu suhtlus väliskeskkonnaga.

Tehniliselt tuleb esmalt eristada portaali kahte põhilist kihti: anonüümne avalik vaade ja autentimist nõudev iseteeninduskiht. Autentimisfunktsionaalsus realiseerub läbi kesksete identiteediteenuste, mille käigus luuakse kasutajale sessioon, mille alusel tehakse lehitsejast kasutaja nimel päringuid erinevatesse infosüsteemidesse. Sellest hetkest alates muutub lehitseja aktiivseks osapooleks mitme süsteemi vahelises andmevahetuses. Vanglate kontekstis tuleb selline funktsionaalsus käsitleda täielikult keelatuna, kuna see võimaldab kasutajal edastada ja vastu võtta andmeid väljaspool vangla kontrollitud kanaleid. See sisaldab lugematult arvul võimalusi varjatud suhtluseks suvaliste väliste osapooltega ja neid funktsionaalsusi ei ole võimalik võrgutasemel piirata, kuna kogu tegevus toimub rakenduse sees. Selleks on vajalik, et sealsed lugematud teenuse osutajad teeksid igaüks oma teenustes arendustöid, kuid see ei oleks teostatav.

Sellest tulenevalt tuleb tehniliselt rakendada meetmed, mis välistavad igasuguse sisselogimise võimaluse. See hõlmab autentimisega seotud URL-ide, otspunktide ja ümbersuunamismehhanismide blokeerimist nii kasutajaliidese tasandil kui ka võrgu tasemel, et vältida autentimisprotsessi käivitamist ka otsese URL-i sisestamise kaudu. Samuti tuleb katkestada sessioonihalduse mehhanismid, sealhulgas autentimisküpsiste ja märgendite loomine ning edastamine, ning välistada ühekordse autentimise (Single Sign-On) ahelad, mille kaudu autentimine võiks toimuda kaudselt teiste teenuste kaudu.

Samas ei ole üksnes sisselogimisfunktsionaalsuse keelamine piisav, kuna kontrollimatu suhtlus võib tekkida ka muude tehniliste mehhanismide kaudu. Seetõttu tuleb paralleelselt analüüsida ja piirata kõiki sisend-väljundkanaleid, mida veebirakendus kasutab. See hõlmab HTML-vorme, JavaScripti kaudu tehtavaid API-päringuid (XHR, fetch), võimalikke WebSocket-ühendusi ning muid andmeedastusmehhanisme. Iga selline kanal tuleb kas eemaldada rakendustasandil või blokeerida võrgu tasemel, kuna nende kaudu võib toimuda andmete edastamine kolmandatele osapooltele ka ilma klassikalise autentimiseta.

Täiendavalt tuleb kontrollida kogu väljaminevat võrguühendust, mida lehitseja veebilehe kasutamisel loob. Ka anonüümses vaates võib portaal teha automaatseid päringuid erinevatesse domeenidesse, sealhulgas analüütika-, CDN- või teenusepakkujate otspunktidesse. Nende ühenduste kaudu võib toimuda andmete edastamine või tekkida kaudne suhtluskanal. Seetõttu tuleb rakendada ranget domeeni- ja otspunktide põhist whitelisti ning blokeerida kõik lubamata ühendused nii DNS-, IP- kui ka HTTP(S)-tasemel.

Samuti tuleb analüüsida kliendipoolset koodi, kuna JavaScript võib dünaamiliselt luua uusi suhtluskanaleid, sealhulgas genereerida päringuid, laadida väliseid ressursse või käivitada ümbersuunamised. Selle riski maandamiseks tuleb rakendada siseturbepoliitika piiranguid, mis lubavad ainult eelnevalt määratud allikatest pärit skripte ja ühendusi, ning vajadusel piirata või täielikult

keelata aktiivne skriptimine. Ilma selleta ei ole võimalik välistada, et veebirakendus loob jooksvalt uusi andmesidekanaleid, mida eelnev analüüs ei hõlmanud.

Lisaks tuleb arvestada portaali rolliga teiste teenuste vahendajana. Isegi kui otsene autentimine on blokeeritud, võivad erinevad lingid ja suunamised viia kasutaja keskkondadesse, kus suhtlus on võimalik või kus autentimine käivitub automaatselt. Seetõttu tuleb rakendada terviklikku ümbersuunamiste ja domeenikontrolli, mis katkestab kõik katsed liikuda keskkondadesse, kus võib tekkida kontrollimatu suhtlus.

