EUROOPA
KOMISJON

Brüssel, 14.2.2024
COM(2024) 64 final

KOMISJONI ARUANNE EUROOPA PARLAMENDILE JA NÕUKOGULE

määruse (EL) 2021/784 (mis käsitleb võitlemist terroristliku veebisisu levitamise vastu) rakendamise kohta

{SWD(2024) 36 final}

1. KOKKUVÕTE

Määrus (EL) 2021/784, mis käsitleb võitlemist terroristliku veebisisu levitamise vastu, annab liikmesriikidele Euroopa tasandi õigusraamistiku, et kaitsta kodanikke internetis terroristliku materjaliga kokkupuutumise eest. Määruse eesmärk on tagada digitaalse ühtse turu sujuv toimimine, käsitledes veebimajutusteenuste väärkasutamist terroristliku veebisisu üldsusele levitamiseks. Määrusega püütakse ära hoida seda, et terroristid kasutavad internetti oma sõnumite levitamiseks, et hirmutada, radikaliseerida ja värvata inimesi ning hõlbustada terrorirünnakute läbiviimist. See on eriti oluline praeguses olukorras, kus konfliktid ja ebastabiilsus mõjutavad Euroopa julgeolekut. Venemaa agressioonisõda Ukraina vastu ja Hamasi poolt 7. oktoobril 2023 Iisraeli vastu toime pandud terrorirünnak tõid internetis kaasa terroristliku sisu levitamise kasvu.

Ebaseadusliku sisu vastu võitlemise õigusraamistikku tugevdati veelgi digiteenuste õigusakti jõustumisega 16. novembril 2022. Digiteenuste õigusaktiga reguleeritakse selliste digiteenuste osutajate kohustusi, kes toimivad vahendajatena tarbijate ühendamisel sisu, teenuste ja kaupadega. Nii kaitstakse kasutajaid internetis paremini ja aidatakse kaasa turvalisema internetikeskkonna loomisele.

Terroristliku veebisisu levitamise vastu võitlemist käsitlevat määrust hakati kohaldama 7. juunil 2022. Määruse artikli 22 kohaselt esitab komisjon Euroopa Parlamendile ja nõukogule aruande määruse kohaldamise kohta (edaspidi „rakendusaruanne“).

Rakendamisaruanne põhineb sellise teabe hindamisel, mida liikmesriigid, Europol ja veebimajutusteenuse pakkujad määruses sätestatud kohustuste kohaselt esitavad. Hindamise põhjal võib määruse rakendamisega seotud peamised järeldused kokku võtta järgmiselt:

- 31. detsembri 2023. aasta seisuga oli **23 liikmesriiki** määranud asutuse(d), kellel on õigus teha määruses sätestatud eemaldamiskorraldusi[1]. Liikmesriikide ametiasutuste loetelu on kättesaadav komisjoni veebisaidil ja seda ajakohastatakse korrapäraselt[2].

- 31. detsembri 2023. aasta seisuga oli komisjon saanud teavet vähemalt **349 terroristliku sisu eemaldamise korralduse** kohta, mille on välja andnud kuue liikmesriigi (Hispaania, Rumeenia, Prantsusmaa, Saksamaa, Tšehhi ja Austria) pädevad asutused. Enamasti võeti nende peale kiiresti meetmeid terroristliku sisu eemaldamiseks või sellele juurdepääsu blokeerimiseks. See näitab, et määrusega ette nähtud vahendeid on hakatud kasutama ja need aitavad tagada, et veebimajutusteenuse pakkujad eemaldavad terroristliku sisu kiiresti vastavalt artikli 3 lõikele 3. Komisjonile esitatud teabe kohaselt ei ole neid eemaldamiskorraldusi vaidlustatud.

[1] Komisjoni poolt määruse artikli 12 lõike 4 kohaselt loodud veebiregistris on loetletud artikli 12 lõikes 1 osutatud pädevad asutused ja artikli 12 lõike 2 kohaselt iga pädeva asutuse juurde määratud või asutatud kontaktpunkt. Registrit ajakohastatakse korrapäraselt liikmesriikidelt saadud teadete põhjal. Riikide pädevate asutuste ja kontaktpunktide loetelu (europa.eu).

[2] Riikide pädevate asutuste ja kontaktpunktide loetelu (europa.eu).

- Määruse kohaldamisel, eriti eemaldamiskorralduste menetlemisel, on liikmesriikide pädevate asutuste ja Europoli, eelkõige Europoli internetisisust teavitamise üksuse (EU IRU) tegevus **hästi koordineeritud**.
- 3. juulil 2023 võeti kasutusele Europoli vahend **PERCI**[3]. Mõned liikmesriigid on seda vahendit edukalt kasutanud nii eemaldamiskorralduste kui ka esildiste[4] edastamiseks. Hispaania, Saksamaa, Austria, Prantsusmaa ja Tšehhi pädevad asutused on kasutanud seda vahendit eemaldamiskorralduste edastamiseks. Alates PERCI käivitamisest 3. juulil kuni 31. detsembrini 2023 menetleti PERCI raames kokku vähemalt 14 615 esildist.
- Kuigi määrus ei sisalda esildiste kohta konkreetseid meetmeid, on komisjonile esitatud teabe kohaselt alates määruse kohaldamise algusest **hakanud veebimajutusteenuse pakkujad esildistele rohkem reageerima**.
- Komisjoni andmetel ei ole 31. detsembri 2023. aasta seisuga tuvastatud, et ükski veebimajutusteenuse pakkuja oleks puutunud kokku terroristliku sisuga, nagu on määratletud määruse artikli 5 lõikes 4. Selline tuvastamine on kõnealuses artiklis kirjeldatud erimeetmete kohaldamise eeltingimus. Veebimajutusteenuse pakkujate esitatud läbipaistvusaruannete kohaselt on veebimajutusteenuse pakkujad aga võtnud meetmeid, **et käsitleda oma teenuste väärkasutamist terroristliku sisu levitamiseks**. Eelkõige on nad võtnud vastu konkreetsed tingimused terroristliku sisu leviku piiramiseks ning kohaldavad sel otstarbel ka muid sätteid ja meetmeid.
- Veebimajutusteenuse pakkujad on võtnud vastu ka meetmed, et teatada **otsesest ohust elule** vastavalt määruse artikli 14 lõikele 5.