Kokkuvõttes tähendab eesti.ee portaali kasutamise lubatavuse tehniline tagamine vanglate kontekstis mitte ainult sisselogimisfunktsionaalsuse täielikku välistamist, vaid ka kõigi otseste ja kaudsete andmevahetusmehhanismide elimineerimist. See hõlmab sisendkanalite, API-päringute, skriptide, väliste ühenduste ja suunamiste kontrolli ning blokeerimist. Ainult sellise mitmekihilise ja süstemaatilise lähenemisega on võimalik tagada, et veebilehe kasutamine ei võimalda vangil mingil viisil kontrollimatult suhelda või andmeid edastada väljapoole vanglateenistuse järelevalvet.

Maksu- ja Tolliameti veebikeskkonna (emta.ee) hindamisel vanglate kontekstis tuleb lähtuda sellest, et tegemist on tehniliselt keeruka e-teenuste platvormiga, mille põhieesmärk on võimaldada kasutajatel teostada isikustatud toiminguid ning suhelda riigiasutusega digitaalsel teel. Seetõttu ei saa seda käsitleda pelgalt informatsiooni kuvava veebilehena, vaid kui süsteemi, mille kaudu toimub aktiivne ja struktureeritud andmevahetus kasutaja ja riiklike infosüsteemide vahel.

Arhitektuurselt koosneb keskkond avalikust infokihist ja eraldiseisvast e-teenuste kihist, kuhu ligipääs eeldab kasutaja autentimist. Autentimise tulemusel luuakse sessioon, mille alusel saab kliendirakendus (lehitseja) teha kasutaja nimel päringuid Maksu- ja Tolliameti süsteemidesse ning seotud andmekogudesse. Selline mehhanism tähendab, et lehitseja ei ole enam pelgalt passiivne sisu kuvaja, vaid toimib aktiivse vahendina, mille kaudu edastatakse ja töödeldakse kasutajaspetsiifilisi andmeid. Vanglateenistuse vaates tuleb selline funktsionaalsus välistada, kuna see loob otsese võimaluse kontrollimatuks andmesideks väliste süsteemidega.

Seetõttu on keskseks tehniliseks nõudeks kõikide sisselogimist võimaldavate funktsioonide blokeerimine. See hõlmab nii kasutajaliideses nähtavate autentimisvalikute eemaldamist kui ka nende taga olevate tehniliste lahenduste – sealhulgas autentimisotspunktide, ümbersuunamismehhanismide ja identiteeditеenustega seotud domeenide – ligipääsu keelamist. Samuti tuleb takistada sessioonide tekkimist ja säilitamist, näiteks blokeerides autentimisküpsised ja muud sessioonihalduse komponendid, mis võimaldaksid kasutajal saada ligipääsu e-teenustele ka kaudsete mehhanismide kaudu.

Samas tuleb arvestada, et suhtlusvõimalused ei piirdu üksnes autentitud keskkonnaga. Ka avalikus vaates võib esineda funktsionaalsusi, mis võimaldavad kasutajal sisestada ja edastada andmeid, näiteks kontaktivormide või muude päringulahenduste kaudu. Tehniliselt realiseeruvad need tavaliselt HTTP päringutena või kliendipoolsete skriptide abil tehtavate API-kutsetena. Sellised mehhanismid tuleb tuvastada ja neutraliseerida, kas eemaldades need kasutajaliidesest või blokeerides vastavad päringud võrgutasemel.

Täiendav tähelepanu tuleb pöörata veebilehe poolt algatatavale väljaminevale liiklusele. Ka ilma kasutaja otsese sisendita võib rakendus luua ühendusi erinevate väliste teenustega, näiteks laadides skripte, kasutades analüütikat või pöördudes muude teenusepakkujate poole. Selliste ühenduste kontrollimiseks tuleb rakendada ranget lubatud sihtkohtade loetelu ning piirata kogu muu liiklus, et välistada soovimatud või eelnevalt hindamata andmevood.

Kliendipoolse täitmise osas tuleb arvestada, et veebirakenduse loogika võib olla suurel määral realiseeritud JavaScripti abil, mis võimaldab dünaamiliselt luua uusi päringuid ja ühendusi. Seetõttu ei piisa ainult nähtavate funktsioonide eemaldamisest, vaid vajalik on piirata ka skriptide käivitamist ja nende võimet suhelda väliste teenustega, näiteks rakendades sisuturbe poliitikaid või muid täitmispiiranguid.

Samuti tuleb arvestada, et veebileht võib sisaldada suunamisi teistesse keskkondadesse, kus kehtivad erinevad reeglid ja kus võib olla võimalik nii autentimine kui ka suhtlus. Selliste juhtumite puhul tuleb

rakendada domeeni- ja suunamispõhist kontrolli, mis takistab kasutajal liikuda keskkondadesse, kus kontrollitud kasutustingimused ei ole tagatud.

Kokkuvõtlikult tähendab emta.ee veebikeskkonna lubatavuse tagamine vanglateenistuse vaates eelkõige seda, et tuleb välistada kõik funktsioonid, mis võimaldavad kasutajal end tuvastada, algatada andmevahetust või kasutada veebilehte suhtluskanalina. See eeldab nii autentimisvõimaluste täielikku blokeerimist kui ka laiemat tehnilist kontrolli kõigi andmeside mehhanismide üle, et tagada, et veebilehe kasutamine ei võimalda ühelgi viisil kontrollimatut suhtlust või andmete edastamist väljapoole vanglateenistuse järelevalvet.

PPA veebilehe (www.politsei.ee) puhul tuleb samuti lähtuda sellest, et tegemist ei ole üksnes informatiivse keskkonnaga, vaid veebirakendusega, mis sisaldab lisaks avalikule sisule ka mitmeid interaktiivseid teenuseid ning võimalusi asutusega suhtlemiseks. Sellest tulenevalt tuleb veebilehte käsitleda kui potentsiaalset andmesidekanalit, mille kaudu võib toimuda kasutaja ja väliskeskkonna vaheline info liikumine, ning hinnata selle kasutamist vanglate kontekstis eelkõige sellest aspektist.

Tehniliselt koosneb politsei.ee veebikeskkond avalikust infokihist ning mitmest funktsionaalsest komponendist, mis võimaldavad kasutajal algatada toiminguid või edastada andmeid. Nende hulka kuuluvad näiteks erinevad taotluste ja teadete esitamise vormid, vihje edastamise võimalused, kontaktivõimalused ning lingid e-teenustesse, mis võivad paikneda eraldi süsteemides. Sellised lahendused realiseeruvad tüüpiliselt HTTP POST päringute või JavaScripti kaudu tehtavate API-kutsetena, mille kaudu kasutaja sisestatud andmed edastatakse serveritesse. Vanglateenistuse vaates tuleb selliseid mehhanisme käsitleda kui potentsiaalseid suhtluskanaleid, kuna need võimaldavad kahepoolset või vähemalt ühepoolset kontrollimata andmeedastust.

Seetõttu on vajalik tuvastada ja piirata kõik sisendmehhanismid, mis võimaldavad kasutajal andmeid edastada. See hõlmab nii nähtavaid vorme kui ka võimalikke dünaamilisi lahendusi, mis võivad olla realiseeritud kliendipoolse skriptimise kaudu. Tehniliselt tähendab see kas vastavate elementide eemaldamist kasutajaliidesest või nende taga olevate päringute blokeerimist võrgu- või rakendustasandil (seda saaks teha vaid PPA), et vältida olukorda, kus kasutaja saab andmeid edastada ka siis, kui kasutajaliides seda otseselt ei võimalda.

Lisaks tuleb arvestada, et politsei.ee veebileht sisaldab mitmeid suunamisi ja viiteid teistele keskkondadele, sealhulgas riiklikele e-teenustele, kus võib olla vajalik kasutaja autentimine. Kuigi autentimine ei pruugi toimuda otse politsei.ee domeenis, võivad lingid viia keskkondadesse, kus on võimalik sisselogimine ning seeläbi isikustatud teenuste kasutamine. Sellest tulenevalt tuleb rakendada tehnilised piirangud, mis välistavad kõik sisselogimisvõimalused ka kaudsete suunamiste kaudu, blokeerides nii vastavad domeenid kui ka ümbersuunamismehhanismid.

Täiendavalt tuleb hinnata veebilehe poolt algatatavat väljaminevat liiklust. Ka avaliku sisu kuvamisel võib lehitseja luua ühendusi erinevate väliste teenustega, näiteks laadides skripte, kasutades analüütikateenuseid või pöördudes muude ressursside poole. Selliste ühenduste kaudu võib toimuda andmete edastamine, mistõttu tuleb rakendada ranget lubatud domeenide ja otspunktide loetelu ning blokeerida kõik ülejäänud ühendused. Seejuures on oluline jälgida mitte ainult otseseid päringuid, vaid ka võimalikke ümbersuunamisahelaid ja taustal toimuvat andmevahetust.