Komisjon kuulutas 2021. aastal välja projektikonkursi, et toetada **väiksemaid veebimajutusteenuse pakkujaid** määruse rakendamisel. 2022. aastal sõlmis komisjon lepingud kolme projekti jaoks (vt punkt 4.8), millega alustati tööd 2023. aastal ja mis on juba andnud mõningaid tulemusi, aidates väikeettevõtjatel määruse nõudeid täita.

Komisjon on algatanud rikkumismenetluse 22 liikmesriigi suhtes, kes ei ole määranud määruse artikli 12 lõike 1 kohaselt pädevaid asutusi ega täitnud artikli 12 lõigetest 2 ja 3 ning artikli 18 lõikest 1 tulenevaid kohustusi, ning saatis 26. jaanuaril 2023 välja **ametlikud kirjad**[5]. Pärast rikkumismenetluste algatamist kasvas nende liikmesriikide arv, kes teatasid eemaldamiskorralduste menetlemise eest vastutavatest pädevatest asutustest, nagu nähtub veebiregistris avaldatud teabest[6]. 21. detsembriks 2023 oli üksteist 2023. aasta jaanuaris algatatud rikkumismenetlust lõpetatud[7].

[3]PERCI (*Plateforme Européenne de retraits des Contenus illégaux sur Internet*) on ebaseadusliku sisu eemaldamise platvorm, mille on välja töötanud ja mida haldab Europol. See toetab määruse rakendamist, pakkudes muu hulgas tehnilist lahendust veebimajutusteenuse pakkujatele suunatud esildiste ja eemaldamiskorralduste töötlemiseks.

[4] Esildised on mehhanism, mille abil hoiatada veebimajutusteenuse pakkujaid, et need saaksid vabatahtlikult kaaluda, kas sisu vastab nende tingimustele. Määruses (põhjendus 40) on märgitud, et esildised on osutunud tõhusaks ja peaksid eemaldamiskorralduste kõrval kasutusele jääma.

[5] Vt pressiteade: Terroristlik veebisisu (europa.eu).

[6] Riikide pädevate asutuste ja kontaktpunktide loetelu (europa.eu). Veebiregistris on teave 23 liikmesriigi pädevate asutuste kohta, kes teevad eemaldamiskorraldusi vastavalt artikli 12 lõike 1 punktile a.

[7] Soome, Malta, Tšehhi, Taani, Rumeenia, Rootsi, Läti, Hispaania, Leedu, Austria ja Slovakkia.

Liikmesriikide ja Europoli kaudu veebimajutusteenuse pakkujatelt saadud teabe põhjal andis komisjon hinnangu, et määruse kohaldamisel on olnud terroristliku veebisisu leviku piiramisele **positiivne mõju**.

2. TAUST

Määrust hakati kohaldama 7. juunil 2022. Selle eesmärk on tagada digitaalse ühtse turu sujuv toimimine, käsitledes veebimajutusteenuste väärkasutamist terroristliku veebisisu üldsusele levitamiseks. See annab liikmesriikidele eemaldamiskorralduse näol sihipärase vahendi, mille abil käsitleda terroristliku veebisisu levitamist, ning võimaldab liikmesriikidel nõuda iga suurusega veebimajutusteenuse pakkujatelt konkreetsete meetmete võtmist, et kaitsta oma teenuseid terroristliku sisuga kokkupuutumisel terroristide poolt ärakasutamise eest.

Lisaks laiendati koos digiteenuste õigusakti jõustumisega 16. novembril 2022 regulatiivset keskkonda laia kohaldamisalaga horisontaalsete õigusaktidega, mille eesmärk on tagada tarbijatele turvalisem digikeskkond, tõhusad meetmed ebaseadusliku sisu vastu võitlemiseks ja läbipaistvamad teenusetingimused. Digiteenuste õigusaktiga antakse komisjonile ulatuslikud järelevalve-, uurimis- ja jõustamisvolitused, et võtta meetmeid väga suurte digiplatvormide ja otsingumootorite suhtes. Need meetmed hõlmavad teabenõudeid ja ettevõtete sisu modereerimise meetmete uurimist koos võimalusega määrata trahve.

Digiteenuste õigusakt võimaldab võidelda ebaseadusliku sisu kõigi vormide vastu ja võimaldab komisjonil nõuda platvormidelt andmeid selle tõendamiseks, et nad täidavad oma kohustusi seoses sisu eemaldamisega. Terroristliku veebisisu vastane määrus on sellise ebaseadusliku sisu vastu võitlemisel veel võimsam vahend – see sisaldab õiguslikku kohustust eemaldada sisu ühe tunni jooksul pärast eemaldamiskorralduse kättesaamist ja tõhusaid karistusmehhanisme.

Nagu Europol on viimastel aastatel avaldatud terrorismi olukorda ja suundumusi käsitlevates aruannetes (TE-SAT-aruanded)[8] rõhutanud, kasutavad terroristid internetti laialdaselt oma sõnumite levitamiseks, et hirmutada, radikaliseerida ja värvata inimesi ning hõlbustada terrorirünnakute läbiviimist. Kuigi vabatahtlikud meetmed ja mittesiduvad soovitused on aidanud vähendada terroristliku veebisisu kättesaadavust, vähendasid teatavad asjaolud – sealhulgas vabatahtlikud mehhanismid kasutusele võtnud veebimajutusteenuse pakkujate väike arv[9] ja liikmesriikide menetluseeskirjade killustatus – liikmesriikide ja veebimajutusteenuse pakkujate vahelise koostöö tulemuslikkust ja tõhusust ning tingisid vajaduse kehtestada reguleerivad meetmed[10]. Seetõttu on määruse tõhus kohaldamine võitluses terroristliku veebisisu levitamise vastu keskse tähtsusega. Komisjon on liikmesriikide pädevaid asutusi selles protsessis ennetavalt toetanud.

[8] Europoli TE-SAT 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf and 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

[9] Euroopa Komisjon, (2018) Impact Assessment accompanying the Proposal for a Regulation on preventing the dissemination of terrorist content online, SWD(2018) 408 final, viimati vaadatud 4. mail 2023 aadressil: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN.

[10] Samas.

Määruse artikli 22 kohaselt oli komisjonil kohustus esitada Euroopa Parlamendile ja nõukogule 7. juuniks 2023 määruse kohaldamise kohta aruanne (edaspidi „rakendusaruanne“), milles tuginetakse liikmesriikide esitatud teabele, mis omakorda tugineb osaliselt veebimajutusteenuse pakkujate esitatud teabele (artikkel 21). Viivitus rakendamisaruande esitamisel on tingitud ühelt poolt sellest, et liikmesriigid ja veebimajutusteenuse pakkujad edastasid põhiteabe komisjonile hilinemisega. Teiselt poolt peeti oluliseks kajastada rakendamisaruandes PERCI kasutamist, mis hakkas toimima 3. juulil 2023 ja mida on sellest ajast alates kasutatud eemaldamiskorralduste töötlemiseks vastavalt määrusele.

Käesoleva rakendamisaruande ainus eesmärk on anda faktiline ülevaade määruse kohaldamisega seotud küsimustest. See ei sisalda määruse tõlgendusi ja selles ei avaldata arvamust määruse kohaldamisel kasutatud tõlgenduste või muude meetmete kohta.

Kooskõlas määruse artikli 21 lõikega 2 pidi komisjon samaks kuupäevaks (7. juuniks 2023) koostama üksikasjaliku kava määruse väljundite, tulemuste ja mõju seiramiseks. Täpsemalt tuleks seirekavas sätestada andmete ja muu vajaliku tõendusmaterjali kogumisel kasutatavad näitajad ja vahendid ning kogumise sagedus. Selline kava on esitatud lisatud komisjoni talituste töödokumendis. Selles määratakse kindlaks meetmed, mida komisjon ja liikmesriigid peavad võtma andmete ja muude tõendite kogumiseks ja analüüsimiseks, et jälgida määruse kohaldamise edenemist ja mõju ning hinnata määrust vastavalt artiklile 23.

3. ARUANDE EESMÄRK JA METOODIKA

Käesoleva aruande eesmärk on hinnata määruse kohaldamist ja selle senist mõju terroristliku veebisisu levitamise piiramisele. Muu hulgas hinnatakse liikmesriikide ja veebimajutusteenuse pakkujate võetud meetmeid, näiteks nende teenusetingimuste ja kogukonnasuuniste muutmist, nende täitmist ja eemaldamiskorraldustele reageerimist.

Selleks kogus komisjon liikmesriikidelt, Europoli internetisisust teavitamise üksuselt (EU IRU) ja veebimajutusteenuse pakkujatelt teavet, muu hulgas määruse artiklite 7, 8 ja 21 kohastes läbipaistvus- ja seirearuannetes sisalduvat teavet. Artiklite 8 ja 21 kohane teave saadi 18 liikmesriigilt. Teavet veebimajutusteenuse pakkujate võetud meetmete kohta koguti nende iga-aastaste läbipaistvusaruannete, Europoli, ja komisjoni talitustega toimunud otsese vabatahtliku teabevahetuse kaudu. Käesolev rakendamisaruanne sisaldab teavet, mille komisjon sai kuni 31. detsembrini 2023.

Seire- ja läbipaistvuskohustused (artiklid 21, 7 ja 8)

Rakendusaruande koostamiseks on liikmesriigid vastavalt määruse artikli 21 lõikele 1 kohustatud koguma oma pädevatelt asutustelt ja oma jurisdiktsiooni alla kuuluvatelt veebimajutusteenuse pakkujatelt teavet iga aasta 31. märtsiks. See hõlmab teavet meetmete kohta, mida nad on võtnud määruse kohaselt eelmisel kalendriaastal. Artikli 21 lõikes 1 on osutatud sellele, mis liiki teavet peaksid liikmesriigid määruse täitmiseks võetud meetmete kohta koguma: näiteks üksikasjad eemaldamiskorralduste kohta, uurimise huvides säilitatud sisule juurdepääsu taotluste, kaebuste lahendamise menetluste ning halduslike ja kohtulike läbivaatamiste arv.

Määruse artikli 7 lõike 1 kohaselt peavad veebimajutusteenuse pakkujad oma tingimustes selgelt esitama terroristliku sisu levitamise vastu võitlemise põhimõtted, sealhulgas asjakohasel juhul sisulise selgituse erimeetmete toimimise kohta.

Lisaks on määruse artikli 7 lõikes 2 sätestatud, et iga veebimajutusteenuse pakkuja, kes on asjaomasel kalendriaastal võtnud terroristliku sisu levitamise vastaseid meetmeid või kellelt on nõutud meetmete võtmist vastavalt määrusele, teeb üldsusele kättesaadavaks läbipaistvusaruande selliste meetmete võtmise kohta antud aastal. Aruanne tuleks avaldada enne järgmise aasta 1. märtsi.

Määruse artikli 7 lõikes 3 on sätestatud miinimumteave, mida need läbipaistvusaruanded peaksid sisaldama: näiteks terroristliku sisu kindlakstegemiseks ja sellele juurdepääsu blokeerimiseks võetud meetmed, eemaldatud ja/või ennistatud ühikute arv ning kaebuste tulemused.