Kliendipoolse koodi osas tuleb arvestada, et JavaScript võib dünaamiliselt luua uusi ühendusi, laadida täiendavaid komponente või käivitada funktsionaalsusi, mis ei ole esmapilgul nähtavad. Seetõttu tuleb rakendada täitmispiiranguid, näiteks sisuturbe poliitikaid (*Content Security Policy*), mis piiravad lubatud skriptide ja ühenduste allikaid, ning vajadusel piirata või keelata aktiivne skriptimine, et välistada varjatud suhtlusmehhanismide tekkimine. Samuti tuleb eraldi hinnata kõiki multimeedia ja väliste komponentide kasutusi, näiteks lisatud kaarte, videolahendusi või muid interaktiivseid elemente, mis võivad sisaldada täiendavaid funktsionaalsusi või viiteid kolmandate osapoolte keskkondadele. Selliste komponentide puhul tuleb tagada, et need ei võimalda kasutajal liikuda edasi keskkondadesse, kus suhtlus või autentimine on võimalik.

PPA veebilehe kasutamise lubatavuse tagamine vanglate kontekstis tähendab seda, et tuleb eemaldada või blokeerida kõik funktsioonid, mis võimaldavad andmete sisestamist, suhtluse algatamist või sisselogimist, ning lisaks tagada, et kaudsete tehniliste mehhanismide kaudu ei teki võimalust kontrollimatuks andmesideks. See eeldab mitmekihilist kontrolli nii kasutajaliidese,

rakenduse kui ka võrgu tasemel, et välistada olukord, kus veebileht toimib vangile suhtluskanalina väljapoole vanglateenistuse järelevalvet.

Kaebuses on vaatluse all Maksu- ja Tolliameti (EMTA), Politsei- ja Piirivalveameti (PPA), Justiits- ja Digiministeeriumi (JDM) ja Riigiportaali eesti.ee veebilehed, millele kaebaja soovib juurdepääsu. EMTA veebilehe sisukaardilt nähtub veidi alla 400 veebilehe, mis omakorda võivad hargneda alamlehtedeks, millel võib paikneda veebilink või video, mis pärineb mõnest välisest domeenist. Iga leht, link video, fail tuleb üle kontrollida. Selleks tuleb veebilehitseja tööriistadega vaadelda veebilehitseja ja serveri vahel toimuvat suhtlust üle http protokolli. Iga lehe, lingi vm kohta tekib lehitseja võrgumonitooringu tööriistas kuni mitusada kannet, mis on vaja kõik üle kontrollida. Arvestades EMTA lehe mahtu, võib neid kandeid olla üle 10 000. Need sisaldavad kõiki ressursse, mida veebileht kasutab (sisu, kujundus, pildid, ikoonid jne). Suur osa nendest ressurssidest asuvad väljaspool EMTA domeeni, mis tähendab, et kõik need asukohad, kust ressurss laetakse, tuleb välja tuua lähteülesandesse. Selle töö käigus kontrollitakse ka seda, et vangile ei tekiks suhtlusvõimalusi läbi analüüsitava veebilehe. Lähteülesande koostamine võtab aega 2 nädalat, administraatori töö ja testimine 1,5 nädalat. Sellele lisanduks järjepidev töö veebilehega, st tuleb kontrollida, kas lehele on lisandunud uusi funktsioone, teabevälju, mille kaudu on võimalik teateid saata (nt e-postile mingit teavet tellida). Riskid ei pruugi ka sellise seire puhul olla tuvastatavad, sest kontrollija ei näe alati ette kinnipeetavast lähtuvat motivatsiooni, miks peaks mingit veebilehe funktsiooni kasutama mittesihtotstarbeliselt (vt VAPO ja AET-i näited). Paraku on nende riskide maandamine pea et võimatu, st ennetada neid ei ole võimalik, tegeleda saab üksnes tagajärjega, luues kinnipeetavatest lähtuva erilahenduse, mis võtab vanglalt järelevalve ressurssi, mida oleks otstarbekam suunata taasühiskonnastamisesse.

PPA ja eesti.ee veebilehtede ülesehitust arvestades saab öelda, et tegevuste maht ja toimingute sisu on suurusjärgus sama, mis on toodud välja eelmises punktis. Eesti.ee puhul eeldab enamik veebilehe kasutusvõimalustest isikutunnistuse abil autentimist, mis aga ei ole kinnipeetavatel võimalik. JDMi veebilehe puhul on töötlemise maht mõnevõrra väiksem, s.o u 40% tegevuste mahust võrreldes EMTA veebilehega.

Selgitame lisaks, et vaidlusaluste nelja veebilehe osas kui võtta arvesse kõik neli käsitletud veebikeskkonda – www.eesti.ee, EMTA (www.emta.ee), JDM (www.justdigi.ee) ja PPA (www.politsei.ee) –, siis tuleb kogukulu hinnata mitte üksikute lehtede summana lihtsas korrutuses, vaid arvestades nii ühekordset auditi- ja seadistuskulu kui ka püsivat seire- ja hoolduskulu. Esmane audit ja seadistamine kõigi nelja veebilehe puhul oleks lähtuvalt veebilehtede tehnilisest analüüsist kokku eesti.ee lehe puhul 10-15 tööpäeva, emta.ee puhul 8-12 tööpäeva, politsei.ee lehe puhul 6-10 tööpäeva, justdigi.ee puhul 4-7 tööpäeva, st kokku u 28-44 tööpäeva. Kui arvestada, et tööd tehakse paralleelselt 2–3 spetsialisti poolt, oleks tööde kestus u 2–4 nädalat , kokku u 30–45 tööpäeva. Rahaline kulu oleks u 7500–18 000 € (s.o ühekordne kulu). Sellele lisandub jooksev seire ja hooldus (aastane kulu). Kõigi nelja lehe koosmõjus oleks vaja tagada pidev muutuste jälgimine (kasutajaliides, lingid, API-d, autentimine), *whitelisti'de* uuendamine (domeenid, otspunktid, testimine (kas blokeeringud toimivad), intsidentide käsitlemine (kui midagi muutub ootamatult). See tähendaks lisaks vähemalt 1 täistööajaga spetsialist. Perioodilise lisakoormuse (auditid, muudatused) aastane töömaht põhiseire osas oleks u 200–220 tööpäeva ning lisaauditid u 20–40 tööpäeva. Kokku seega u 220–260 tööpäeva aastas, millega kaasneb rahaline kulu kokku u 60 000–70 000 € aastas. Selle juures tuleb arvestada, et veebilehti tuleb monitoorida igapäevaselt. Automatiseeritud monitooring peab olema pidev, sellele lisanduks regulaarne käsitsi kontroll (igapäevane ülesanne). Eriti kriitiliselt tuleb jälgida uute autentimisvoogude ilmumist, kui lisanduvad uued vormid või API otspunktid, uued välisdomeenid.

Kogukulu esimesel aastal esmasele auditile 7500–18 000 eurot, jooksvad kulud u 60 000–70 000 eurot, kokku seega kuni 88 000 eurot esimesel aastal ja igal järgneval aastal u 60 000–70 000 aastas. Rõhutame, et see kulu on üksnes analüüsitud nelja veebilehe puhul. Seega, nelja vaidlusaluse veebilehe turvaline lubamine vanglate kontekstis tähendab pidevat tehnilist järelevalvet (mitte ühekordset seadistust), vähemalt ühe spetsialisti püsivat töökoormust, kümnete tuhandete eurode suurust aastast kulu ning ka siis ei ole võimalik riski täielikult elimineerida, vaid üksnes seda maandada läbi järjepideva kontrolli.

e) Viru Vangla ning justiits- ja digiminister: ***milline on praegu juurdepääsetavate veebilehtede haldajate ja vangla või JDM-i (RIK-i/RIA) omavaheline suhtlus selleks, et samade (keelatud suhtlemisest tulenevate) riskide realiseerumist ära hoida?***

Eelnevalt selgitasin, millist töömahtu nõuab veebilehe põhjalik kontrollimine. Suures osas tehakse samu 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. Samuti on välja töötatud e-poe rakendus, mis võimaldab teha vangla poes oste mugavamalt ja tõhusamalt.

f) Viru Vangla ning justiits- ja digiminister: ***kui palju maksab praegu igakuiselt nende veebilehtede turvalisena hoidmine, millele kinnipeetavatel on juurdepääs lubatud.***

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 3000–8000 eurot. Iga lisanduva asutuse veebilehe lisandumine tähendab vanglateenistuse jaoks samasugust kulu.

Eeltoodud põhjendustele ja vastustele tuginevalt leian, et VangS § 31[1] esimene lause (kuni 31.03.2024 kehtinud redaktsioonis), samuti VangS § 31[1] lg 1 esimene lause (alates 01.04.2024 kehtivas redaktsioonis) ja VskE § 52[1] lg 1 (alates 31.03.2024 kehtivas redaktsioonis), mis koostoimes keelasid või keelavad kinnipeetavale juurdepääsu neljale vaidlusalusele veebilehele (JDM, EMTA, PPA, eesti.ee), on põhiseadusega kooskõlas.

Lugupidamisega

(allkirjastatud digitaalselt)

Liisa-Ly Pakosta
justiits- ja digiminister

Lisa:

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

Laura Glaase 51916910
Laura.Glaase@justdigi.ee