Määruse artikli 8 kohaselt avaldavad liikmesriikide määratud pädevad asutused igal aastal läbipaistvusaruanded oma määruse kohase tegevuse kohta. Artikli 8 lõikes 1 on osutatud miinimumteabele, mida need aruanded peaksid sisaldama[11].

31. detsembri 2023. aasta seisuga oli 18 liikmesriiki saatnud komisjonile teabe määruse kohaselt võetud meetmete kohta ning 23 liikmesriiki oli määranud asutus(ed), kellel on õigus teha määruses sätestatud eemaldamiskorraldusi.

4. KONKREETSED HINNATAVAD TEEMAD

4.1. EEMALDAMISKORRALDUSED (artikkel 3)

31. detsembri 2023. aasta seisuga olid Hispaania, Rumeenia, Prantsusmaa, Saksamaa, Austria ja Tšehhi pädevad asutused teatanud komisjonile vähemalt 349 eemaldamiskorraldusest, mille adressaadid olid Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L, FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net ja Catbox.

Hispaania pädev asutus (CITCO – Centro de Inteligencia contra el Terrorismo y el Crimen Organizado) on saatnud 62 eemaldamiskorraldust, Rumeenia pädev asutus (ANCOM – Autoritatea Națională pentru Administrare și Reglementare în Comunicații) kaks eemaldamiskorraldust ja Prantsusmaa pädev asutus (OCLCTIC – L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) 26 eemaldamiskorraldust. Pärast Hamasi terrorirünnakut Iisraeli vastu on Saksamaa pädev asutus (BKA – Bundeskriminalamt) saatnud 249 eemaldamiskorraldust.

Hispaania pädev asutus on saatnud 62 eemaldamiskorraldust: 18 enne PERCI käivitamist ja 44 PERCI kaudu. Ta kirjeldas üksikasjalikult eemaldamiskorralduste saatmist ja esimeste eemaldamiskorralduste järelmeetmeid, mis on määruse mõju paremaks mõistmiseks väga oluline.

[11] Vt määruse (EL) 2021/784 artikli 8 lõike 1 tekst https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32021R0784

Hispaania pädev asutus tegi kaks esimest eemaldamiskorraldust 24. aprillil 2023[12]. Need olid seotud kahe terroristliku sisu ühikuga, millest üks puudutas parempoolset terrorismi ja teine džihadismi. Esimene eemaldamiskorraldus tehti PDF-dokumendi kohta, mis oli postitatud piiramatu juurdepääsuga Telegrami kanalile ning toetas terroristlikku vägivalda ja ülistas parempoolseid terrorirünnakuid. Teine eemaldamiskorraldus tehti Internet Archive'i üles laaditud terroristliku sisuga video kohta, mis kujutas terroriorganisatsiooni Islamiriik džihadiste lahingus. Need kaks ühikut eemaldati mõlemalt platvormilt vähem kui tunni jooksul ehk kooskõlas määruse artikli 3 lõikega 3. Hispaania ametiasutuste esitatud hinnangus selgitati, et nad eelistasid kasutada esildise asemel eemaldamiskorraldust ja seda peamiselt kahel põhjusel: vastavus määruse eemaldamiskorraldusi käsitlevatele nõuetele ja asja kiireloomulisus. Hispaania pädev asutus saatis seejärel järgmised eemaldamiskorraldused.

Hispaania ametiasutus tõi esile probleemid seoses sellega, et üks veebimajutusteenuse pakkuja (Meta) kasutab eemaldamiskorralduste jaoks veebivormi, selle asemel et pakkuda otsekontakti. Veebivorm tekitas probleeme ka suhtlemisel selle liikmesriigi pädeva asutusega, kus on veebimajutusteenuse pakkuja peamine tegevuskoht.

Prantsusmaa pädev asutus väljastas oma esimese eemaldamiskorralduse 13. juulil 2023 jagamisplatvormile Justpaste.it, mis eemaldas terroristliku sisu ühe tunni jooksul. Kõnealune sisu oli Al Qaeda, täpsemalt tema India haru (AQIS) meediaorgani Rikan Ka Mimber propaganda. Europoli PERCI platvormil kinnitati sisu täielikku eemaldamist.

Saksamaa pädev asutus väljastas 16., 18. ja 24. oktoobril 2023 vastavalt kuus, 16 ja viis eemaldamiskorraldust Hamasi ja Palestiina Islami Džihaadi propaganda kohta. Juurdepääs sisule blokeeriti ELis kooskõlas määruse artikli 3 lõikega 3. Saksamaa pädev asutus saatis kõigepealt esildised ja tegi seejärel eemaldamiskorraldused, kuna esildistele ei reageeritud. Pärast Hamasi rünnakut 7. oktoobril 2023 on Saksamaa pädev asutus saatnud 249 eemaldamiskorraldust, peamiselt Telegramile[13].

Tšehhi pädev asutus ja Austria pädev asutus väljastasid vastavalt X-ile ja Telegramile kaks ja kaheksa eemaldamiskorraldust.

Seoses asjaoluga, et üks veebimajutusteenuse pakkuja kasutab eemaldamiskorralduste vastuvõtmiseks veebivormi, osutasid Hispaania ametiasutused kahele probleemile: 1) seoses määruse artikli 3 lõikega 2 ei võimalda veebivorm liikmesriikide pädevatel asutustel anda enne esimese eemaldamiskorralduse tegemist veebimajutusteenuse pakkujale teavet kohaldatavate menetluste ja tähtaegade kohta; 2) seoses artikli 4 lõikega 1 ei võimalda veebivorm esitada eemaldamiskorralduse koopiat samaaegselt selle liikmesriigi pädevale asutusele, kus on veebimajutusteenuse pakkuja peamine tegevuskoht, ja veebimajutusteenuse pakkuja seaduslikule esindajale.

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo
[13] Komisjonile kättesaadava teabe kohaselt.

4.2 PIIRIÜLESED EEMALDAMISKORRALDUSED (artikkel 4)

Hispaania pädev asutus ei saanud 2023. aasta aprillis tehtud kahe esimese eemaldamiskorralduse koopiaid saata selle liikmesriigi asutusele, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või seaduslik esindaja, kuna kummalgi veebimajutusteenuse pakkujal ei olnud sel ajal ELis peamist tegevuskohta ega määratud esindajat. Järgnevate eemaldamiskorralduste koopiad saatis Hispaania pädev asutus selle liikmesriigi pädevale asutusele, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või seaduslik esindaja.

Liikmesriigid märkisid, et eemaldamiskorralduste edastamine kolmandates riikides asuvatele veebimajutusteenuse pakkujatele, kes ei ole veel täitnud kohustust määrata ELis seaduslik esindaja, on keeruline. Sellega seoses toetas komisjon liikmesriike selle tagamisel, et veebimajutusteenuse pakkujad täidaksid oma kohustuse määrata ELis seaduslik esindaja ja kontaktpunkt (määruse artikli 15 lõige 1), näiteks e-posti aadress, et tagada viivitamatu tegutsemine. Lisaks on komisjon tuletanud veebimajutusteenuse pakkujatele nende kohustusi meelde mitmesugustel foorumitel, sealhulgas ELi internetifoorumil.

Komisjonile kättesaadava teabe kohaselt ei ole ükski selle liikmesriigi pädev asutus, kus asub veebimajutusteenuse pakkuja peamine tegevuskoht, seni kontrollinud eemaldamiskorraldust vastavalt määruse artiklile 4, et teha kindlaks, kas sellega rikutakse tõsiselt või ilmselt määrust või põhiõigusi ja -vabadusi, kuna ühtegi põhjendatud kontrollitaotlust ei ole siiani esitatud. Seetõttu ei ole ükski ametiasutus seni tuvastanud, et mõni eemaldamiskorraldus oleks rikkunud määrust või põhiõigusi.

Ükski veebimajutusteenuse pakkuja ei ole seni taastanud sellise eemaldamiskorralduse objektiks olevat sisu (või sellele juurdepääsu), mille kohta on tehtud määruse artikli 4 kohane kontroll, sest sellist kontrolli ei ole toimunud ja ennistamistaotlusi ei ole esitatud. Seega puudub teave selle kohta, kui kaua kulub tavaliselt sisu või sellele juurdepääsuks taastamiseks, või vajalike meetmete kohta, mida veebimajutusteenuse pakkujad võtavad sisu taastamiseks või sellele uuesti juurdepääsu võimaldamiseks.

4.3. ÕIGUSKAITSEVAHENDID (artikkel 9)

Komisjonile kättesaadava teabe kohaselt ei ole veebimajutusteenuse pakkujad seni eemaldamiskorraldusi või artikli 5 lõike 4 kohaseid otsuseid kohtutes vaidlustanud. Üks veebimajutusteenuse pakkuja väitis siiski, et eemaldamiskorraldust ei ole võimalik täita.

Liikmesriikide esitatud teabe kohaselt[14] on vähemalt kaksteist liikmesriiki kehtestanud tõhusad menetlused, mis võimaldavad veebimajutusteenuse pakkujatel ja sisuteenuse pakkujatel vaidlustada tehtud eemaldamiskorraldus ja/või artikli 4 lõike 4 või artikli 5 lõike 4, 6 või 7 kohane otsus pädeva asutuse liikmesriigi kohtutes (artikli 9 lõiked 1 ja 2). Liikmesriikides, kus sellised meetmed on kehtestatud, osutatakse nendes enamasti kohtuasjadele. Seda, kas need meetmed on

[14] Esitatud teave ei pruugi olla täielik. Vaja oleks täiendavaid hindamisi, et saada täielik ja täielikult ajakohane ülevaade sellest, kuidas liikmesriigid rakendasid nõuet tagada tõhusate õiguskaitsemeetmete kättesaadavus.

„tõhusad“ või eriomased määrusele, ei saa liikmesriikidelt siiani saadud andmete põhjal siiski kindlaks teha, kuna seni ei ole ühtegi otsust vaidlustatud.

4.4. ERIMEETMED JA LÄBIPAISTVUS (artiklid 5 ja 7)

Olemasoleva teabe kohaselt ei ole seni ükski veebimajutusteenuse pakkuja määruse artikli 5 lõike 4 tähenduses terroristliku sisuga kokku puutunud. Järelikult ei kohaldata selles artiklis sätestatud erimeetmete võtmise nõuet (veel) ühegi veebimajutusteenuse pakkuja suhtes.

Siiski võib märkida, et veebimajutusteenuse pakkujate esitatud läbipaistvusaruannete kohaselt on mitu veebimajutusteenuse pakkujat võtnud meetmeid, et käsitleda oma teenuste väärkasutamist terroristliku sisu levitamiseks; eelkõige on nad võtnud vastu konkreetsed tingimused terroristliku sisu leviku piiramiseks ning kohaldavad sel otstarbel ka muid sätteid ja meetmeid. Nagu eespool märgitud, peavad veebimajutusteenuse pakkujad tagama artikli 7 kohaselt läbipaistvuse mitte ainult läbipaistvusaruandluse kaudu, vaid ka lisades oma tingimustesse selge teabe.

4.5. OTSENE OHT ELULE (artikli 14 lõige 5)

Määruse artikli 14 lõikes 5 on sätestatud, et kui veebimajutusteenuse pakkuja saab teadlikuks terroristlikust sisust, millega kaasneb otsene oht elule, teavitab ta sellest viivitamata asjaomastes liikmesriikides kuritegude uurimise ja nende eest süüdistuse esitamisega tegelevaid pädevaid asutusi. Kui asjaomaseid liikmesriike ei ole võimalik kindlaks teha, edastab veebimajutusteenuse pakkuja teabe asjakohaste järelmeetmete võtmiseks Europolile.

31. detsembriks 2023 oli komisjonile teatatud üheksast juhtumist, kus Europoli internetisisust teavitamise üksus on saanud teavet terroristliku sisu kohta, millega kaasneb otsene oht elule. Kuna määruse artikli 14 lõikes 5 ei ole sätestatud kohustust kõikidel juhtudel Europoli teavitada, võib teadete arv olla suurem. Hispaania oli ainus liikmesriik, kes esitas teavet artikli 14 lõike 5 kohaldamise kohta. 18. aprillil 2023 said Hispaania ametiasutused Amazonilt teate väidetava terroristliku sisu kohta, millega kaasneb otsene oht elule, Twitchi videomängude platvormil. Hindamisel leiti, et sisu ei ole määruse tähenduses terroristlik sisu, millega kaasneb otsene ohtu elule.

4.6. VEEBIMAJUTUSTEENUSE PAKKUJATE, PÄDEVATE ASUTUSTE JA EUROPOLI KOOSTÖÖ (artikkel 14)

Nagu eespool mainitud, on Europol välja arendanud platvormi PERCI, et toetada määruse rakendamist, tsentraliseerides, koordineerides ja hõlbustades **eemaldamiskorralduste ja esildiste edastamist** liikmesriikidelt veebimajutusteenuse pakkujatele. Platvorm toimib alates 3. juulist 2023. Enne PERCI täielikku rakendamist oli Europol kehtestanud erandolukorra menetluse, et toetada eemaldamiskorralduste käsitsi edastamist, sisu dekonfliktimist, et vältida sekkumist käimasolevatesse uurimistesse, ja kriisile reageerimist otsese ohu korral elule.

PERCI on ühtne süsteem, mis võimaldab pädevatel asutustel, veebimajutusteenuse pakkujatel ja Europolil teha määrusega hõlmatud küsimustes koostööd, nagu on ette nähtud määruse artiklis 14. PERCI:

- on pilvepõhine lahendus, mille eesmärk on tagada pilvandmetöötlusel turvalisus ja andmekaitse;
- on koostööl põhineva ja reaalajas toimuva teabevahetuse ja koordineerimise ühtne platvorm, mis toetab terroristliku sisu kiiret eemaldamist;
- hõlbustab piiriüleste eemaldamiskorralduste kontrolli;
- tugevdab dekonfliktimist, mis on oluline vältimaks olukorda, kus ühe liikmesriigi pädev asutus saadab eemaldamiskorralduse teises liikmesriigis käimasoleva uurimise objektiks oleva sisu kohta;
- võimaldab veebimajutusteenuse pakkujal saada eemaldamiskorraldusi ühtsel ja standarditud viisil ühest kanalist.

PERCI võimaldab edastada ka esildisi.

Lisaks sellele, et PERCI on oluline seoses esildistega (vt määruse põhjendus 40), hõlbustab see praegu eemaldamiskorralduste edastamist (artiklid 3 ja 4), liikmesriikide aruandlust (artikkel 8) ja koordineerimist ning dekonfliktimist seoses käimasoleva uurimisega, mis puudutab sisu, mille kohta eemaldamiskorraldus kavatsetakse saata (artikkel 14). PERCI-t arendatakse praegu edasi, et see hakkaks toetama määrusest tulenevaid lisaülesandeid, nagu piiriüleste eemaldamiskorralduste kontroll (artikkel 4)[15].

Liikmesriigid kinnitasid, et vastavalt määruse artiklile 14:

- vahetavad pädevad asutused teavet, koordineerivad ja teevad koostööd teiste pädevate asutustega;
- vahetavad pädevad asutused teavet, koordineerivad ja teevad koostööd Europoliga;
- on olemas mehhanismid koostöö tõhustamiseks, vältides samal ajal sekkumist teistes liikmesriikides toimuvatesse uurimistesse;
- enamik liikmesriike peab PERCI-t eemaldamiskorralduste edastamisel eelistatud vahendiks, kuna see võimaldab koordineerida tegevust dekonfliktimise abil.

4.7. MÕJU ESILDISTELE

Esildised terroristliku sisu kohta on vabatahtlik vahend, mida kasutati juba enne määruse vastuvõtmist. Kuigi määrus ei sisalda esildiste kohta konkreetseid norme, ei takista miski

[15] Üksikasjalikum teave: artiklid 3 ja 4: eemaldamiskorralduste edastamine; artikli 3 lõiked 6–8: veebimajutusteenuse pakkujate tagasiside; artikli 4 lõiked 3–7: kontrollimehhanism; artikkel 7: aruandlus; artikli 14 lõige 1: dekonfliktimine, koordineerimine, topelttöö vältimine; artikli 14 lõige 3: turvaline sidekanal; artikli 14 lõige 4: Europoli loodud spetsiaalse vahendi kasutamine; artikli 14 lõige 5: teavitamine otsesest ohust elule; põhjendus 40: esildiste edastamine.

liikmesriike ja Europoli määruse põhjenduse 40 kohaselt kasutamast terroristliku veebisisu vastu võitlemiseks esildisi.

Europoli internetisisust teavitamise üksus on alates oma loomisest 2015. aastal aktiivselt tegelenud terroristliku veebisisu tuvastamise ja selle kohta veebimajutusteenuse pakkujatele esildiste tegemisega ning loonud vahendeid (nt PERCI ja varem IRMA[16]), et hõlbustada esildiste edastamist.

Komisjonile esitatud teabe kohaselt kasutavad liikmesriikide ametiasutused teatavate veebimajutusteenuse pakkujate puhul jätkuvalt esildisi. Samas võivad nad kaaluda eemaldamiskorralduste tegemist veebimajutusteenuse pakkujatele, kes ei reageeri esildistele, või muudel põhjustel, näiteks kui sisu on vaja kiiresti eemaldada.

4.8. VÄIKSEMATE VEEBIMAJUTUSTEENUSE PAKKUJATE TOETAMINE MÄÄRUSE RAKENDAMISEL

Määrusega on kehtestatud veebimajutusteenuse pakkujatele mitmesuguseid kohustusi. Suurtel veebimajutusteenuse pakkujatel on tavaliselt määruse rakendamiseks vajalik tehniline võimekus, inimkontrolli suutlikkus ja teadmised olemas, kuid väikeste pakkujate rahalised, tehnilised ja inimressursid ning oskusteave võivad olla piiratumad. Samal ajal püüavad pahatahtlikud osalejad üha enam väiksemate veebimajutusteenuste pakkujate teenuste nõrkusi ära kasutada. See võib tuleneda ka asjaolust, et suuremad veebimajutusteenuse pakkujad modereerivad sisu tõhusamalt. Kuigi see suundumus näitab sisu modereerimise meetmete edukust, näitab see ka vajadust toetada väiksemaid veebimajutusteenuse pakkujaid suutlikkuse ja teadmiste suurendamisel, et täita määruse nõudeid.

Sellele probleemile reageerimiseks algatas komisjon Sisejulgeolekufondi raames projektikonkursi, et toetada väiksemaid veebimajutusteenuse pakkujaid määruse rakendamisel[17]. Komisjon valis välja kolm projekti,[18] mida toetada kolmeosalise lähenemisviisiga. Esiteks teavitades ja suurendades teadlikkust määruse normidest ja nõuetest, teiseks töötades välja, rakendades ja võttes kasutusele vahendid ja raamistikud, mida on vaja terroristliku veebisisu levitamise vastu võitlemiseks, ning kolmandaks jagades kogu tööstusharus kogemusi ja parimaid tavasid.

Nimetatud kolm projekti käivitati 2023. aastal ja need on juba andnud väärtuslikke tulemusi. Näiteks leiti FRISCO projekti kaardistamisaruandes,[19] et mikro- ja väikestel veebimajutusteenuse

[16] Europol lõi 2016. aastal internetisisust teavitamise haldamise rakenduse (IRMA), et toetada internetipõhiste teenuste osutajatele ebaseadusliku sisu kohta esildiste tegemist. Algselt said IRMA-le juurdepääsu Europoli töötajad ja seitsme liikmesriigi internetisisust teavitamise üksused. 3. juulil 2023 asendati IRMA PERCI-ga.

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-tco_en.pdf

[18] 1) Tehisintellektil põhinev raamistik mikro- (ja väikeste) veebimajutusteenuse pakkujate toetamiseks terroristlikust veebisisust teatamisel ja selle eemaldamisel (ALLIES), 2) võitlus terroristliku veebisisu vastu (FRISCO) ja 3) Technology Against Terrorism Europe (TATE). Lisateave: Rahastamine ja hanked (europa.eu).

[19] Küsitlus viidi läbi kuuekuulisel ajavahemikul, mis lõppes 2023. aasta mais. Aruande alus on 48 Euroopa veebimajutusteenuse pakkuja tagasiside, 33 vastust veebiküsitlusele ja 15 vestlust. FRISCO, *D2.1: Mapping Report on needs and barriers for compliance Understanding small and micro hosting service providers' needs and awareness in relation to implementing the TCO Regulation requirements*, kättesaadav aadressil Deliverables | Frisco (friscoproject.eu).

pakkujatel on üldiselt määrusest väga piiratud teadlikkus ja teadmised, ning rõhutati, et kuna neil puuduvad sageli ööpäevaringsed teenused, võib neil esineda raskusi, et eemaldamiskorraldustele ühe tunni jooksul vastata. Probleemiks on vahendite nappus, samuti õiguskaitseasutustega suhtlemise kanalite loomine. Enam kui pooled küsitletud veebimajutusteenuse pakkujad ei modereeri kasutajate loodud sisu ja märkisid, et nad ei ole oma platvormidel kunagi terroristliku sisuga kokku puutunud. Kui nende veebimajutusteenuse pakkujate platvormidel peaks sellist sisu esinema, võtavad nad tõenäoliselt ühekordseid meetmeid.

Nende kolme projekti kaudu toetatakse väikesi veebimajutusteenuse pakkujaid nende püüdlustes järgida määruse eeskirju. Muu hulgas luuakse kontaktpunkte ja rakendatakse mehhanisme kasutajate kaebuste jaoks.

Lisaks võib määruse artikli 3 lõige 2 – mille kohaselt tuleb veebimajutusteenuse pakkujatele, kellele ei ole varem eemaldamiskorraldust tehtud, esitada õigeaegselt teave kohaldatavate menetluste ja tähtaegade kohta – olla eriti oluline just väiksemate veebimajutusteenuse pakkujate puhul.

4.9. PÕHIÕIGUSTE KAITSE

Määrus sisaldab mitmesuguseid kaitsemeetmeid, et suurendada vastutust ja läbipaistvust seoses terroristliku veebisisu eemaldamiseks võetud meetmetega. Sellega seoses viidatakse eeltoodule, eelkõige teabele õiguskaitsevahendite, aruandluse ja piiriüleste eemaldamiskorralduste erimehhanismi kohta.

Lisaks nõutakse määruse artiklis 23, et komisjon annaks määruse hindamise raames aru kaitsemehhanismide, eelkõige artikli 4 lõikes 4, artikli 6 lõikes 3 ja artiklites 7–11 osutatud mehhanismide toimimise ja tõhususe kohta. Sellised kaitsemeetmed on seotud kaebuste, õiguskaitsevahendite ja karistusmehhanismidega, mis on vastu võetud ja rakendatud veebisisu eksliku eemaldamise ohu vastu, et kaitsta sisuteenuse ja veebimajutusteenuse pakkujaid. Kaitsemehhanismide toimimise ja tõhususe hindamine on seega osa artikli 23 kohasest hindamisest.

Sellega seoses on määruse artikli 21 lõikes 2 osutatud seirekavas ette nähtud näitajate raamistik, mille abil hinnata määruse mõju põhiõigustele ja mida kasutatakse määruse hindamisel.

Seirekava toetab hindamise osana läbiviidavat analüüsi, mis käsitleb määruse kontekstis rakendatavate kaitsemeetmete toimimist ja tõhusust ning nende mõju põhiõigustele. See mõjuvaldkond kajastab määruse artiklis 23 nimetatud kahte valdkonda: kaitsemehhanismide, eelkõige artikli 4 lõikes 4, artikli 6 lõikes 3 ja artiklites 7–11 osutatud kaitsemehhanismide toimimine ja tõhusus; b) määruse kohaldamise mõju põhiõigustele, eelkõige väljendus- ja teabevabadusele, eraelu puutumatusele ja isikuandmete kaitsele.

4.10. PÄDEVAD ASUTUSED (artikkel 13)

Määruse artikli 13 kohaselt peavad liikmesriigid tagama, et nende pädevatel asutustel on vajalikud volitused ja piisavad ressursid, et saavutada eesmärgid ja täita kohustused, mis tulenevad

määrusest. Mõned liikmesriigid on rakendanud järgmisi meetmeid, et tagada pädevatele asutustele vajalikud volitused ja piisavad ressursid:

- uute organite/direktoraatide loomine,
- lisarahastuse ja täiendavate töötajate eraldamine ning
- uute õigusraamistike loomine.

5. KOKKUVÕTE

On äärmiselt oluline, et kõik ELi tasandi vahendid ja meetmed rakendataks täielikult, et kiiresti tegeleda internetis levitatava ebaseadusliku sisuga. Seda eriti ebaseadusliku sisu suure hulga tõttu, nagu oli hiljuti näha Hamasi poolt Iisraeli vastu toime pandud rünnakuga seotud sisu puhul.

Määrus aitab suurendada avalikku julgeolekut kogu liidus ja vältida olukorda, kus terroristid kasutavad siseturul tegutsevaid veebimajutusteenuse pakkujaid oma sõnumite levitamiseks, et hirmutada, radikaliseerida ja värvata inimesi ning hõlbustada terrorirünnakute läbiviimist.

Pärast rikkumismenetluste algatamist 2023. aasta jaanuaris **on tehtud edusamme**. 31. detsembri 2023. aasta seisuga oli 23 liikmesriiki määranud artikli 12 lõike 1 alusel pädevad asutused, nagu on näha veebiregistris. Tänu sellele on määruses sätestatud meetmeid ja vahendeid süsteemsemalt kasutatud. 22st 2023. aasta jaanuaris algatatud rikkumismenetlusest 11 oli 21. detsembriks 2023 lõpetatud. Komisjon kutsub ülejäänud liikmesriike tungivalt üles võtma vajalikke meetmeid, et määrata vastavalt artikli 12 lõikele 1 pädevad asutused ning täita artikli 12 lõigetest 2 ja 3 ning artikli 18 lõikest 1 tulenevaid kohustusi.

Üldiselt on liikmesriigid teatanud, et eemaldamiskorralduste edastamine veebimajutusteenuse pakkujatele on olnud Europoli toetusel sujuv. Liikmesriikidelt ja Europolilt saadud teabe põhjal on pärast määruse jõustumist edastatud vähemalt 349 **terroristliku sisu eemaldamise korraldust**. Kümnel juhul ei eemaldanud üks veebimajutusteenuse pakkuja terroristlikku sisu ega blokeerinud sellele juurdepääsu määrusega kehtestatud ühetunnise tähtaja jooksul.

Liikmesriikidelt ja Europolilt saadud teabe kohaselt on alates määruse jõustumisest suurenenud ka reageerimine terroristlikku sisu käsitlevatele esildistele, kuigi määrus ei sisalda sellekohaseid norme. Lisaks sai Europol veebimajutusteenuse pakkujatelt üheksal juhul teavet terroristliku sisu kohta, millega kaasneb otsene oht elule, nagu on sätestatud artikli 14 lõikes 5.

Loodud on tõhusamad sidekanalid ja menetlused, eriti alates PERCI platvormi käivitamisest 3. juulil 2023. See on toonud kaasa süsteemsema lähenemisviisi eemaldamiskorralduste edastamisele. PERCI-t kasutatakse ka suure hulga esildiste edastamiseks. Liikmesriigid ja Europol väljendasid ootust, et PERCI kasutuselevõtt aitab kaasa nende vahendite kasutamisele võitluses terroristliku veebisisu vastu.

Eelneva põhjal leiab komisjon, et üldiselt on määrus avaldanud terroristliku veebisisu leviku piiramisele **positiivset mõju**. Siiski ületas eemaldamiskorralduse saanud veebimajutusteenuse pakkuja kümnel juhul 349st määruses terroristliku sisu eemaldamiseks või sellele juurdepääsu blokeerimiseks kehtestatud ühetunnist tähtaega.

Komisjon toetab ennetavalt liikmesriike ja veebimajutusteenuse pakkujaid, muu hulgas tehniliste seminaride abil, mida korraldati enne ja pärast määruse kohaldamise algust. Viimane seminar toimus 24. novembril 2023. Samuti toetab komisjon väiksemaid veebimajutusteenuse pakkujaid, et tagada määruse täielik ja kiire kohaldamine ning aidata neil lahendada seni esinenud probleeme.

Komisjon jälgib määruse rakendamist ja kohaldamist ka edaspidi. Komisjon jälgib tähelepanelikult määruses sätestatud vahendite tulemuslikkust seirekava abil, mida kasutatakse määruse hindamiseks vastavalt artiklile 23.